High Availability (SSO) Deployment Guide

Last Updated: December, 2014

Introduction

This document provides information on the theory of operation and configuration for the Cisco Unified Wireless LAN Controller (WLC) as it pertains to supporting stateful switchover of access points and clients (AP and Client SSO).

The new High Availability (HA) feature (that is, AP SSO) set within the Cisco Unified Wireless Network software release version 7.3 and 7.4 allows the access point (AP) to establish a CAPWAP tunnel with the Active WLC and share a mirror copy of the AP database with the Standby WLC. The APs do not go into the Discovery state when the Active WLC fails and the Standby WLC takes over the network as the Active WLC.

There is only one CAPWAP tunnel maintained at a time between the APs and the WLC that is in an Active state. The overall goal for the addition of AP SSO support to the Cisco Unified Wireless LAN is to reduce major downtime in wireless networks due to failure conditions that may occur due to box failover or network failover.

To support High Availability without impacting service, there needs to be support for seamless transition of clients and APs from the active controller to the standby controller. Release 7.5 supports Client Stateful Switch Over (Client SSO) in Wireless LAN controllers. Client SSO will be 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 WLC when the client associates to the WLC or the client’s parameters change. Fully authenticated clients, i.e. the ones in Run state, are synced to the Standby and thus, client re-association is avoided on switchover making the failover seamless for the APs as well as for the clients, resulting in zero client service downtime and no SSID outage.

Cisco Systems, Inc.
www.cisco.com

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- WLCs 5500 Series, 7500/8500 Series, and WiSM-2
- APs 700, 1130, 1240, 1250, 1040, 1140, 1260, 1600, 2600, 3500, 3600 Series APs, and 1520 or 1550 Series Mesh APs (MAPs).

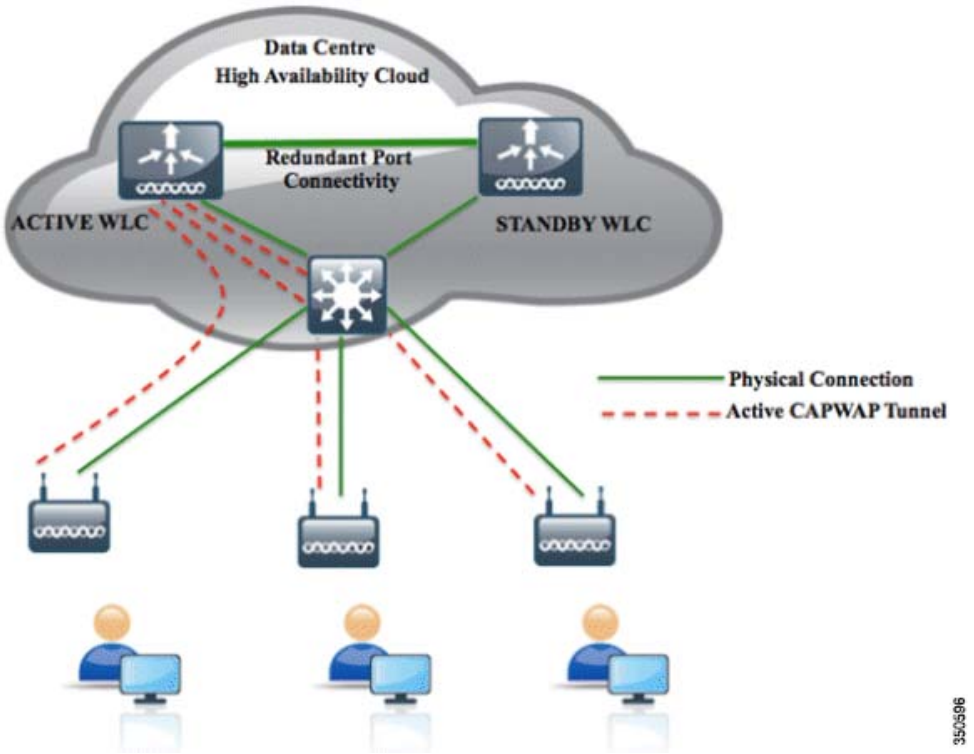
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Topology

This document uses this network topology.



High Availability in Release 7.3 and 7.4

The new architecture for HA is for box-to-box redundancy. In other words, 1:1 where one WLC will be in an Active state and the second WLC will be in a Hot Standby state continuously monitoring the health of the Active WLC via a Redundant Port. Both the WLCs will share the same set of configurations including the IP address of the Management interface. The WLC in the Standby state does not need to be configured independently as the entire configuration (Bulk Configuration while boot up and Incremental Configuration in runtime) will be synced from the Active WLC to the Standby WLC via a Redundant Port. The AP's CAPWAP State (only APs which are in a run state) is also synced, and a mirror copy of the AP database is maintained on the Standby WLC. The APs do not go into the Discovery state when the Active WLC fails and the Standby WLC takes over the network's Active WLC.

There is no preempt functionality. When the previous Active WLC comes back, it will not take the role of the Active WLC, but will negotiate its state with the current Active WLC and transition to a Standby state. The Active and Standby decision is not an automated election process. The Active/Standby WLC is decided based on HA SKU (Manufacturing Ordered UDI) from release 7.3 onwards. A WLC with HA SKU UDI will always be the Standby WLC for the first time when it boots and pairs up with a WLC running a permanent count license. For existing WLCs having a permanent count license, the Active/Standby decision can be made based on manual configuration.

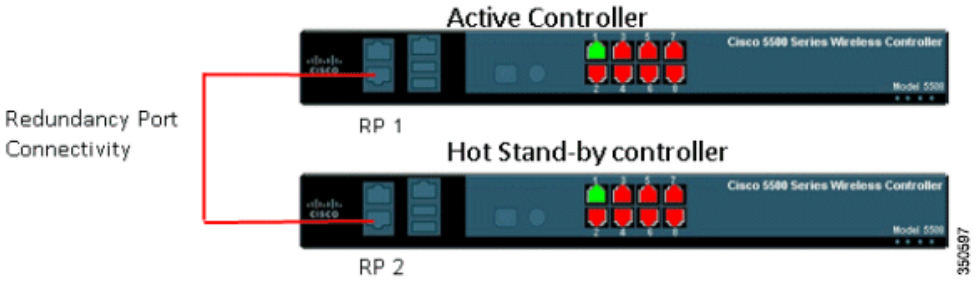
AP SSO is supported on 5500/7500/8500 and WiSM-2 WLCs. Release 7.3 only supports AP SSO that will ensure that the AP sessions are intact after switchover.

Client SSO is supported on 5500/7500/8500 and WiSM2 WLCs from release 7.5 onwards. For more information see High Availability in Release 7.5.

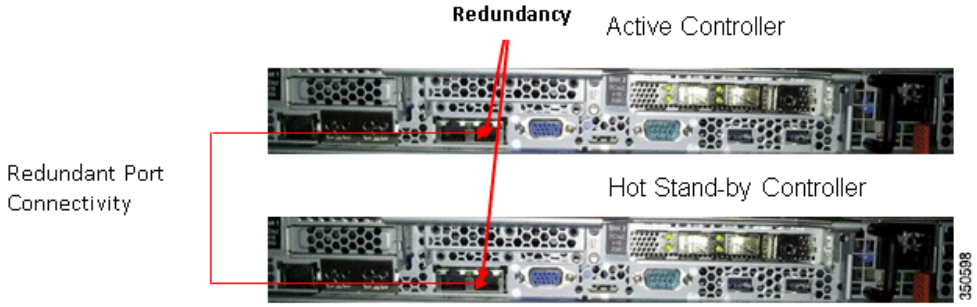
HA Connectivity Using Redundant Port on the 5500/7500/8500 WLC

- 5500/7500/8500 WLCs have a dedicated Redundancy Port which should be connected back to back in order to synchronize the configuration from the Active to the Standby WLC.
- Keep-alive packets are sent on the Redundancy Port from the Standby to the Active WLC every 100 msec (default timer) in order to check the health of the Active WLC.
- Both the WLCs in HA setup keep track of gateway reachability. The Active WLC sends an Internet Control Message Protocol (ICMP) ping to the gateway using the Management IP address as the source, and the Standby WLC sends an ICMP ping to the gateway using the Redundancy Management IP address. Both the WLCs send an ICMP ping to the gateway at a one-second interval.
- It is highly recommended to have back-to-back direct connectivity between Redundant Ports.

Here you can see the Redundant Port Connectivity between 5500 WLCs in an HA Setup:



Here you can see the Redundant Port Connectivity between Flex 7500 WLCs in an HA setup:



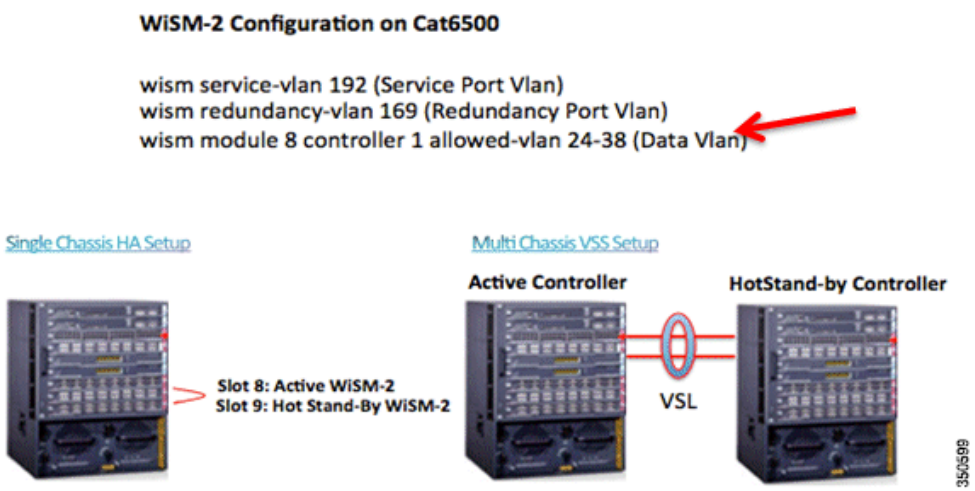
Note A direct physical connection between Active and Standby Redundant Ports is highly recommended. The distance between the connections can go up to 100 meters at per Ethernet cable standards.

High Availability Connectivity Using Redundant VLAN on WiSM-2 WLC

- WiSM-2 WLCs have a dedicated Redundancy VLAN which is used to synchronize the configuration from the Active WLC to the Standby WLC.
- A Redundancy VLAN should be a Layer 2 VLAN dedicated for the HA Pairing process. It should not be spanned across networks and should not have any Layer 3 SVI interface. No data VLAN should be used as a Redundancy VLAN.
- Keep-alive packets are sent on Redundancy VLAN from the Standby WLC to the Active WLC every 100 msec (default timer) in order to check the health of the Active WLC.

- Both the WiSMs in a HA setup keep track of gateway reachability. Active WLC sends an ICMP ping to the gateway using the Management IP address as the source, and the Standby WLC sends an ICMP ping to the gateway using the Redundancy Management IP address. Both the WLCs send an ICMP ping to the gateway at a one-second interval.
- To achieve HA between WiSM-2, it can be deployed in a single chassis or can also be deployed between multiple chassis using VSS as well as by extending Redundancy VLAN between two chassis.

This diagram shows HA Connectivity in a single chassis and extending Redundancy VLAN in a multiple chassis VSS setup:



Warning **The Redundancy VLAN should be a non routable VLAN. In other words, no layer 3 interface should be created for this VLAN and can be allowed on VSL Link to extend HA setup between multiple chassis in VSS setup. It is important to make sure this VLAN is dedicated for the HA process and is not part of any Data VLAN, or else it may result in unpredictable results.**

Note The Redundancy VLAN should be created like any normal Data VLAN on IOS® switches. Redundancy VLAN is configured for redundant port on WiSM-2 blades connected to a backplane. There is no need to configure an IP address for the Redundancy VLAN as it will receive an auto-generated IP which is discussed later in this document.

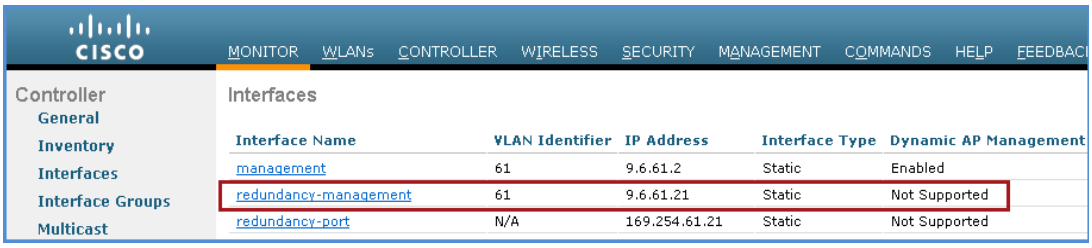
Note On Cisco WiSM2 and Cisco Catalyst 6500 Series Supervisor Engine 2T, if HA is enabled, post switchover, the APs might disconnect and reassociate with the WiSM2 controller. To prevent this from occurring, before you configure HA, we recommend that you verify–in the port channel–the details of both the active and standby Cisco WiSM2 controllers, that the ports are balanced in the same order, and the port channel hash distribution is using fixed algorithm. If they are not in order, you must change the port channel distribution to be fixed and reset Cisco WiSM2 from the Cisco Catalyst 6500 Series Supervisor Engine 2T. You can use the command `show etherchannel port-channel` to verify the port channel member order and load value. You can use the `config command port-channel hash-distribution fixed` to make the distribution fixed.

Note To support the active and standby WLCs in different data centers, in release 7.5, back-to-back redundancy port connectivity between peers is no longer mandatory and the redundancy ports can be connected via switches such that there is L2 adjacency between the two controllers. See Redundancy Port Connectivity in 7.5 for more information.

Introduction of New Interfaces for HA Interaction

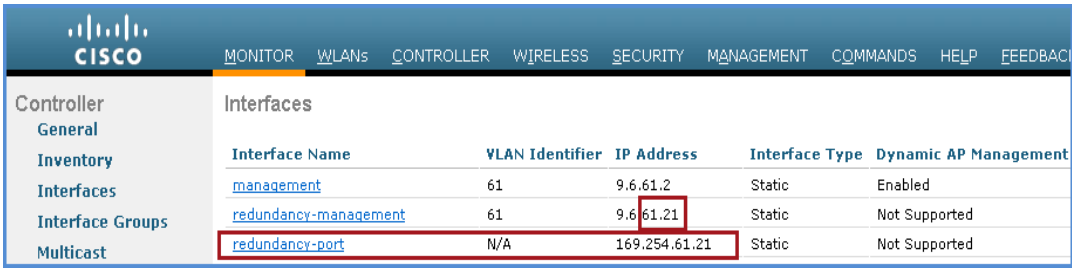
Redundancy Management Interface

The IP address on this interface should be configured in the same subnet as the management interface. This interface will check the health of the Active WLC via network infrastructure once the Active WLC does not respond to Keepalive messages on the Redundant Port. This provides an additional health check of the network and Active WLC, and confirms if switchover should or should not be executed. Also, the Standby WLC uses this interface in order to source ICMP ping packets to check gateway reachability. This interface is also used in order to send notifications from the Active WLC to the Standby WLC in the event of Box failure or Manual Reset. The Standby WLC will use this interface in order to communicate to Syslog, the NTP server, and the TFTP server for any configuration upload.



Redundancy Port

This interface has a very important role in the new HA architecture. Bulk configuration during boot up and incremental configuration are synced from the Active WLC to the Standby WLC using the Redundant Port. WLCs in a HA setup will use this port to perform HA role negotiation. The Redundancy Port is also used in order to check peer reachability sending UDP keep-alive messages every 100 msec (default timer) from the Standby WLC to the Active WLC. Also, in the event of a box failure, the Active WLC will send notification to the Standby WLC via the Redundant Port. If the NTP server is not configured, a manual time sync is performed from the Active WLC to the Standby WLC on the Redundant Port. This port in case of standalone controller and redundancy VLAN in case of WISM-2 will be assigned an auto generated IP Address where last 2 octets are picked from the last 2 octets of Redundancy Management Interface (the first 2 octets are always 169.254).



Configure HA from the CLI

Complete these steps:

1. Before you configure HA, it is mandatory to have both the controllers' management interface in the same subnet:

   WLC 1:

```
(5508) >show interface summary

 Number of Interfaces..... 5

Interface Name                   Port Vlan Id  IP Address      Type    Ap Mgr Guest
-------------------------------- ---- -------- --------------- ------- ------ -----
management                       1    61       9.6.61.2        Static  Yes    No
redundancy-management            1    61       0.0.0.0         Static  No     No
redundancy-port                  N/A  N/A      0.0.0.0         Static  No     No
service-port                     N/A  N/A      0.0.0.0         DHCP    No     No
virtual                          N/A  N/A      1.1.1.1         Static  No     No
```

   WLC 2:

```
(5508) >show interface summary

 Number of Interfaces..... 5

Interface Name                   Port Vlan Id  IP Address      Type    Ap Mgr Guest
-------------------------------- ---- -------- --------------- ------- ------ -----
management                       1    61       9.6.61.3        Static  Yes    No
redundancy-management            1    61       0.0.0.0         Static  No     No
redundancy-port                  N/A  N/A      0.0.0.0         Static  No     No
service-port                     N/A  N/A      0.0.0.0         DHCP    No     No
virtual                          N/A  N/A      1.1.1.1         Static  No     No
```

2. HA is disabled by default. Before you enable HA, it is mandatory to configure the Redundancy Management IP Address and Peer Redundancy Management IP Address. Both the interfaces should be in the same subnet as the Management Interface. In this example, 9.6.61.21 is the Redundancy Management IP Address for WLC 1, and 9.6.61.23 is the Redundancy Management IP Address for WLC 2. It also needs to be configured so that 9.6.61.23 is the Redundancy Management IP Address of WLC 2 and 9.6.61.21 is the Redundancy Management IP Address of WLC 1.

   Use this CLI in order to configure the Redundancy and Peer Redundancy Management IP Address:

   WLC 1:

```
(5508) >config interface address redundancy-management 9.6.61.21 peer-redundancy-management 9.6.61.23

(5508) >show interface summary

 Number of Interfaces..... 5

Interface Name                   Port Vlan Id  IP Address      Type    Ap Mgr Guest
-------------------------------- ---- -------- --------------- ------- ------ -----
management                       1    61       9.6.61.2        Static  Yes    No
redundancy-management            1    61       9.6.61.21       Static  No     No
redundancy-port                  N/A  N/A      169.254.61.21   Static  No     No
service-port                     N/A  N/A      0.0.0.0         DHCP    No     No
virtual                          N/A  N/A      1.1.1.1         Static  No     No
```

WLC 2:

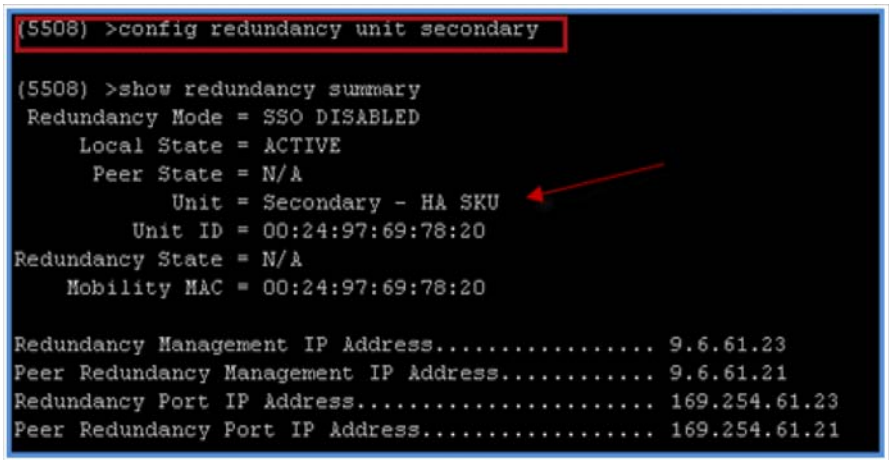
```
(5508) >config interface address redundancy-management 9.6.61.23 peer-redundancy-management 9.6.61.21


(5508) >show interface summary


 Number of Interfaces..... 5

Interface Name                   Port Vlan Id  IP Address      Type    Ap Mgr Guest
-------------------------------- ---- -------- --------------- ------- ------ -----
management                       1    61       9.6.61.2        Static  Yes    No
redundancy-management            1    61       9.6.61.23       Static  No     No
redundancy-port                  N/A  N/A      169.254.61.23   Static  No     No
service-port                     N/A  N/A      0.0.0.0         DHCP    No     No
virtual                          N/A  N/A      1.1.1.1         Static  No     No
```

3. Configure one WLC as Primary (by default, the WLC HA Unit ID is Primary and should have a valid AP-BASE count license installed) and another WLC as Secondary (AP base count from the Primary WLC will be inherited by this unit) using the CLI in this step. In this example, WLC 1 is configured as Primary, and WLC 2 is configured as Secondary:

   WLC 1:

```
(5508) >config redundancy unit primary

(5508) >show redundancy summary
 Redundancy Mode = SSO DISABLED
      Local State = ACTIVE
       Peer State = N/A
             Unit = Primary
          Unit ID = 00:24:97:69:D2:20
Redundancy State = N/A
    Mobility MAC = 00:24:97:69:D2:20

Redundancy Management IP Address.................. 9.6.61.21
Peer Redundancy Management IP Address............. 9.6.61.23
Redundancy Port IP Address........................ 169.254.61.21
Peer Redundancy Port IP Address................... 169.254.61.23
```

   WLC 2:



Note You do not need to configure the unit as Secondary if it is a factory ordered HA SKU that can be ordered from release 7.3 onwards. A factory ordered HA SKU is a default Secondary unit, and will take the role of the Standby WLC the first time it is paired with an Active WLC that has a valid AP Count License.

If you want to convert any existing WLC as a Standby WLC, do so using the config redundancy unit secondary command in the CLI. This CLI command will only work if the WLC which is intended to work as Standby has some number of permanent license count. This condition is only valid for the 5500 WLC, where a minimum of 50 AP Permanent licenses are needed to be converted to Standby. There is no restriction for other WLCs such as the WiSM2, 7500, and 8500.

4. After the WLCs are configured with Redundancy Management and Peer Redundancy Management IP Addresses and Redundant Units are configured, it is time to enable SSO. It is important to make sure that physical connections are up between both the controllers (that is, both the WLCs are connected back to back via the Redundant Port using an Ethernet cable) and the uplink is also connected to the infrastructure switch and the gateway is reachable from both the WLCs before SSO is enabled.

   Once SSO is enabled, it will reboot the WLCs. While it boots, the WLCs negotiate the HA role as per the configuration via Redundant Port. If the WLCs cannot reach each other via Redundant Port or via the Redundant Management Interface, the WLC configured as Secondary may go in to Maintenance Mode. Maintenance Mode is discussed later in this document.

5. Use the CLI in this step in order to enable AP SSO. Remember that enabling AP SSO will initiate a WLC reboot.

   WLC 1:

```
(5508) >config redundancy mode sso

All unsaved configuration will be saved.
And the system will be reset. Are you sure? (y/n)y

Configuration Saved!
System will now restart!
```

350607

WLC 2:

```
(5508) >config redundancy mode sso

All unsaved configuration will be saved.
And the system will be reset. Are you sure? (y/n)y

Configuration Saved!
System will now restart!
```

350608

6. Enabling SSO will reboot the WLCs in order to negotiate the HA role as per the configuration performed. Once the role is determined, configuration is synced from the Active WLC to the Standby WLC via the Redundant Port. Initially, the WLC configured as Secondary will report XML mismatch and will download the configuration from Active and reboot again. During the next reboot after role determination, it will validate the configuration again, report no XML mismatch, and process further in order to establish itself as the Standby WLC.

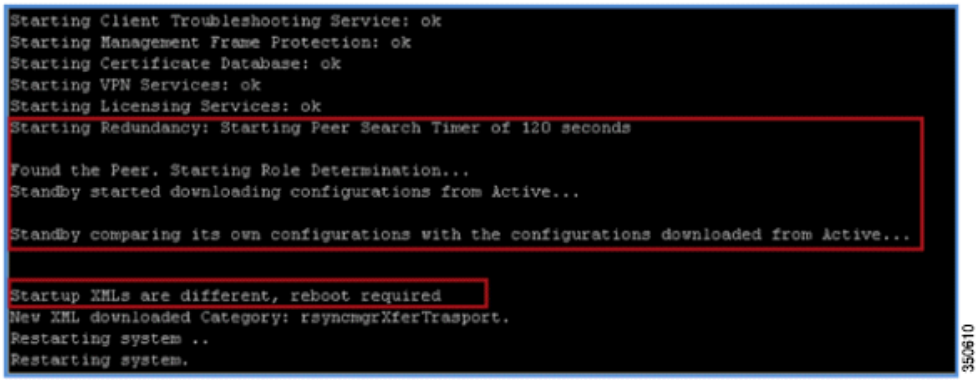
   These are the boot-up logs from both the WLCs:

   WLC 1:

```
Starting Switching Services: ok
Starting QoS Services: ok
Starting Policy Manager: ok
Starting Data Transport Link Layer: ok
Starting Access Control List Services: ok
Starting Client Troubleshooting Service: ok
Starting Management Frame Protection: ok
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...
Starting LWAPP: ok
Starting CAPWAP: ok
Starting LOCP: ok
Starting Security Services: ok
Starting Policy Manager: ok
Starting Authentication Engine: ok
Starting Mobility Management: ok
Starting Virtual AP Services: ok
```

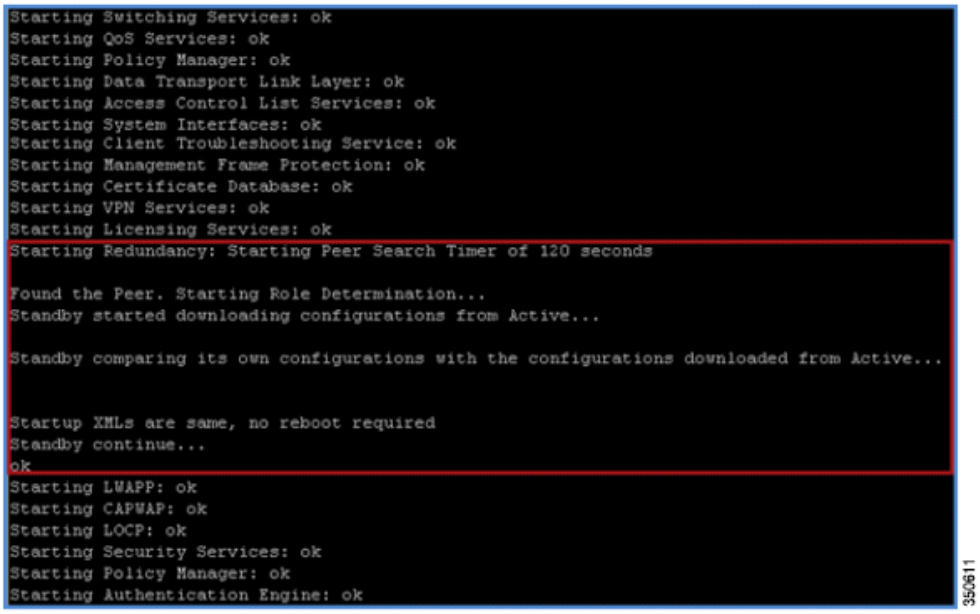
350609

   WLC 2 on first reboot after enabling SSO:



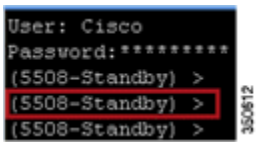
Note Once SSO is enabled, the Standby WLC can be accessed via console connection or via SSH on the service port and on the redundant management interface.

WLC 2 on second reboot after downloading XML configuration from Active:

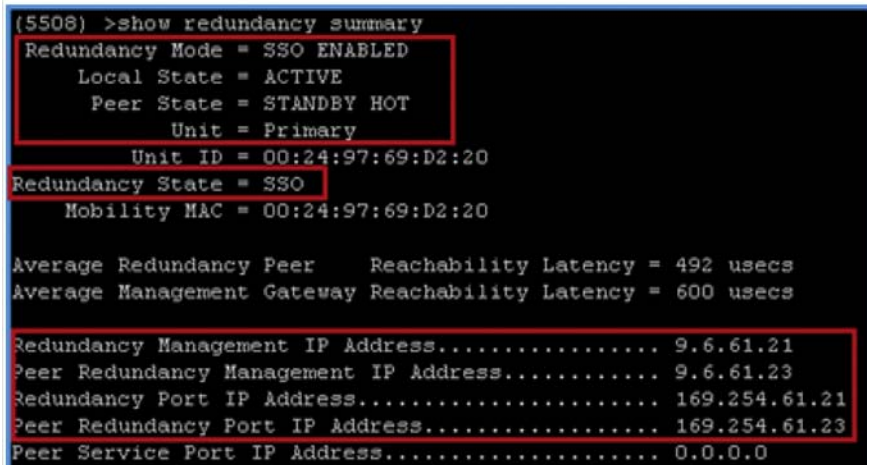


7. After SSO is enabled, WLC is rebooted, and the XML configuration is synced, WLC 1 will transition its state to Active and WLC 2 will transition its state to Standby HOT. From this point onwards, GUI/Telnet/SSH for WLC 2 on the management interface will not work, as all the configurations and management should be done from the Active WLC. If required, the Standby WLC (WLC 2, in this example) can only be managed via the Console or Service Port.

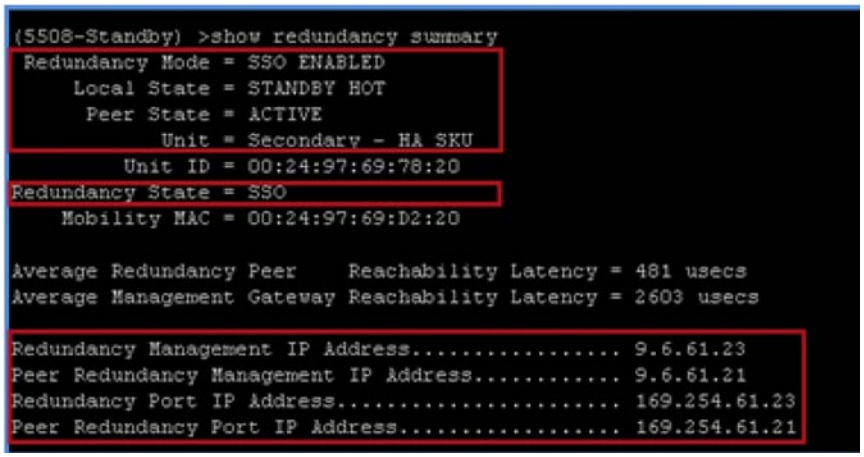
   Also, once the Peer WLC transitions to the Standby Hot state, -Standby keyword is automatically appended to the Standby WLCs prompt name.



8. Complete these steps in order to check the redundancy status:
   a. For WLC 1, go to **Monitor > Redundancy > Summary**:



   b. For WLC 2, go to Console connection:



Note Once SSO is enabled, the Standby WLC can be accessed via console connection or via SSH on the service port and on the redundant management interface.

Disabling SSO on HA Pair

1. On primary controller, disable SSO using the command:

   Config redundancy mode disable

   The Active and Standby WLCs reboot once this command is executed.

   The standby controller, when it comes back after the reboot, has the same IP address on interfaces as the primary controller and all the ports disabled.

2. On the standby controller, re-enter the correct IP addresses corresponding to the management and dynamic interfaces and execute the following command:

   Config port adminmode all enable

3. Save the configuration on the controller.

4. To re-enable SSO, execute the command **Config redundancy sso** on the primary and secondary controllers.

   Both controllers reboot and pair up in the SSO mode. The standby will sync its configuration from the primary and come back in Hot-standby mode.

Configure HA from the GUI

Complete these steps:

1. Before you configure HA, it is mandatory to have both the controllers' management interface in the same subnet:

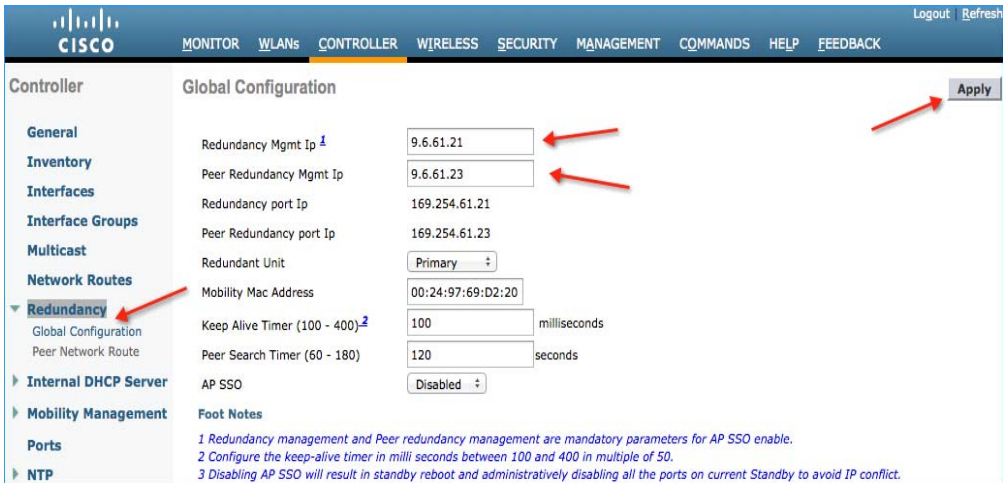
   WLC 1:

   WLC 2:

2. HA is disabled by default. Before you enable HA, it is mandatory to configure the Redundancy Management IP Address and the Peer Redundancy Management IP Address. Both interfaces should be in the same subnet as the Management Interface. In this example, 9.6.61.21 is the Redundancy Management IP Address for WLC 1, and 9.6.61.23 is the Redundancy Management IP Address for WLC 2. It needs to be configured on WLC 2 where 9.6.61.23 is the Redundancy Management IP Address of WLC 2 and 9.6.61.21 is the Redundancy Management IP Address of WLC 1.

   Enter the IP Address for both interfaces, and click **Apply**.

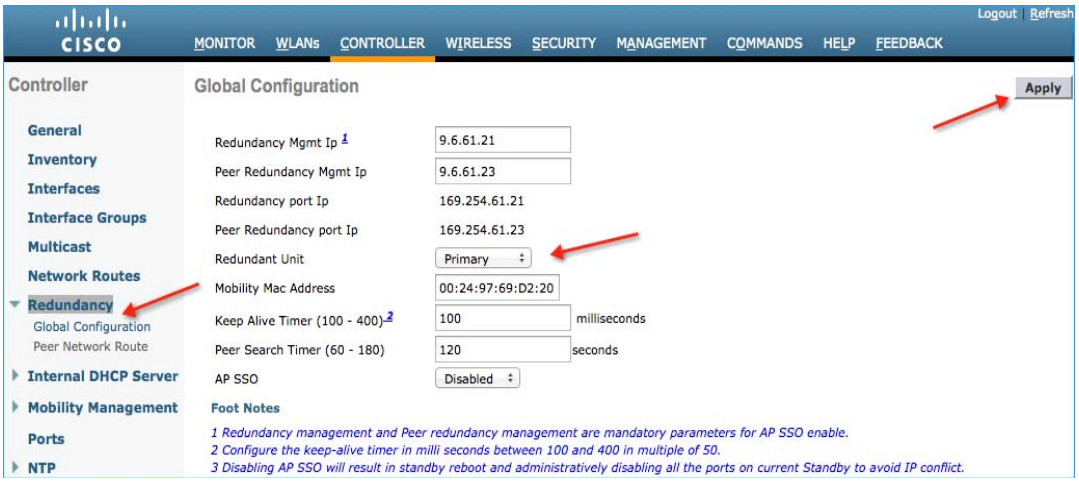
   WLC 1:



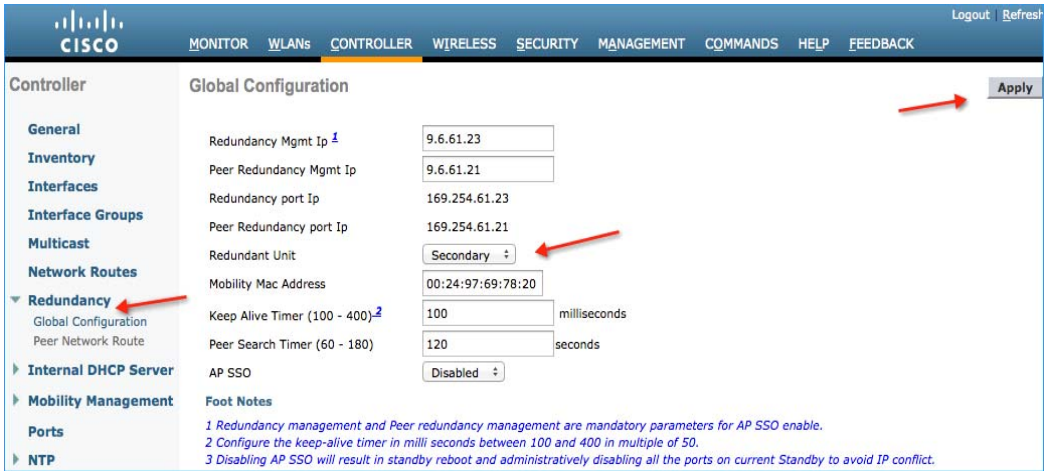
WLC 2:

3. Configure one WLC as **Primary** and the other WLC as **Secondary** from the Redundant Unit drop-down list. In this example, WLC 1 is configured as Primary and WLC 2 is configured as Secondary. Once configured, click **Apply**.

   WLC 1:



WLC 2:



Note You do not need to configure the unit as Secondary if it is a factory ordered HA SKU ordered from release 7.3 onwards. A factory ordered HA SKU is the default Secondary unit and will take the role of the Standby WLC the first time it is paired with an Active WLC with a valid AP Count License.

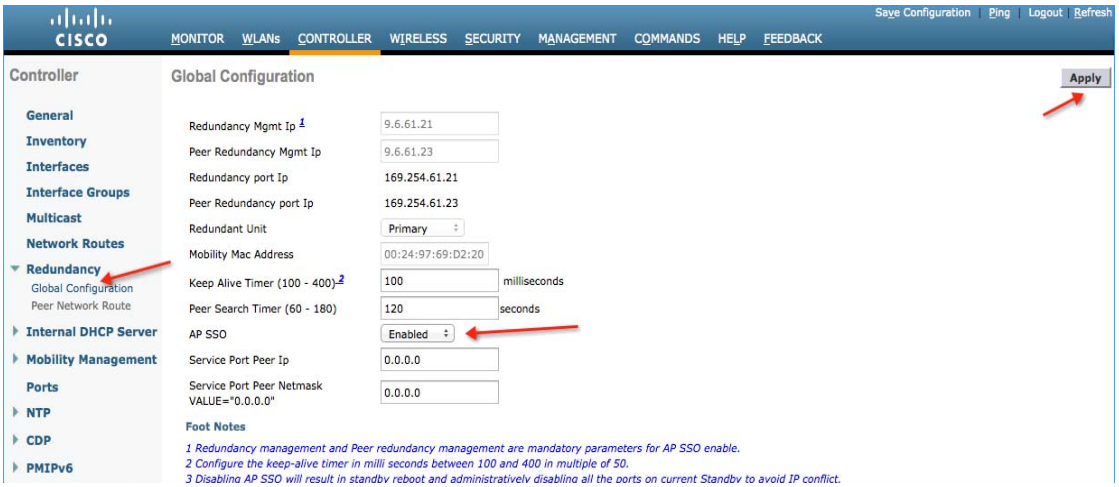
If you want to convert any existing WLC as a Standby WLC, do so by using the config redundancy unit secondary command in the CLI. This CLI only works if the WLC which is intended to work as standby has some number of permanent license count. This condition is only valid for the 5500 WLC, where a minimum of 50 AP Permanent licenses are needed to be converted to Standby. There is no restriction for other WLCs such as the WiSM2, 7500, and 8500.

4. After the WLCs are configured with Redundancy Management and Peer Redundancy Management IP Address and Redundant Units are configured, it is time to enable SSO. It is important to make sure that physical connections are up between both the controllers (that is, both the WLCs are connected back to back via Redundant Port using an Ethernet cable) and the uplink is also connected to the infrastructure switch and the gateway is reachable from both the WLCs before SSO is enabled.

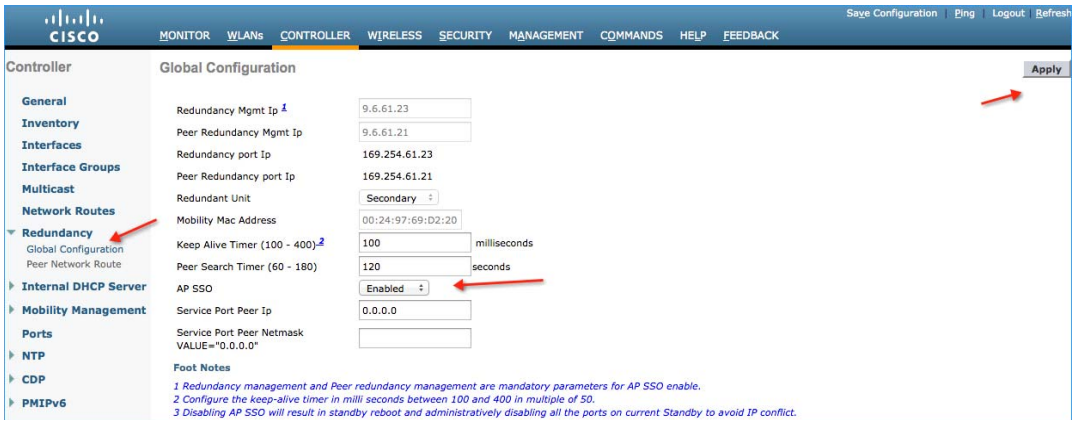
Once SSO is enabled, it will reboot the WLCs. While it boots, the WLCs negotiate the HA role as per the configuration via Redundant Port. If the WLCs cannot reach each other via the Redundant Port or via the Redundant Management Interface, the WLC configured as Secondary may go in Maintenance Mode. Maintenance Mode is discussed later in this document.

5. In order to enable AP SSO, select Enabled from the drop-down list on both the WLCs, and click **Apply.** After you enable AP SSO, the WLCs reboot and the default information is populated in other fields like Peer Service Port IP, Peer Redundancy port IP, and so forth.

   WLC 1:



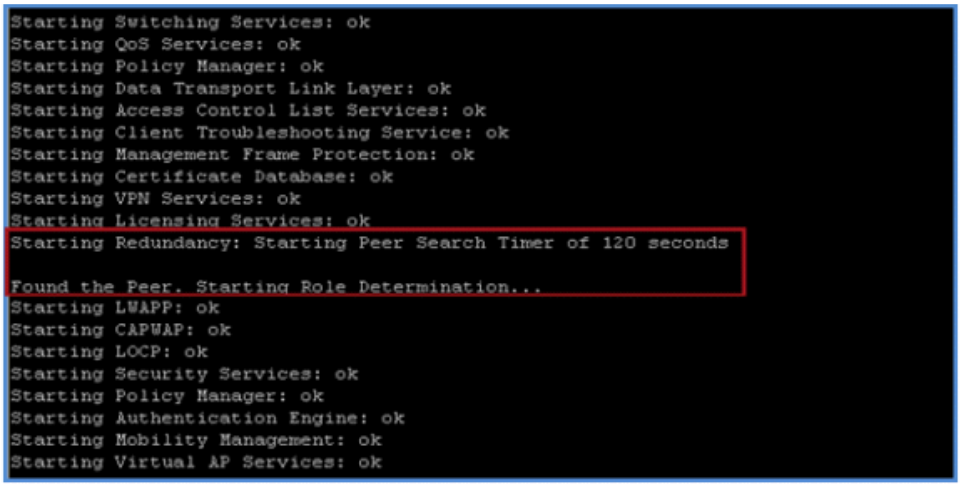
   WLC 2:



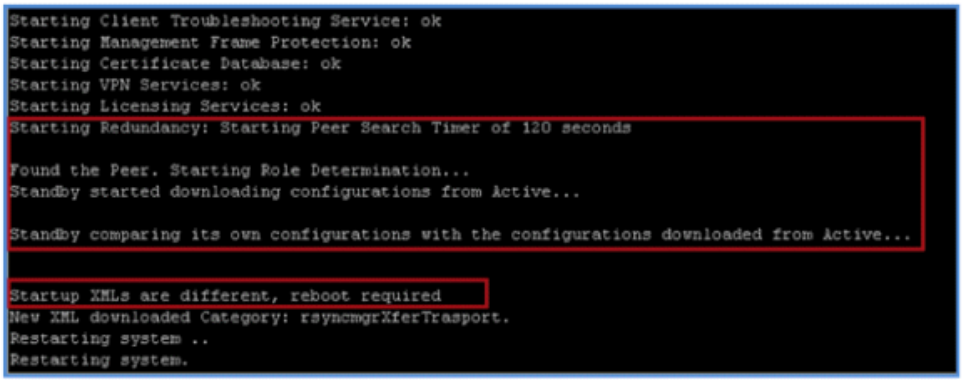
6. Enabling SSO will reboot the WLCs in order to negotiate the HA role as per the configuration performed. Once the role is determined, configuration is synced from the Active WLC to the Standby WLC via the Redundant Port. Initially WLC configured, as Secondary will report XML mismatch and will download the configuration from Active and reboot again. During the next reboot after role determination, it will validate the configuration again, report no XML mismatch, and will process further in order to establish itself as the Standby WLC.

   These are the boot-up logs from both the WLCs:

   WLC 1:



WLC on first reboot after enabling SSO:



Note Once SSO is enabled, the Standby WLC can be accessed via console connection or via SSH on the service port and on the redundant management interface.

WLC 2 on second reboot after downloading XML configuration from Active:

```
Starting Switching Services: ok
Starting QoS Services: ok
Starting Policy Manager: ok
Starting Data Transport Link Layer: ok
Starting Access Control List Services: ok
Starting System Interfaces: ok
Starting Client Troubleshooting Service: ok
Starting Management Frame Protection: ok
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...
Standby started downloading configurations from Active...

Standby comparing its own configurations with the configurations downloaded from Active...


Startup XMLs are same, no reboot required
Standby continue...
ok
Starting LWAPP: ok
Starting CAPWAP: ok
Starting LOCP: ok
Starting Security Services: ok
Starting Policy Manager: ok
Starting Authentication Engine: ok
```

350624

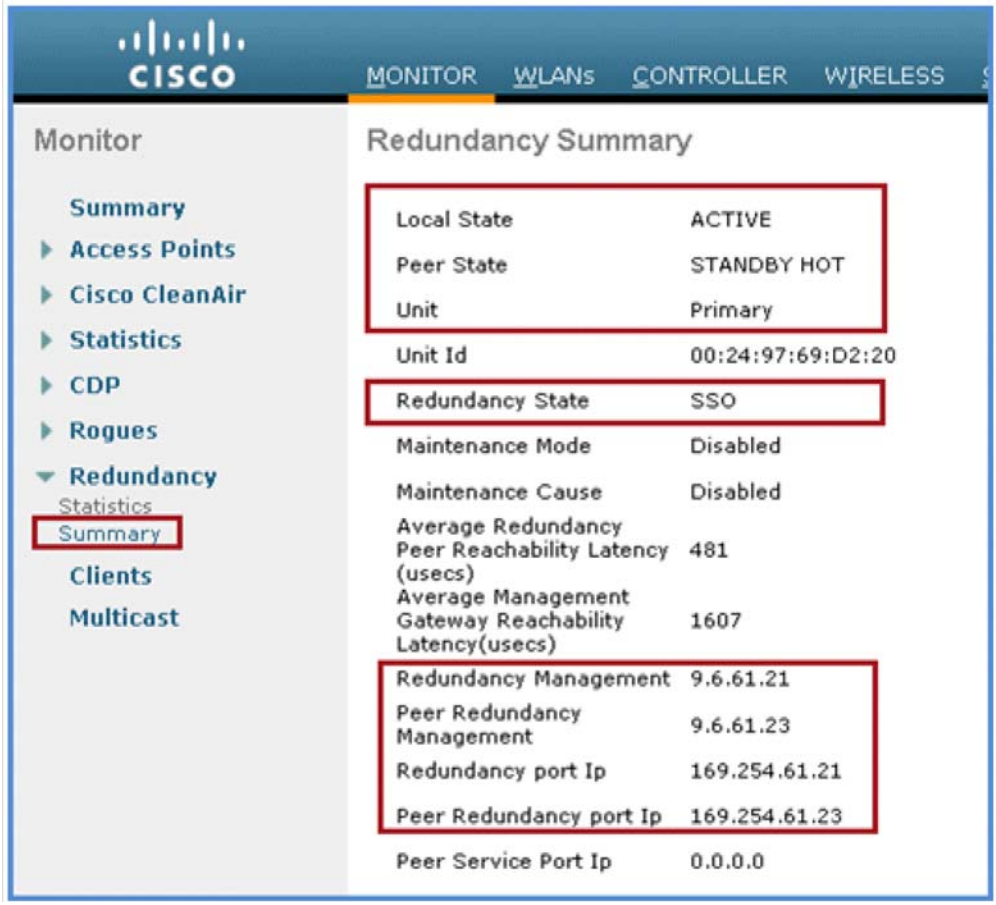
7. After SSO is enabled, WLC is rebooted, and the XML configuration is synced, WLC 1 transitions its state as Active and WLC 2 transitions its state to STANDBY HOT. From this point onwards, GUI/Telnet/SSH for WLC 2 on the management interface will not work, as all the configurations and management should be done from the Active WLC. If required, the Standby WLC (WLC 2, in this case) can only be managed via the Console or Service Port.

   Also, once Peer WLC transitions to the STANDBY HOT state, the -Standby keyword is automatically appended to Standby WLCs prompt name.

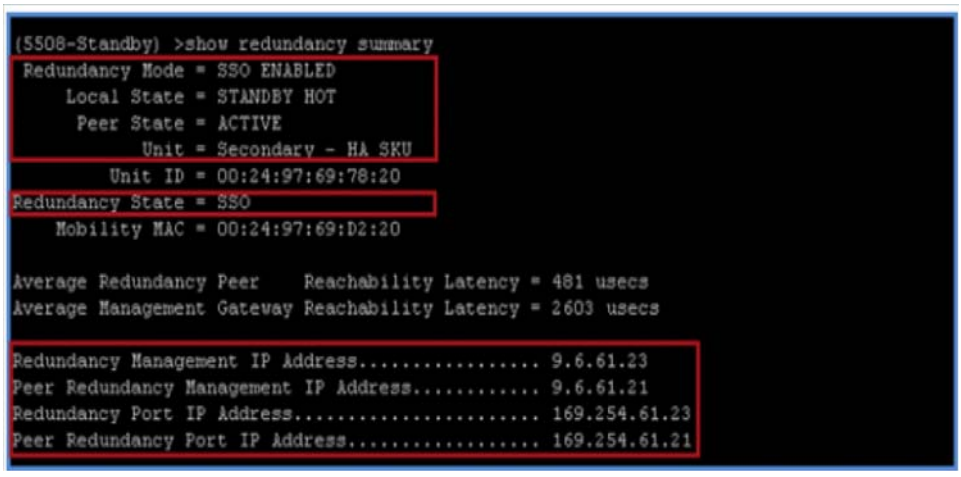
```
User: Cisco
Password:*********
(5508-Standby) >
(5508-Standby) >
(5508-Standby) >
```

350625

8. Complete these steps in order to check the redundancy status:
   a. For WLC 1, go to **Monitor > Redundancy > Summary**:



b. For WLC 2, go to Console connection:



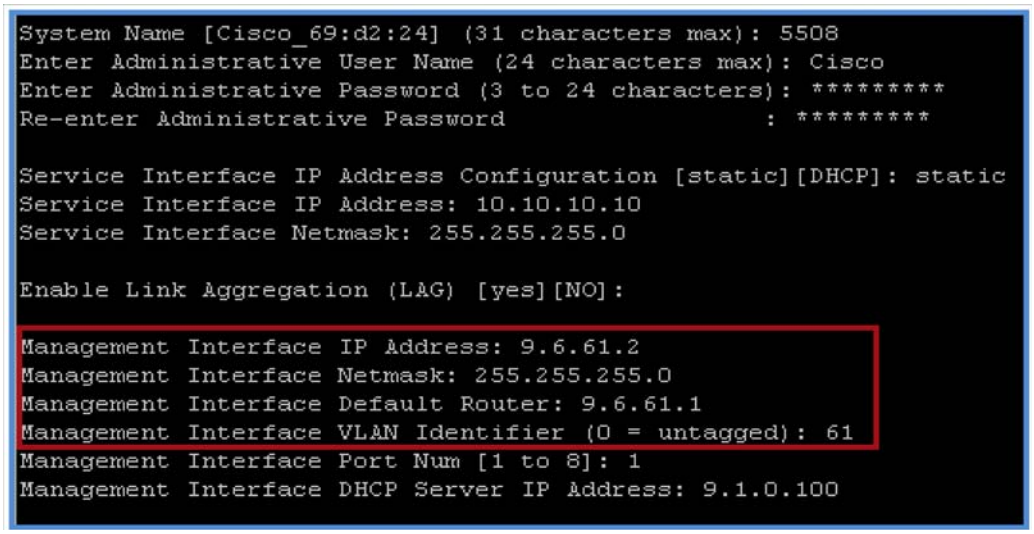
Note Once SSO is enabled, the Standby WLC can be accessed via console connection or via SSH on the service port and on the redundant management interface.

Configure HA from the Configuration Wizard

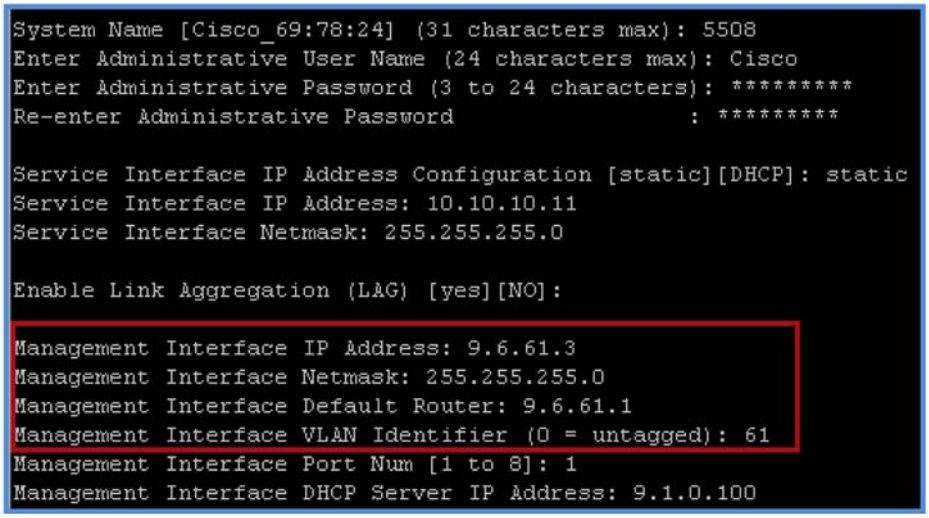
Complete these steps:

1. HA between two WLCs can also be enabled from the configuration wizard. It is mandatory to configure the Management IP Address of both the WLCs in same subnet before you enable HA.

   WLC 1:



   WLC 2:



2. Once the Management IP is configured, the wizard will prompt you to enable HA. Enter yes in order to enable HA, which is followed by the configuration of the Primary/Secondary Unit and the Redundancy Management and Peer Management IP Address.

   - In this example, WLC 1 is configured as the Primary WLC, which will take the role of the Active WLC. WLC 2 is configured as Secondary, which will take the role of the Standby WLC.

- After entering the Primary/Secondary Unit, it is mandatory to configure the Redundancy Management and the Peer Redundancy Management IP Address. Both the interfaces should be in the same subnet as the Management Interface. In this example, 9.6.61.21 is the Redundancy Management IP Address for WLC 1 and 9.6.61.23 is the Redundancy Management IP Address for WLC 2. It needs to be configured on WLC 2 where 9.6.61.23 is the Redundancy Management IP Address of WLC 2 and 9.6.61.21 is the Redundancy Management IP Address of WLC 1.

WLC 1:

```
System Name [Cisco_69:d2:24] (31 characters max): 5508
Enter Administrative User Name (24 characters max): Cisco
Enter Administrative Password (3 to 24 characters): *********
Re-enter Administrative Password                  : *********

Service Interface IP Address Configuration [static][DHCP]: static
Service Interface IP Address: 10.10.10.10
Service Interface Netmask: 255.255.255.0

Enable Link Aggregation (LAG) [yes][NO]:

Management Interface IP Address: 9.6.61.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 9.6.61.1
Management Interface VLAN Identifier (0 = untagged): 61
Management Interface Port Num [1 to 8]: 1
Management Interface DHCP Server IP Address: 9.1.0.100

Enable HA [yes][NO]: yes

Configure HA Unit [PRIMARY][secondary]: Primary

Redundancy Management IP Address: 9.6.61.21

Peer Redundancy Management IP Address: 9.6.61.23

Virtual Gateway IP Address: 1.1.1.1
```

WLC 2:

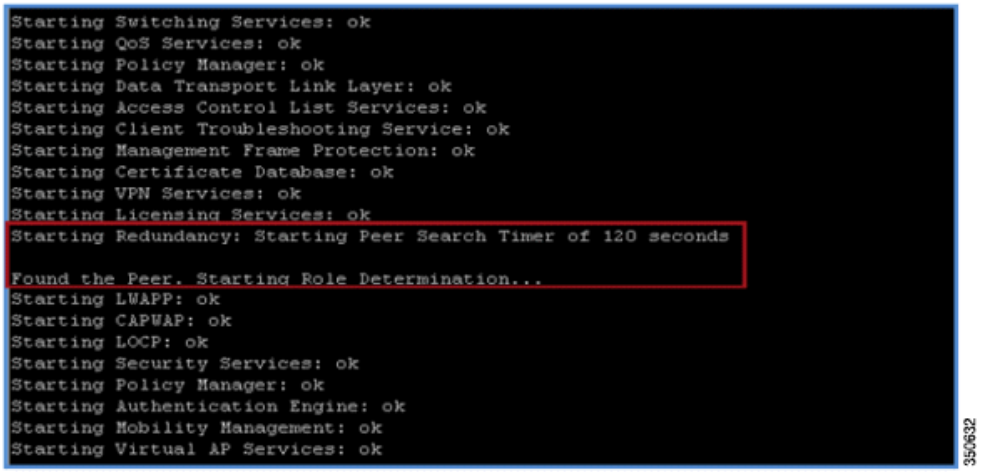
```
System Name [Cisco_69:78:24] (31 characters max): 5508
Enter Administrative User Name (24 characters max): Cisco
Enter Administrative Password (3 to 24 characters): *********
Re-enter Administrative Password                  : *********

Service Interface IP Address Configuration [static][DHCP]: static
Service Interface IP Address: 10.10.10.11
Service Interface Netmask: 255.255.255.0

Enable Link Aggregation (LAG) [yes][NO]:

Management Interface IP Address: 9.6.61.3
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 9.6.61.1
Management Interface VLAN Identifier (0 = untagged): 61
Management Interface Port Num [1 to 8]: 1
Management Interface DHCP Server IP Address: 9.1.0.100

Enable HA [yes][NO]: yes

Configure HA Unit [PRIMARY][secondary]: secondary

Redundancy Management IP Address: 9.6.61.23

Peer Redundancy Management IP Address: 9.6.61.21

Virtual Gateway IP Address: 1.1.1.1
```

3. After you enable HA from the configuration wizard, continue to configure these legacy wizard parameters:
   - Virtual IP Address
   - Mobility Domain Name
   - SSID
   - DHCP Bridging Mode
   - Radius configuration
   - Country Code
   - NTP configuration, and so forth

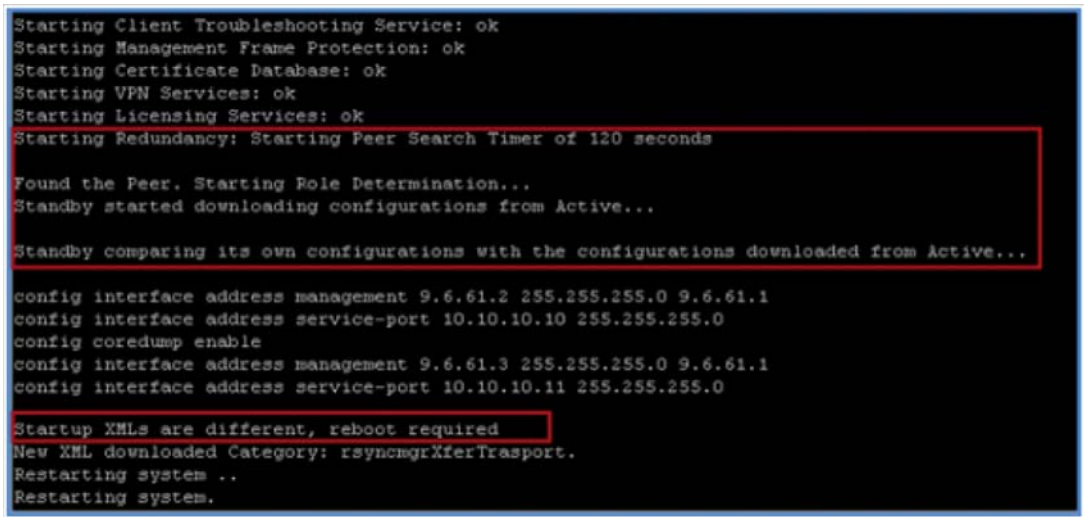
   The WLCs will reboot after you save the configuration at the end.
4. While booting, the WLCs will negotiate the HA role as per the configuration done. Once the role is determined, the configuration is synced from the Active WLC to the Standby WLC via the Redundant Port. Initially WLC is configured, as Secondary will report XML mismatch and will download the configuration from Active and reboot again. During the next reboot after role determination, it will validate the configuration again, report no XML mismatch, and process further in order to establish itself as the Standby WLC.

   These are the boot-up logs from both the WLCs:

   WLC 1:



WLC 2 on first reboot after enabling HA:



WLC 2 on second reboot after downloading XML configuration from Active:

```
Starting Switching Services: ok
Starting QoS Services: ok
Starting Policy Manager: ok
Starting Data Transport Link Layer: ok
Starting Access Control List Services: ok
Starting System Interfaces: ok
Starting Client Troubleshooting Service: ok
Starting Management Frame Protection: ok
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...
Standby started downloading configurations from Active...

Standby comparing its own configurations with the configurations downloaded from Active...


Startup XMLs are same, no reboot required
Standby continue...
ok
Starting LWAPP: ok
Starting CAPWAP: ok
Starting LOCP: ok
Starting Security Services: ok
Starting Policy Manager: ok
Starting Authentication Engine: ok
```

350634

Note Once SSO is enabled, the Standby WLC can be accessed via console connection or via SSH on the service port and on the redundant management interface.

5. After HA is enabled followed by WLC reboots and XML configuration is synced, WLC 1 will transition its state as Active and WLC 2 will transition its state as STANDBY HOT. From this point onwards GUI/Telnet/SSH for WLC 2 on management interface will not work, as all the configurations and management should be done from Active WLC. If required, the Standby WLC (WLC 2, in this case) can only be managed via the Console or Service Port.

   Also, once the Peer WLC transitions to the STANDBY Hot state, the -Standby keyword is automatically appended to the Standby WLCs prompt name.

```
User: Cisco
Password:*********
(5508-Standby) >
(5508-Standby) >
(5508-Standby) >
```

350635

6. Complete these steps in order to check the redundancy status:
   a. For WLC 1:

```
(5508) >show redundancy summary
 Redundancy Mode = SSO ENABLED
     Local State = ACTIVE
      Peer State = STANDBY HOT
            Unit = Primary
         Unit ID = 00:24:97:69:D2:20
Redundancy State = SSO
    Mobility MAC = 00:24:97:69:D2:20

Average Redundancy Peer    Reachability Latency = 486 usecs
Average Management Gateway Reachability Latency = 2043 usecs

Redundancy Management IP Address.................. 9.6.61.21
Peer Redundancy Management IP Address............. 9.6.61.23
Redundancy Port IP Address........................ 169.254.61.21
Peer Redundancy Port IP Address................... 169.254.61.23
Peer Service Port IP Address...................... 10.10.10.11
```

b. For WLC 2, go to Console connection:

```
(5508-Standby) >show redundancy summary
 Redundancy Mode = SSO ENABLED
     Local State = STANDBY HOT
      Peer State = ACTIVE
            Unit = Secondary - HA SKU
         Unit ID = 00:24:97:69:78:20
Redundancy State = SSO
    Mobility MAC = 00:24:97:69:D2:20

Average Redundancy Peer    Reachability Latency = 506 usecs
Average Management Gateway Reachability Latency = 676 usecs

Redundancy Management IP Address.................. 9.6.61.23
Peer Redundancy Management IP Address............. 9.6.61.21
Redundancy Port IP Address........................ 169.254.61.23
Peer Redundancy Port IP Address................... 169.254.61.21
```

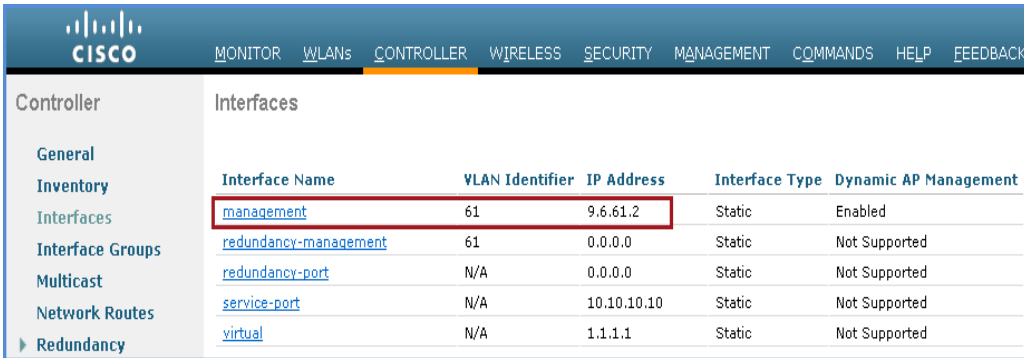
Note Once SSO is enabled, the Standby WLC can be accessed via console connection or via SSH on the service port and on the redundant management interface.

Configure HA from Cisco Prime

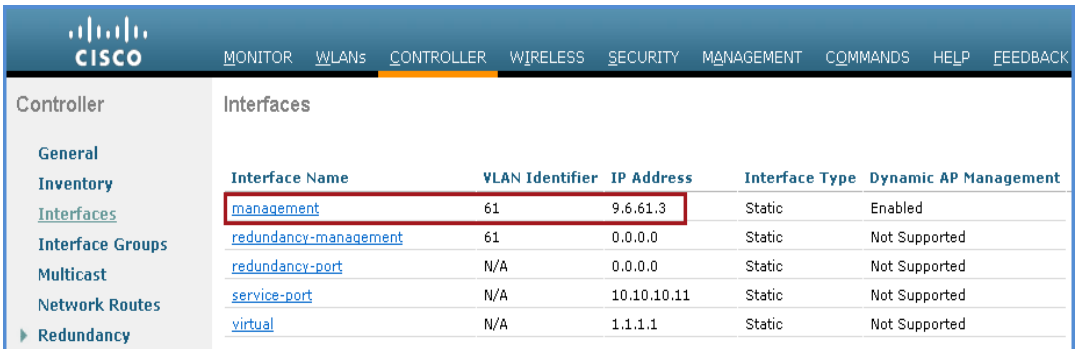
Complete these steps:

1. Before you configure HA, it is mandatory to have both the controllers' management interface in the same subnet.

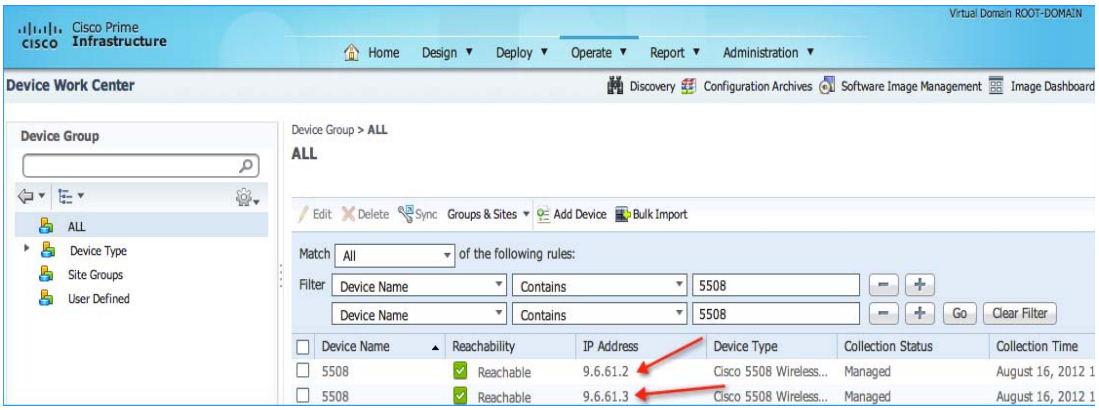
WLC 1:



WLC 2:



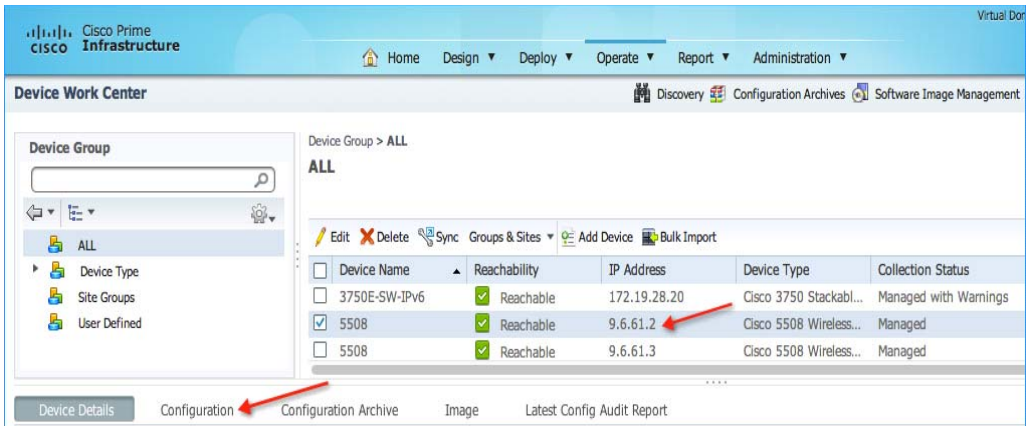
2. Add both the controllers in Cisco Prime using their individual Management IP Address. Once added, both the WLCs can be viewed under **Operate > Device Work Center**.



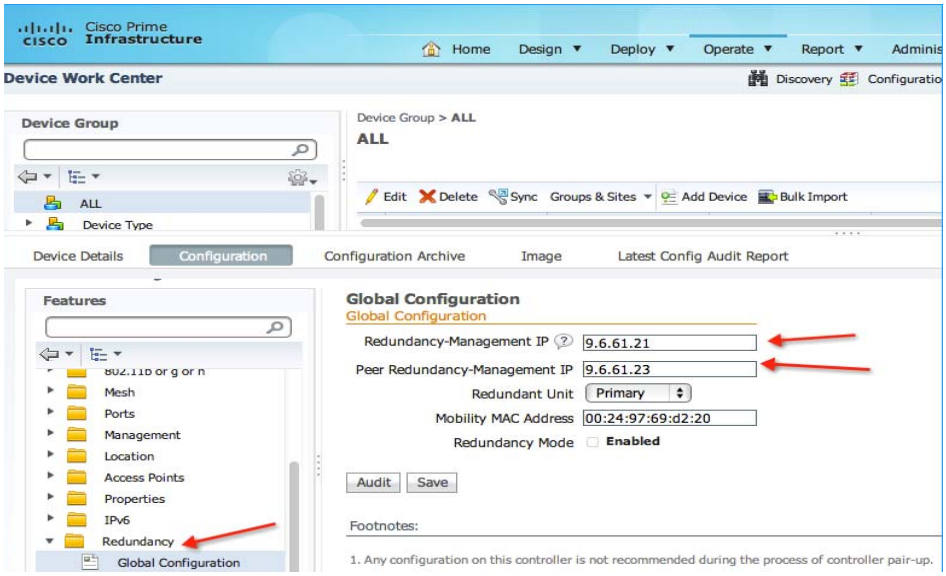
3. HA is disabled by default. Before you enable HA, it is mandatory to configure the Redundancy Management IP Address and the Peer Redundancy Management IP Address. Both the interfaces should be in the same subnet as the Management Interface. In this example, 9.6.61.21 is the Redundancy Management IP Address for WLC 1 and 9.6.61.23 is the Redundancy Management IP Address of WLC 2. It needs to be configured on WLC 2 where 9.6.61.23 is the Redundancy Management IP Address of WLC 2 and 9.6.61.21 is the Redundancy Management IP Address of WLC 1.

In order to configure from Cisco Prime, go to Operate > Device Work Center, and select the controller by clicking on the check box in front of the device on which HA should be configured. Once selected, click the Configuration tab, which provides all the options needed to configure the WLC 1, and repeat the steps for WLC 2.

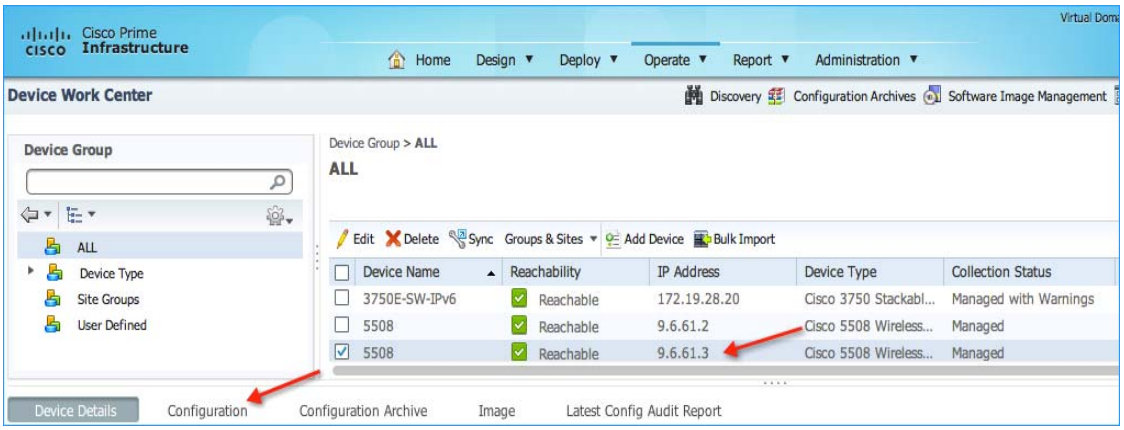
WLC 1:



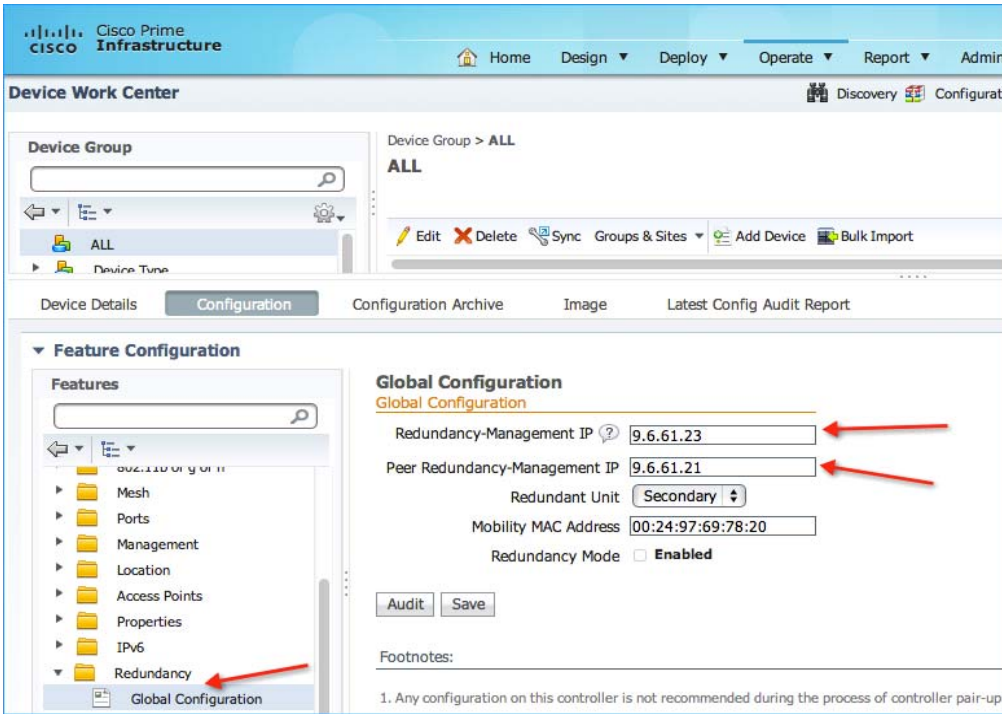
In order to configure the HA parameters for WLC 1, go to **Redundancy > Global Configuration**, enter the Redundancy and Peer Redundancy-Management IP address, and click Save.



WLC 2:

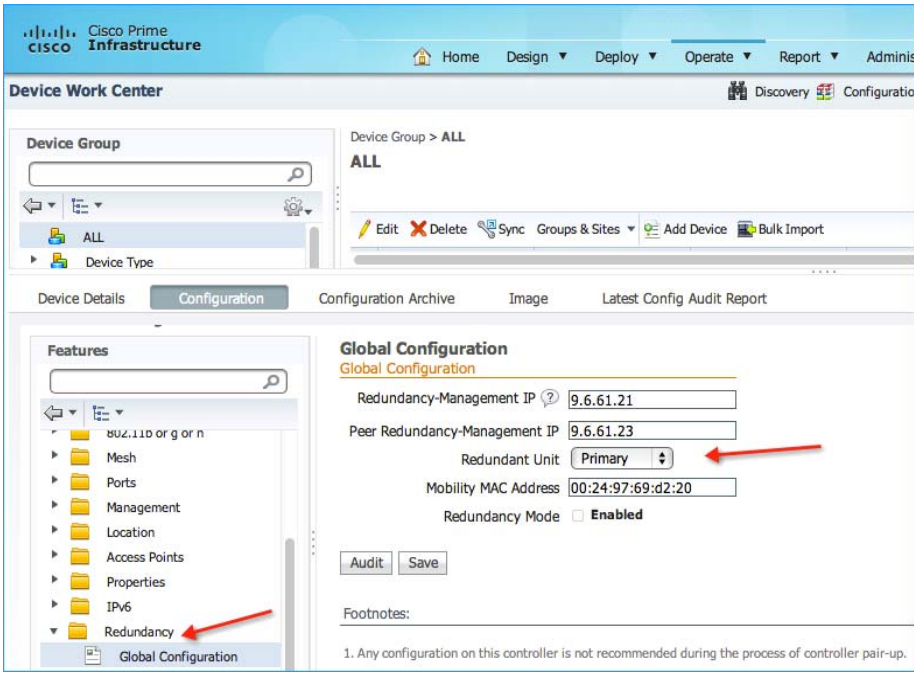


In order to configure the HA parameters for WLC 2, go to **Redundancy > Global Configuration**, enter the Redundancy and Peer Redundancy-Management IP address, and click Save.

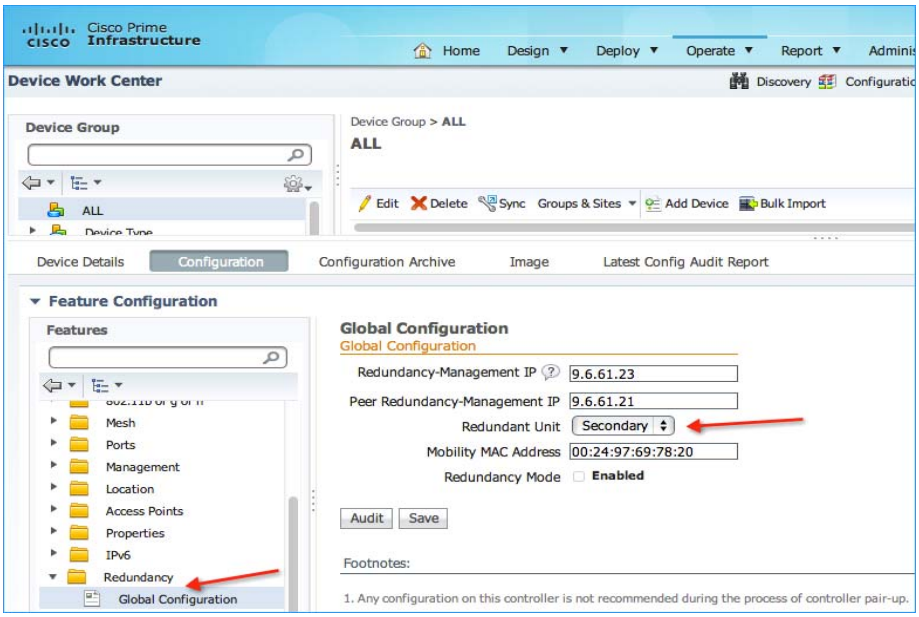


4. Configure one WLC as **Primary** and the other WLC as Secondary from the Redundant Unit drop-down list. In this example, WLC 1 is configured as Primary and WLC 2 is configured as Secondary. Once configured, click **Save**.

   WLC 1:

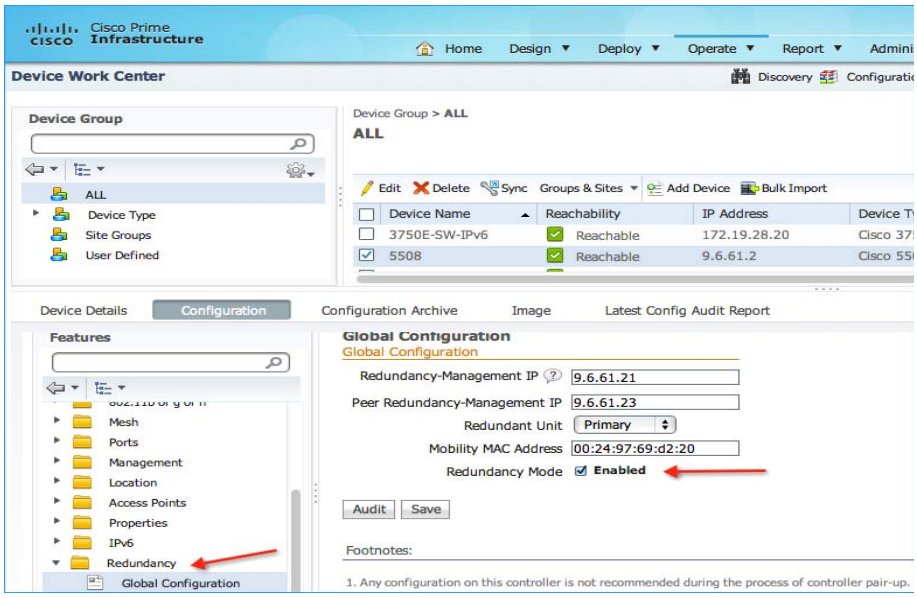


WLC 2:

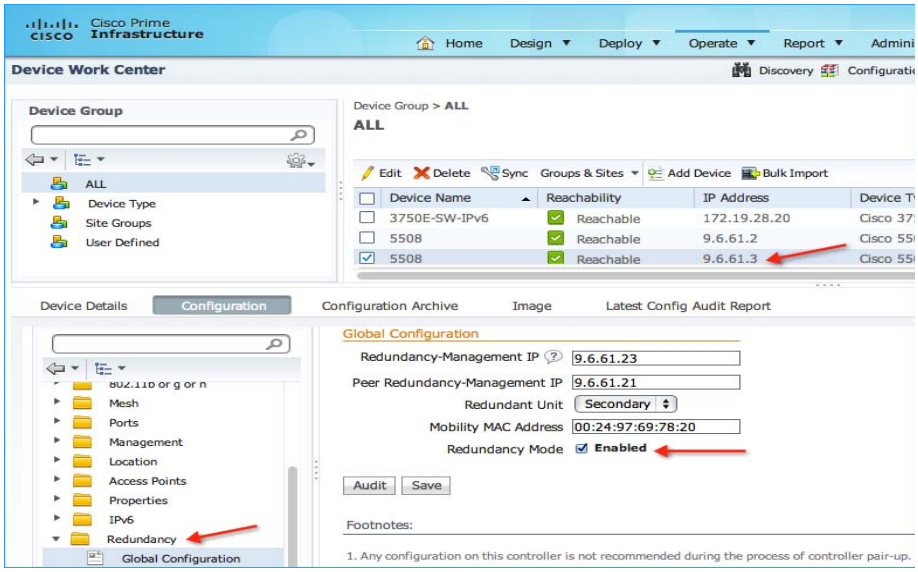


5. After the WLCs are configured with Redundancy Management and Peer Redundancy Management IP Address, and the Redundant Units are configured, it is time to enable SSO. Once SSO is enabled, it will reboot the WLCs. While booting, the WLCs negotiate the HA role as per configuration via Redundant Port. If the WLCs cannot reach each other via the Redundant Port or via the Redundant Management Interface, the WLC configured as secondary may go in to Maintenance Mode. Maintenance Mode is discussed later in this document.
6. Check the **Enabled** check box, in order to enable redundancy mode, and click Save. The WLCs will reboot once redundancy mode is enabled.

WLC 1:



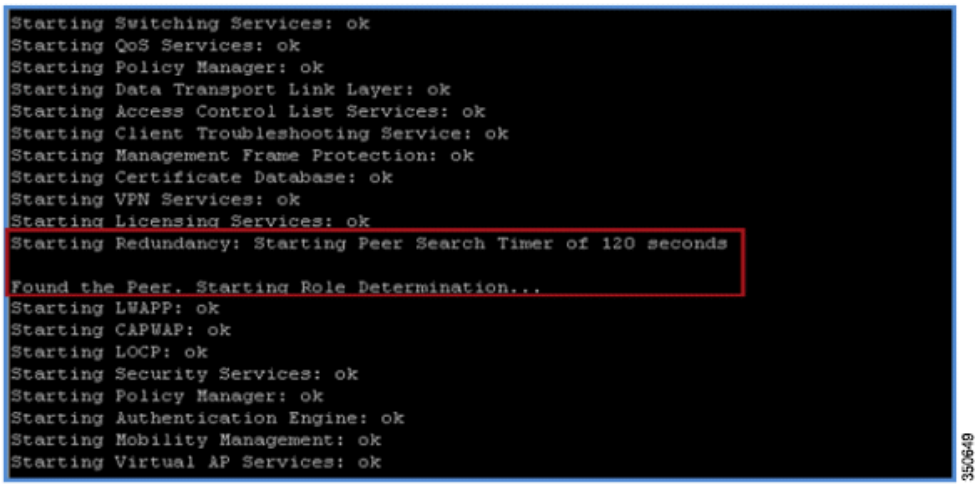
WLC 2:



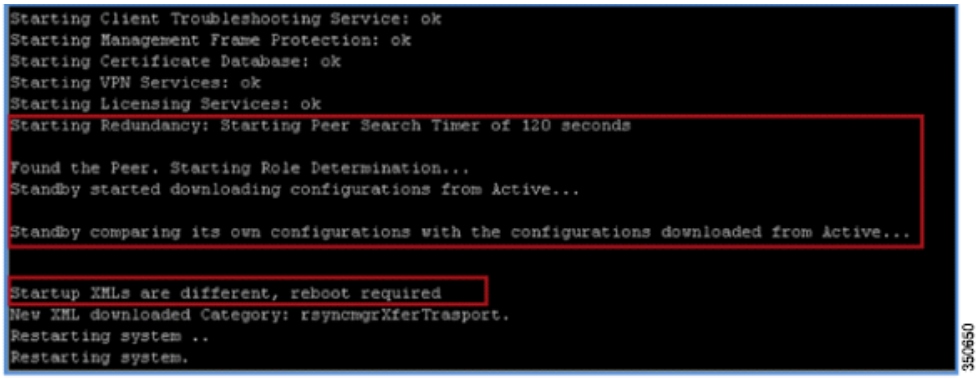
7. Enabling SSO will reboot the WLCs in order to negotiate the HA role as per the configuration performed. Once the role is determined, the configuration is synced from the Active WLC to the Standby WLC via the Redundant Port. Initially WLC configured, as Secondary will report XML mismatch and will download the configuration from Active and reboot again. In the next reboot after role determination, it will validate the configuration again, report no XML mismatch, and process further in order to establish itself as the Standby WLC.

   These are the boot-up logs from both the WLCs:

   WLC 1:



WLC 2 on first reboot after enabling SSO:



Note Once SSO is enabled, the Standby WLC can be accessed via console connection or via SSH on the service port and on the redundant management interface.

WLC 2 on second reboot after downloading XML configuration from Active:

```
Starting Switching Services: ok
Starting QoS Services: ok
Starting Policy Manager: ok
Starting Data Transport Link Layer: ok
Starting Access Control List Services: ok
Starting System Interfaces: ok
Starting Client Troubleshooting Service: ok
Starting Management Frame Protection: ok
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...
Standby started downloading configurations from Active...

Standby comparing its own configurations with the configurations downloaded from Active...


Startup XMLs are same, no reboot required
Standby continue...
ok
Starting LWAPP: ok
Starting CAPWAP: ok
Starting LOCP: ok
Starting Security Services: ok
Starting Policy Manager: ok
Starting Authentication Engine: ok
```

350651

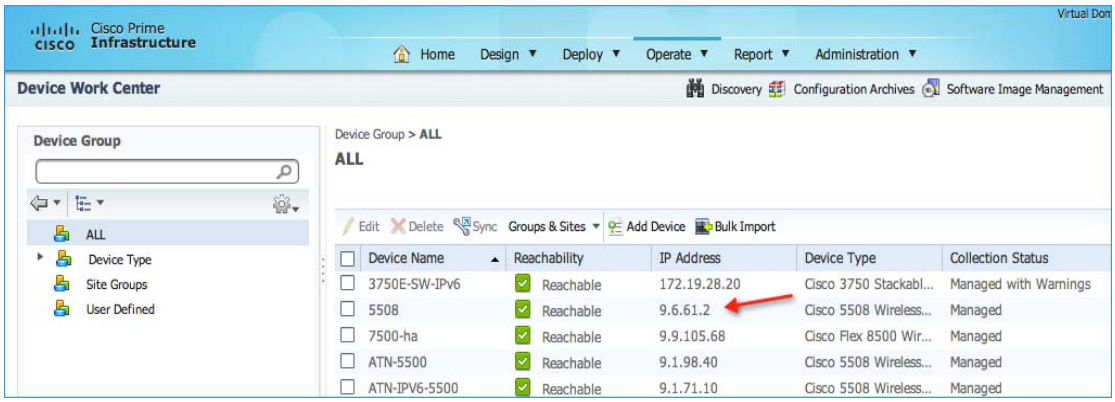
8. After SSO is enabled followed by the WLC reboot and XML configuration is synced, WLC 1 will transition its state as Active and WLC 2 will transition its state as STANDBY HOT. From this point onwards, the GUI/Telnet/SSH for WLC 2 on the management interface will not work, as all the configurations and management should be done from the Active WLC. If required, the Standby WLC (WLC 2, in this case) can only be managed via the Console or Service Port.

   Also, once the Peer WLC transitions to the STANDBY Hot state, the -Standby keyword is automatically appended to the Standby WLCs prompt name.

```
User: Cisco
Password:*********
(5508-Standby) >
(5508-Standby) >
(5508-Standby) >
```

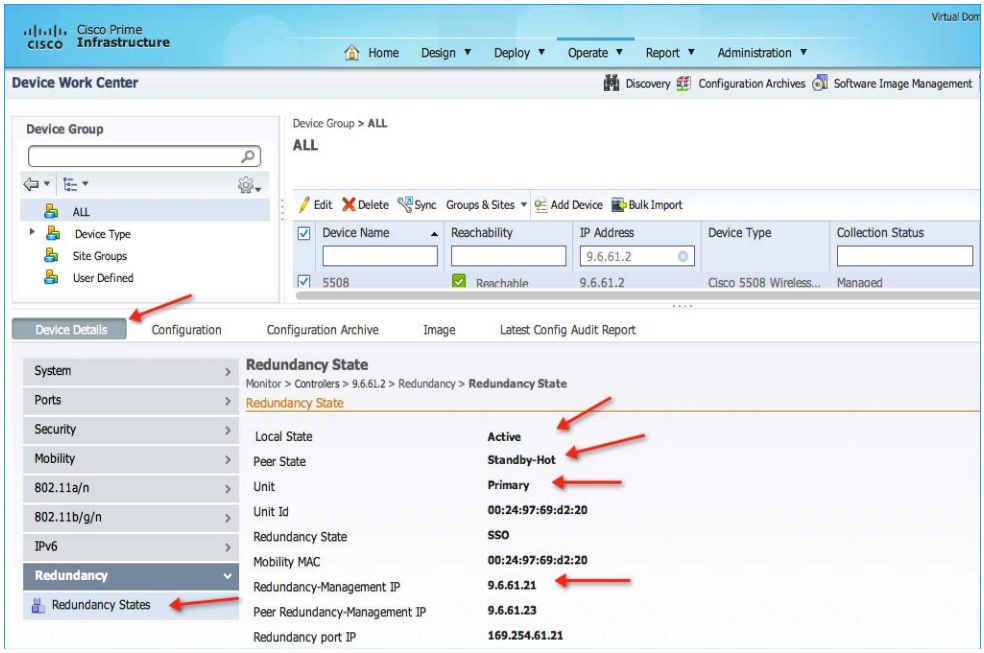
350652

9. Once the HA pairing is formed, Cisco Prime removes/deletes the WLC 2 entry from its database as both the WLCs have the same management IP address. For the network, it is the one box which is active in the network.



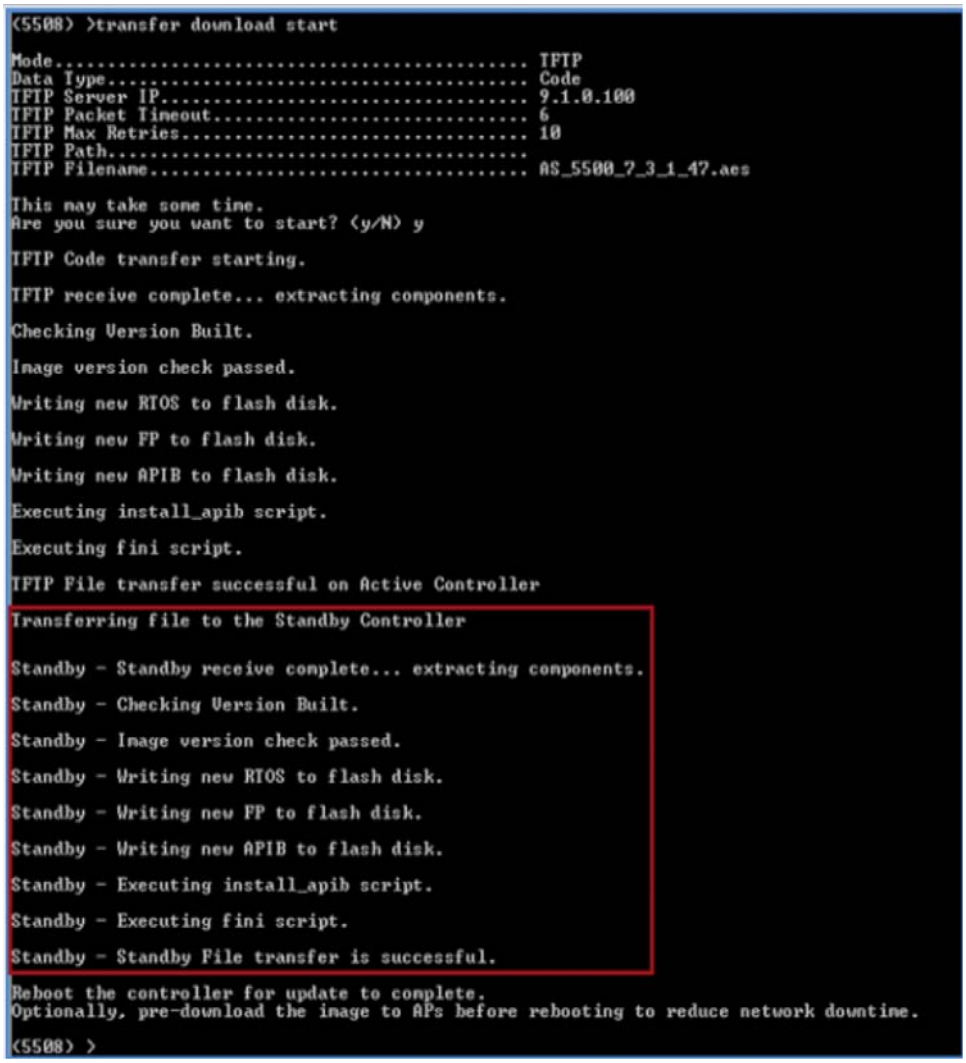
Note From this image, it is clear that only WLC 1 (with an IP address of 9.6.61.2 and configured as Primary Unit) is active on Cisco Prime. WLC 2, which was initially added in Cisco Prime with an IP address 9.6.61.3, is deleted from Cisco Prime database after HA pairing is formed.

10. In order to check the redundancy state of the Active WLC from Cisco Prime, go to **Device Details > Redundancy > Redundancy States**.



Upgrade the WLC in HA Setup

The Standby WLC cannot be upgraded directly from the TFTP/FTP server. After executing all scripts, the Active WLC transfers the image to the Standby WLC. Once the Standby WLC receives the image from the Active WLC, it starts executing upgrade scripts. All the logs for image transfer and script execution on the Standby WLC can be seen on the Active WLC.



Note The FUS image can be upgraded while the controllers have HA enabled. The secondary controller will get upgraded just like it does when upgrading the regular code. However, when you initiate the reboot on the primary controller both controllers will be unreachable until the FUS upgrade completes on both the active and the standby in the HA pair. This process will take around 30 to 40 minutes to complete just like in a non-HA FUS upgrade.

Upgrade Procedure in HA Setup

Complete these steps:

1. After the WLCs are configured in the HA setup, the Standby WLC cannot be upgraded directly from the TFTP/FTP server.
2. Initiate upgrade on the Active WLC in the HA setup via CLI/GUI, and wait for the upgrade to finish.
3. Once the Active WLC executes all the upgrade scripts, it will transfer the entire image to the Standby WLC via the Redundant Port.

4. When the Standby WLC receives the image from the Active WLC, it will start executing the upgrade scripts. The transfer of the image to standby and the execution of the upgrade scripts on the Standby WLC can be seen on the Active WLC Console/Telnet/SSH/Http connection.
5. After a successful message of Standby Upgrade is observed on the Active WLC, it is important to issue the show boot command on the Active WLC in order to make sure the new image is set as the primary image.
6. Once verified, initiate primary image pre-download on the Active WLC in order to transfer the new image to all the APs in the network.
7. After pre-image is completed on all the APs, issue the show AP image all command in order to verify that the primary image on the WLC is set as the backup image on APs.
8. Initiate swap option to interchange the backup image as primary on the APs. With this implementation, the WLC's and AP's primary image is set to the new image.
9. Issue the schedule-reset command as per planned outage with the no swap option in order to reset the APs and WLCs so that they can boot with the new image.
10. All the APs will reboot and join the new Active WLC.
11. Issue the show boot, show sysinfo, show ap image all, and show redundancy summary commands in order to verify that both the WLCs and APs have booted with the new image.

Important Guidelines before Initiating a WLC Upgrade in HA Setup

- Service Upgrade is not supported in this release, so network downtime should be planned before you upgrade the WLCs in the HA setup.
- The peer should be in the Hot Standby state before you start the upgrade in the HA setup.
- It is recommended to reboot both the WLCs almost together after upgrade so that there is no software version mismatch.
- Schedule Reset applies to both the WLCs in the HA setup.
- The Standby WLC can be rebooted from the Active WLC using the reset peer-system command if a scheduled reset is not planned.
- Debug transfer can be enabled on the Active WLC as well as the Standby WLC.
- If Active WLC unexpectedly reboot between software download and reboot both WLCs, you need to reboot both WLCs in order to complete software upgrade.

Download/Upload Facts in HA Setup

- No direct download and upload configuration is possible from the Standby WLC.
- All download file types like Image, Configuration, Web-Authentication bundle, and Signature Files will be downloaded on the Active WLC first and then pushed automatically to the Standby WLC.
- Once the configuration file is downloaded on the Active WLC, it is pushed to the Standby WLC. This results in the reset of the Standby WLC first, followed by the reset of the Active WLC.
- The Peer Service Port and Static route configuration is a part of a different XML file, and will not be applied if downloaded as part of the configuration file.
- The download of certificates should be done separately on each box and should be done before pairing.

- Uploading different file types like Configuration, Event Logs, Crash files, and so forth can be done separately from the Standby WLC. However, the CLI to configure different parameters for upload like Server IP, file type, path and name should be done on the Active WLC. Once the upload parameters are configured on the Active WLC, the `transfer upload peer-start` command should be issued on the Active WLC in order to initiate the upload from the Standby WLC.
- The service port state will be synced from the Active WLC to the Standby WLC. That is, if DHCP is enabled on the Active WLC service port, the Standby WLC will also use DHCP for getting the service port IP address. If the service port of the Active WLC is configured with a Static IP Address, the Standby WLC also needs to be configured with a different Static IP Address. The CLI to configure the IP Address for the Standby WLC service port is `configure redundancy interface address peer-service-port <IP Address>` . This command should be executed from the Active WLC. Also, in order to configure the route on the Standby WLC for out-of-band management on the service port, issue the `configure redundancy peer-route add <Network IP Address > <IP Mask> <Gateway>` command from the Active WLC.

Failover Process in the HA Setup

In the HA setup, the AP's CAPWAP state is maintained on the Active WLC as well as the Standby WLC (only for APs which are in a Run state). That is, Up Time and Association Up Time is maintained on both the WLC, and when switchover is initiated, the Standby WLC takes over the network. In this example, WLC 1 is in an Active state and serving the network, and WLC 2 is in a Standby state monitoring the Active WLC. Although WLC 2 is in Standby state, it still maintains the CAPWAP state of the AP.

WLC 1:

```
(5508) >show ap uptime

Number of APs.................................... 1
Global AP User Name.............................. cisco
Global AP Dot1x User Name........................ Not Configured

AP Name             Ethernet MAC       AP Up Time               Association Up Time
-----------------   -----------------  -----------------------  -----------------------
AP_3500E            c4:7d:4f:3a:07:74  0 days, 02 h 37 m 33 s   0 days, 02 h 36 m 22 s
```

350656

WLC 2:

```
(5508-Standby) >show ap uptime

Number of APs.................................... 1
Global AP User Name.............................. cisco
Global AP Dot1x User Name........................ Not Configured

AP Name             Ethernet MAC       AP Up Time               Association Up Time
-----------------   -----------------  -----------------------  -----------------------
AP_3500E            c4:7d:4f:3a:07:74  0 days, 02 h 38 m 11 s   0 days, 02 h 37 m 00 s
```

350657

Failover for WLCs in HA setup can be categorized into two different sections:

Box Failover

In the case of Box Failover (that is, the Active WLC crashes / system hang / manual reset / force switchover), the direct command is sent from the Active WLC via the Redundant Port as well as from the Redundant Management Interface to the Standby WLC to take over the network. This may take 5-100

msec depending on the number of APs in the network. In the case of power failure on the Active WLC or some crash where the direct command for switchover cannot be sent, it may take 350-500 msec depending on the number of APs in network.

The time it takes for failover in case of power failure on an Active Box also depends on the Keepalive timer configured on the WLC (configured for 100 msec by default). The algorithm it takes to decide the failover is listed here:

- The Standby WLC sends Keepalive to the Active WLC and expects and acknowledgment within 100 msec as per the default timer. This can be configured in range from 100-400 msec.
- If there is no acknowledgment of Keepalive within 100 msec, the Standby WLC immediately sends an ICMP message to the Active WLC via the redundant management interface in order to check if it is a box failover or some issue with Redundant Port connection.
- If there is no response to the ICMP message, the Standby WLC gets aggressive and immediately sends another Keepalive message to the Standby WLC and expects an acknowledgment in 25% less time (that is, 75 msec or 25% less of 100 msec).
- If there is no acknowledgment of Keepalive within 75 msec, the Standby WLC immediately sends another ICMP message to the Active WLC via the redundant management interface.
- Again, if there is no response for the second ICMP message, the Standby WLC gets more aggressive and immediately sends another Keepalive message to the Standby WLC and expects an acknowledgment in time further 25% of actual timer less from last Keepalive timer (that is, 50 msec or last Keepalive timer of 75 msec - 25% less of 100 msec).
- If there is no acknowledgment of the third Keepalive packet within 50 msec, the Standby WLC immediately sends another ICMP message to the Active WLC via the redundant management interface.
- Finally, if there is no response from the third ICMP packet, the Standby WLC declares the Active WLC is dead and assumes the role of the Active WLC.

Network Failover

In the case of a Network Failover (that is, the Active WLC cannot reach its gateway for some reason), it may take 3-4 seconds for a complete switchover depending on the number of APs in the network.

Steps to Simulate Box Failover

Complete these steps:

1. Complete the steps as explained in the configuration section in order to configure HA between two WLCs, and make sure before force switchover is initiated that both the WLCs are paired up as the Active WLC and the Standby WLC.

   For WLC 1:

```
(5508) >show redundancy summary
 Redundancy Mode = SSO ENABLED
     Local State = ACTIVE
      Peer State = STANDBY HOT
            Unit = Primary
         Unit ID = 00:24:97:69:D2:20
Redundancy State = SSO
    Mobility MAC = 00:24:97:69:D2:20

Average Redundancy Peer    Reachability Latency = 486 usecs
Average Management Gateway Reachability Latency = 2043 usecs

Redundancy Management IP Address.................. 9.6.61.21
Peer Redundancy Management IP Address............. 9.6.61.23
Redundancy Port IP Address........................ 169.254.61.21
Peer Redundancy Port IP Address................... 169.254.61.23
Peer Service Port IP Address...................... 10.10.10.11
```

For WLC 2, go to Console connection:

```
(5508-Standby) >show redundancy summary
 Redundancy Mode = SSO ENABLED
     Local State = STANDBY HOT
      Peer State = ACTIVE
            Unit = Secondary - HA SKU
         Unit ID = 00:24:97:69:78:20
Redundancy State = SSO
    Mobility MAC = 00:24:97:69:D2:20

Average Redundancy Peer    Reachability Latency = 506 usecs
Average Management Gateway Reachability Latency = 676 usecs

Redundancy Management IP Address.................. 9.6.61.23
Peer Redundancy Management IP Address............. 9.6.61.21
Redundancy Port IP Address........................ 169.254.61.23
Peer Redundancy Port IP Address................... 169.254.61.21
```

2. Associate an AP to the WLC and check the status of the AP on both the WLCs. In the HA setup, a mirror copy of the AP database is maintained on both the WLCs. That is, APs CAPWAP state in maintained on Active as well as Standby WLC (only for APs which are in Run state) and when switchover is initiated, the Standby WLC takes over the network. In this example, WLC 1 is an Active WLC, WLC 2 is in a Standby state, and the AP database is maintained on both the WLCs.

   WLC 1:

```
(5508) >show ap summary

Number of APs.................................... 1

Global AP User Name.............................. cisco
Global AP Dot1x User Name........................ Not Configured

AP Name             Slots  AP Model             Ethernet MAC       Location         Port  Country  Priority
------------------  -----  -------------------  -----------------  ---------------  ----  -------  --------
AP_3500E            2      AIR-CAP3502E-A-K9    c4:7d:4f:3a:07:74  [redacted]       1     [redacted]     1

(5508) >show ap uptime

Number of APs.................................... 1
Global AP User Name.............................. cisco
Global AP Dot1x User Name........................ Not Configured

AP Name             Ethernet MAC       AP Up Time               Association Up Time
------------------  -----------------  -----------------------  -----------------------
AP_3500E            c4:7d:4f:3a:07:74  0 days, 04 h 27 m 55 s   0 days, 04 h 26 m 44 s
```

350660

WLC 2

```
(5508-Standby) >show ap summary

Number of APs.................................... 1

Global AP User Name.............................. cisco
Global AP Dot1x User Name........................ Not Configured

AP Name             Slots  AP Model             Ethernet MAC       Location         Port  Country  Priority
------------------  -----  -------------------  -----------------  ---------------  ----  -------  --------
AP_3500E            2      AIR-CAP3502E-A-K9    c4:7d:4f:3a:07:74  [redacted]       1     [redacted]     1

(5508-Standby) >show ap uptime

Number of APs.................................... 1
Global AP User Name.............................. cisco
Global AP Dot1x User Name........................ Not Configured

AP Name             Ethernet MAC       AP Up Time               Association Up Time
------------------  -----------------  -----------------------  -----------------------
AP_3500E            c4:7d:4f:3a:07:74  0 days, 04 h 29 m 07 s   0 days, 04 h 27 m 56 s
```

350661

3. Create an open WLAN and associate a client to it. The client database is not synced on the Standby WLC, so the client entry will not be present on the Standby WLC. Once the WLAN is created on the Active WLC, it will also be synced to the Standby WLC via the Redundant Port.

   WLC 1:

```
(5508) >show wlan summary

Number of WLANs.................................. 1

WLAN ID  WLAN Profile Name / SSID                 Status    Interface Name        PMIPv6 Mobility
-------  -------------------------------------  --------  --------------------  ---------------
1        Beta-Test / Beta-Test                  Enabled   management            none

(5508) >show client summary

Number of Clients................................ 1

Number of PMIPV6 Clients......................... 0

MAC Address       AP Name          Status         WLAN/GLAN/RLAN Auth Protocol         Port Wired PMIPV6
----------------- ---------------- -------------- -------------- ---- ---------------- ---- ----- ------

00:40:96:b8:d4:be AP_3500E         Associated     1              Yes  802.11a          1    No    No
```

350662

   WLC 2:

```
(5508-Standby) >show wlan summary

Number of WLANs.................................. 1

WLAN ID  WLAN Profile Name / SSID                 Status    Interface Name        PMIPv6 Mobility
-------  -------------------------------------   --------  --------------------  ---------------
1        Beta-Test / Beta-Test                   Enabled   management            none

(5508-Standby) >show client summary

Number of Clients................................ 0
```

350939

4. Issue the redundancy force-switchover command on the Active WLC. This command will trigger a manual switchover where the Active WLC will reboot and the Standby WLC will take over the network. In this case, the client on the Active WLC will be de-authenticated and join back on the new Active WLC.

   WLC 1:

```
(5508) >redundancy force-switchover

This will reload the active unit and force a switch of activity. Are you sure? (y/N) y


System will now restart!
```

350664

   WLC 2:

```
(5508-Standby) >
HA completed successfully, WLC switch over detection time : 0 msec and  APs switch over time : 1 msec
(5508) >show client summary

Number of Clients................................ 1

Number of PMIPV6 Clients......................... 0

MAC Address       AP Name          Status         WLAN/GLAN/RLAN Auth Protocol         Port Wired PMIPV6
----------------- ---------------- -------------- -------------- ---- ---------------- ---- ----- ------

00:40:96:b8:d4:be AP 3500E         Associated     1              Yes  802.11a          1    No    No
```

350665

Note Observe that the prompt in this example changed from 5508-Standby to 5508. This is because this WLC is now the Active WLC and the time taken for AP switchover is 1 msec.

   WLC 2:

```
(5508) >show ap uptime

Number of APs.................................... 1
Global AP User Name.............................. cisco
Global AP Dot1x User Name........................ Not Configured

AP Name             Ethernet MAC       AP Up Time                Association Up Time
------------------  -----------------  ------------------------  ------------------------
AP_3500E            c4:7d:4f:3a:07:74  0 days, 06 h 13 m 07 s    0 days, 06 h 11 m 56 s
```

350666

   Observe the AP CAPWAP State on WLC 2, which was the Standby WLC initially and is now the Active WLC after switchover. AP Up Time as well as Association Up Time is maintained, and the AP did not go in to the discovery state.

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

Network Issues					
RP Port Status	**Peer Reachable via Redundant Management**	**Gateway Reachable from Active**	**Gateway Reachable from Standby**	**Switchover**	**Results**
Up	Yes	Yes	Yes	No	No Action
Up	Yes	Yes	No	No	Standby will reboot and check for gateway reachability. Will go into maintenance mode if still not reachable.
Up	Yes	No	Yes	Yes	Switchover happens
Up	Yes	No	No	No	No Action
Up	No	Yes	Yes	No	No Action
Up	No	Yes	No	No	Standby will reboot and check for gateway reachability. Will go into maintenance mode if still not reachable.
Up	No	No	Yes	Yes	Switchover happens
Up	No	No	No	No	No Action
Down	Yes	Yes	Yes	No	Standby will reboot and check for gateway reachability. Will go into maintenance mode if still not reachable.
Down	Yes	Yes	No	No	Standby will reboot and check for gateway reachability. Will go into maintenance mode if still not reachable.
Down	Yes	No	Yes	No	Standby will reboot and check for gateway reachability. Will go into maintenance mode if still not reachable.
Down	Yes	No	No	No	Standby will reboot and check for gateway reachability. Will go into maintenance mode if still not reachable.
Down	No	Yes	Yes	Yes	Switchover happens and this may result in Network Conflict
Down	No	Yes	No	No	Standby will reboot and check for gateway reachability. Will go into maintenance mode if still not reachable.

Network Issues					
RP Port Status	**Peer Reachable via Redundant Management**	**Gateway Reachable from Active**	**Gateway Reachable from Standby**	**Switchover**	**Results**
Down	No	No	Yes	Yes	Switchover happens
Down	No	No	No	No	Standby will reboot and check for gateway reachability. Will go into maintenance mode if still not reachable.

System Issues				
Trigger	**RP Port Status**	**Peer Reachable via Redundant Management**	**Switchover**	**Result**
CP Crash	Yes	No	Yes	Switchover happens
DP Crash	Yes	No	Yes	Switchover happens
System Hang	Yes	No	Yes	Switchover happens
Manual Reset	Yes	No	Yes	Switchover happens
Force Switchover	Yes	No	Yes	Switchover happens
CP Crash	No	Yes	Yes	Switchover happens
DP Crash	No	Yes	Yes	Switchover happens
System Hang	No	Yes	Yes	Switchover happens
Manual Reset	No	Yes	Yes	Switchover happens
Force Switchover	No	Yes	Yes	Switchover happens
CP Crash	No	No	Yes	As Updated in Network Issue section

System Issues				
Trigger	**RP Port Status**	**Peer Reachable via Redundant Management**	**Switchover**	**Result**
DP Crash	No	No	Yes	As Updated in Network Issue section
System Hang	No	No	Yes	As Updated in Network Issue section
Manual Reset	No	No	Yes	As Updated in Network Issue section
Force Switchover	No	No	Yes	As Updated in Network Issue section

HA Facts

- HA Pairing is possible only between the same type of hardware and software versions. Mismatch may result in Maintenance Mode. The Virtual IP Address should be the same on both the WLCs before configuring SSO.
- Direct connectivity is recommended between the Active and Standby Redundant Port for 5500/7500/8500 Series of WLCs.
- If none of the management ports are up on the active WLC, a switchover will occur.
- WiSM-2 WLCs should be in same 6500 chassis or can be installed in VSS setup for reliable performance.
- A physical connection between Redundant Port and Infrastructure Network should be done prior to HA configuration.
- The Primary units MAC should be used as Mobility MAC in the HA setup in order to form a mobility peer with another HA setup or independent controller. You also have the flexibility to configure a custom MAC address, which can be used as a Mobility MAC address using the `configure redundancy mobilitymac <custom mac address>` command. Once configured, you should use this MAC address to form a mobility peer instead of using the system MAC address. Once HA is configured, this MAC cannot be changed.
- It is recommended that you use DHCP address assignment for the service port in the HA setup. After HA is enabled, if the static IP is configured for service port, WLC loses the service port IP and it has to be configured again.

- When SSO is enabled, there is no SNMP/GUI access on the service port for both the WLCs in the HA setup.
- Configurations like changing virtual IP address, enabling secureweb mode, configuring web auth proxy, and so forth need a WLC reboot in order to get implemented. In this case, a reboot of the Active WLC will also trigger a simultaneous reboot of the Standby WLC.
- When SSO is disabled on the Active WLC, it will be pushed to the Standby WLC. After reboot, all the ports will come up on the Active WLC and will be disabled on the Standby WLC.
- Keepalive and Peer Discovery timers should be left with default timer values for better performance.
- Clear configuration on the Active WLC will also initiate clear configuration on the Standby WLC.
- Internal DHCP is not supported when SSO is enabled.
- With versions 7.5 and above, AP/Client SSO supports synchronization of L3 MGID between active and standby controllers.
- APs with LSC certificates are supported. The controller's LSC certificate and SCEP configuration must be implemented on the active and standby controllers before activating SSO.

Maintenance Mode

There are few scenarios where the Standby WLC may go into Maintenance Mode and not be able to communicate with the network and peer:

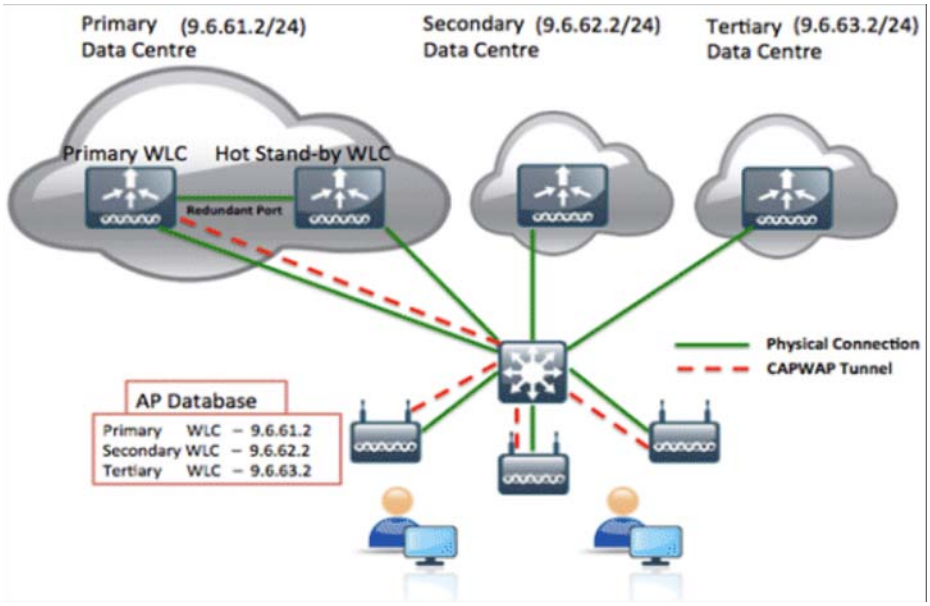
- Non reachability to Gateway via Redundant Management Interface
- WLC with HA SKU which had never discovered peer
- Redundant Port is down
- Software version mismatch (WLC which boots up first goes into active mode and the other WLC in Maintenance Mode)

```
(5508-Standby) >show redundancy summary
 Redundancy Mode = SSO ENABLED
      Local State = NEGOTIATION
       Peer State = DISABLED
             Unit = Secondary - HA SKU
          Unit ID = 00:24:97:69:78:20
Redundancy State = Non Redundant
    Mobility MAC = 00:24:97:69:D2:20

Maintenance Mode = Enabled
Maintenance cause= Negotiation Timeout

Redundancy Management IP Address.............. 9.6.61.23
Peer Redundancy Management IP Address........... 9.6.61.21
Redundancy Port IP Address..................... 169.254.61.23
Peer Redundancy Port IP Address................ 169.254.61.21
```

Note The WLC should be rebooted in order to bring it out of Maintenance Mode. Only the Console and Service Port is active in Maintenance Mode.

SSO Deployment with Legacy Primary/Secondary/Tertiary HA

HA (that is, AP SSO) can be deployed with Secondary and Tertiary Controllers just like today. Both Active and Standby WLCs combined in the HA setup should be configured as primary WLC. Only on failure of both Active and Standby WLCs in the HA setup will the APs fall back to Secondary and further to Tertiary WLCs.



SSO Deployment in Mobility Setup

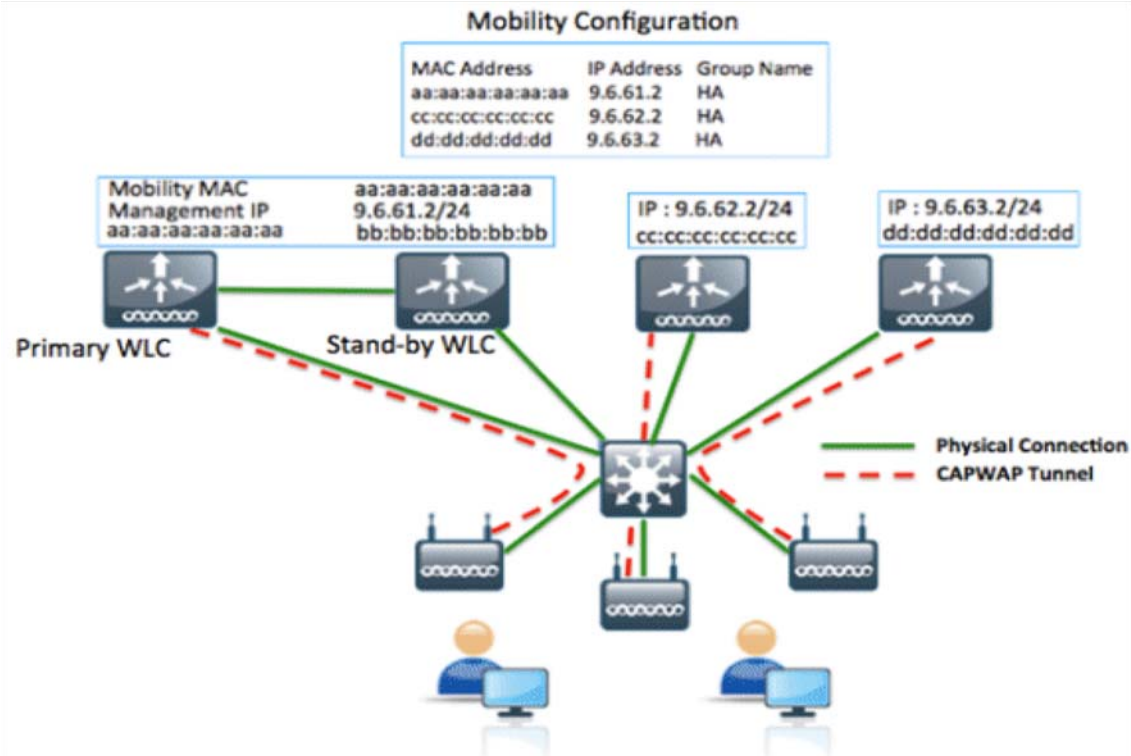
Each WLC has its own unique MAC address, which is used in mobility configuration with an individual controller management IP address. In HA (that is, AP SSO) setup, both the WLCs (Primary and Standby) have their own unique MAC address. In the event of failure of the Primary box and Standby takes over the network if the MAC address of the Primary box is used on another controllers in mobility setup, control path and data path will be down and user has to manually change the MAC to standby MAC address on all the controllers in mobility setup. This is a really cumbersome process as a lot of manual intervention is required.

In order to keep the mobility network stable without any manual intervention and in the event of failure or switchover, the back-and-forth concept of Mobility MAC has been introduced. When the HA pair is set up, by default, the Primary WLC's MAC address is synced as the Mobility MAC address on the Standby WLC which can be seen via the show redundancy summary command on both the controllers.

```
(5508-Standby) >show redundancy summary
 Redundancy Mode = SSO ENABLED
            Unit = Secondary - HA SKU
         Unit ID = 00:24:97:69:78:20
Redundancy State = Non Redundant
    Mobility MAC = 00:24:97:69:D2:20

Redundancy Management IP Address.................. 9.6.61.23
Peer Redundancy Management IP Address............. 9.6.61.21
Redundancy Port IP Address........................ 169.254.61.23
Peer Redundancy Port IP Address................... 169.254.61.21
```

In this output, captured from a Standby controller, the Mobility MAC address can be observed, which is different from the Standbys own MAC address seen as Unit ID. This MAC address is synced from the Active WLC and should be used in mobility configuration. With this implementation, if the Active WLC goes down or even if it is replaced, the Mobility MAC address is still available and active on the Standby WLC. In case the new controller is introduced in the network because of the replacement of the previous Active WLC, it will transition its state as Standby and the same Mobility MAC address is synced again to the new Standby WLC.

You have the flexibility to configure a custom MAC address as Mobility MAC instead of using the default behavior of using the Active WLC MAC address as Mobility MAC. This can be done using the configure redundancy mobilitymac <custom mac address> command on the Active WLC. Once configured, you should use this MAC address on other controllers in order to form a mobility peer instead of using the Active WLC MAC address. This MAC address should be configured before forming the HA pair. Once the HA pair is formed, the Mobility MAC cannot be changed or edited.



In this topology, the Primary and Standby have their own MAC address. With HA pairing, the Active WLC MAC address is synced as a Mobility MAC address, which is the default behavior if a custom MAC is not configured before HA pairing. Once the Active WLC MAC address is synced as the Mobility MAC address, the same MAC is used in mobility configuration on all the controllers in the mobility setup.

Licensing for HA Pair

A HA Pair can be established between two WLCs running in these combinations:

- One WLC has a valid AP Count license and the other WLC has a HA SKU UDI
- Both the WLCs have a valid AP Count license
- One WLC has an Evaluation license and the other WLC has a HA SKU UDI or Permanent license

One WLC has a valid AP Count license and the other WLC has a HA SKU UDI

- HA SKU is a new SKU with a Zero AP Count License.
- The device with HA SKU becomes Standby the first time it pairs up.
- AP-count license info will be pushed from Active to Standby.
- On event of Active failure, HA SKU will let APs join with AP-count obtained and will start 90-day countdown. The granularity of this is in days.
- After 90-days, it starts nagging messages. It will not disconnect connected APs.
- With new WLC coming up, HA SKU at the time of paring will get the AP Count:
  - If the new WLC has a higher AP count than the previous, the 90-day counter is reset.
  - If the new WLC has a lower AP count than the previous, the 90-day counter is not reset.
  - In order to lower AP count after switchover, the WLC offset timer will continue and nagging messages will be displayed after time expiry.
  - Elapsed time and AP-count will be remembered on reboot.
  - The factory default HA-SKU controller should not allow any APs to join.

Both the WLCs have a valid AP Count license

- The CLI should be used to configure one WLC as the Standby WLC (as mentioned in the configuration section) provided it satisfies the requirement of minimum permanent license count. This condition is only valid for the 5500 WLC, where a minimum of 50 AP Permanent licenses are needed to be converted to Standby. There is no restriction for other WLCs such as the WiSM2, 7500, and 8500.
- AP-count license information will be pushed from Active to Standby.
- In the event of a switchover, the new Active WLC will operate with the license count of the previous Active WLC and will start the 90-day countdown.
- The WLC configured as Secondary will not use its own installed license, and only the inherited license from the active will be utilized.
- After 90-days, it starts nagging messages. It will not disconnect connected APs.

- With the new WLC coming up, HA SKU at the time of paring will get the AP Count:
  - If the new WLC has a higher AP count than the previous, the 90-day counter is reset.
  - If the new WLC has a lower AP count than the previous, the 90-day counter is not reset.
  - After switchover to a lower AP count, the WLC offset timer will continue and nagging messages will be displayed after time expiry.

One WLC has an Evaluation license and the other WLC has a HA SKU UDI or Permanent license

- The device with HA SKU becomes the Standby WLC the first time it pairs up with an existing Active WLC running Evaluation License. Or, any WLC running a permanent license count can be configured as the Secondary unit using the CLI configuration provided if it satisfies the requirement of minimum permanent license count. This condition is only valid for the 5500 WLC, where a minimum of 50 AP Permanent licenses are needed to be converted to Standby. There is no restriction for other WLCs such as the WiSM2, 7500, and 8500.
- AP-count license information will be pushed from Active to Standby.
- In the event of a switchover, the new Active WLC will operate with the license count of the previous Active WLC and start the 90-day countdown.
- After 90-days, it starts nagging messages. It will not disconnect connected APs.
- With new the WLC coming up, HA SKU at the time of paring will get the AP Count:
  - If the new WLC has a higher AP count than the previous, the 90-day counter is reset.
  - If the new WLC has a lower AP count than the previous, the 90-day counter is not reset.
  - After switchover to a lower AP count, the WLC offset timer will continue and nagging messages will be displayed after time expiry.

High Availability in Release 7.5

To support High Availability without impacting service, there needs to be support for seamless transition of clients and APs from the active controller to the standby controller. Release 7.5 supports Client Stateful Switch Over (Client SSO) in Wireless LAN controllers. Client SSO will be 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 WLC when the client associates to the WLC or the client’s parameters change. Fully authenticated clients, i.e. the ones in Run state, are synced to the Standby and thus, client re-association is avoided on switchover making the failover seamless for the APs as well as for the clients, resulting in zero client service downtime and no SSID outage.

Redundancy Port Connectivity in 7.5

- In controller release 7.3 and 7.4, back-to-back connectivity through redundancy port restrains the active and standby controllers to be in different locations. There are two mandatory interfaces for redundancy, redundancy port and redundancy management interface. Redundancy port uses dedicated physical port **eth1** (similar to service port). It is used for all redundancy communication

(AP, Client data, configuration sync, keep-alive messages and role negotiation messages). Redundancy management interface is used to check for the reachability of the peer and management gateway.

- To support the active and standby WLCs in different data centers, in release 7.5, back-to-back redundancy port connectivity between peers is no longer mandatory and the redundancy ports can be connected via switches such that there is L2 adjacency between the two controllers.
- Backward compatibility for release 7.3/7.4 will be supported, wherein back-to-back redundancy port connectivity is used for redundancy communication between the WLCs and the redundancy management interface is used to check the reachability to the peer and to management gateway.
- No additional configuration change is required for redundancy port and the configuration remains the same as in 7.3/7.4 release.

Supported HA Topologies

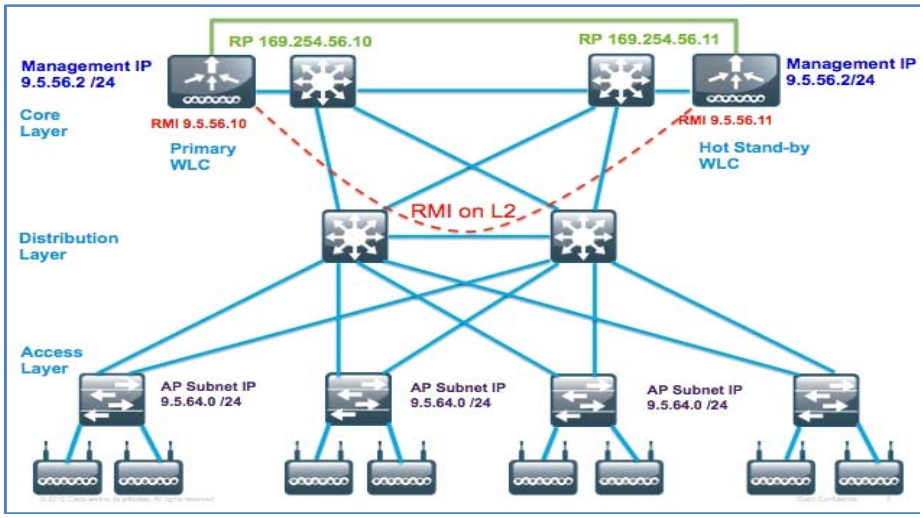
Supported HA Topologies in Release 7.5

5500/7500/8500 Series Controllers

1. Back-to-back Redundancy Port (RP) connectivity between the two WLCs, Redundancy Management Interface (RMI) connectivity to check peer and management gateway reachability.
2. RP connectivity with L2 adjacency between the two WLCs, RMI connectivity to check peer and management gateway reachability. This can be within the same or different data centers.
3. Two 5508, 7500 or 8500 connected to a VSS pair. Primary WLC connected to one 6500 and the Stand-by WLC to the other 6500.

Back-to-back RP Connectivity

Figure 1 Back-to-back RP connectivity



- This is the same topology as was supported in controller release 7.3.
- Configuration Sync and Keepalive messages are sent via Redundancy Port.
- RMI interface is created as part of Management subnet and is used to check peer and management gateway reachability.
- RTT Latency is 80 milliseconds by default. The RTT should be 80% of the Keepalive timer which is configurable in the range 100-400 milliseconds.
- Failure detection time is 3*100 + 60 + jitter (12 msec) = ~400 msec

Note In the above equation, 3 is the Keepalive retry count, 100 is the Keepalive timer, and 60 is 3*10 + 3*10 (3 RMI pings to peer + 3 pings to gateway).

- Bandwidth: 60 Mbps or more
- MTU: 1500

Configuration on Primary WLC:

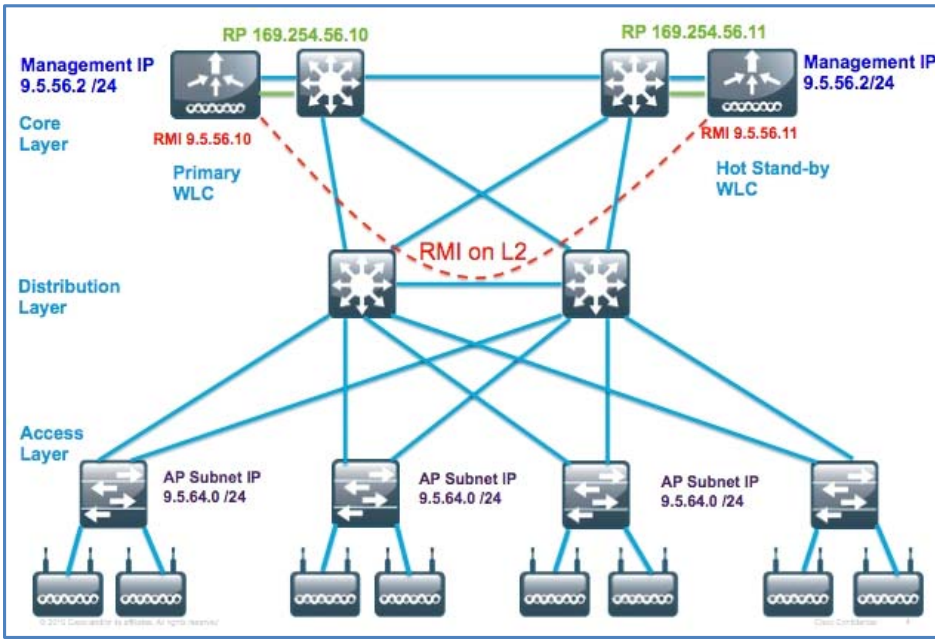
```
configure interface address management 9.5.56.2 255.255.255.0 9.5.56.1
configure interface address redundancy-management 9.5.56.10 peer-redundancy-management
9.5.56.11
configure redundancy unit primary
configure redundancy mode sso
```

Configuration on Hot Standby WLC:

```
configure interface address management 9.5.56.3 255.255.255.0 9.5.56.1
configure interface address redundancy-management 9.5.56.11 peer-redundancy-management
9.5.56.10
configure redundancy unit secondary
configure redundancy mode sso
```

RP Connectivity via Switches

Figure 2 RP connectivity via switches



- Redundancy Port connectivity via switches across data centers is supported in this topology.
- Configuration sync and Keepalives via Redundancy Port.
- RMI interface is created as part of Management subnet and is used to check peer and management gateway reachability.
- RTT Latency is 80 milliseconds by default. The RTT should be 80% of the Keepalive timer which is configurable in the range 100-400 milliseconds.
- Failure detection time is 3*100 + 60 + jitter (12 msec) = ~400 msec
- Bandwidth: 60 Mbps or more
- MTU: 1500

Configuration on Primary WLC

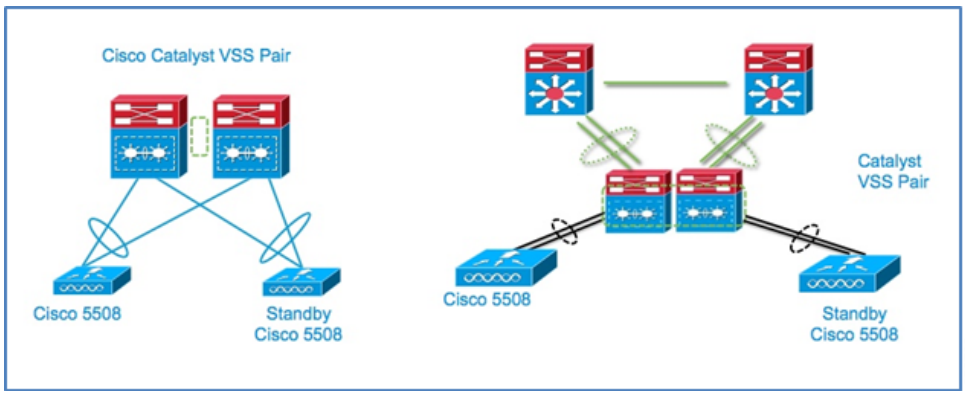
```
configure interface address management 9.5.56.2 255.255.255.0 9.5.56.1
configure interface address redundancy-management 9.5.56.10 peer-redundancy-management
9.5.56.11
configure redundancy unit primary
configure redundancy mode sso
```

Configuration on Hot Standby WLC

```
configure interface address management 9.5.56.3 255.255.255.0 9.5.56.1
configure interface address redundancy-management 9.5.56.11 peer-redundancy-management
9.5.56.10
configure redundancy unit secondary
configure redundancy mode sso
```

5508, 7500 or 8500 Connected to VSS Pair

Figure 3 WLCs connected to VSS Pair



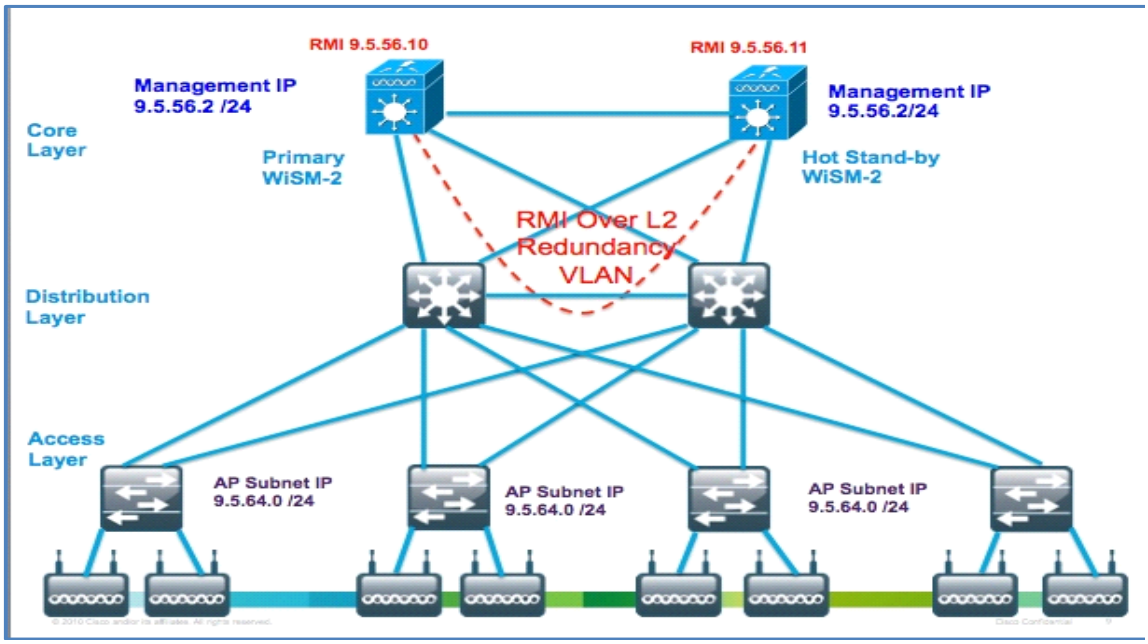
Supported HA Topologies for WiSM2 Controllers

WiSM2 in the Same Chassis

Figure 4 WiSM2 in Single Chassis

WiSM2 in Different Chassis: Redundancy VLAN over L2 Network

Figure 5 WiSM2 connectivity using Redundancy VLAN over L2 network



Configuration on Cat6k for WiSM2

```
wism service-vlan 192 ( service port VLAN )
wism redundancy-vlan 169 ( redundancy port VLAN )
wism module 6 controller 1 allowed-vlan 24-38 ( data VLAN )
```

WiSM2 HA configuration remains the same.

WiSM2 in Different Chassis: VSS Pair

Figure 6 WiSM2 connectivity using VSS Pair

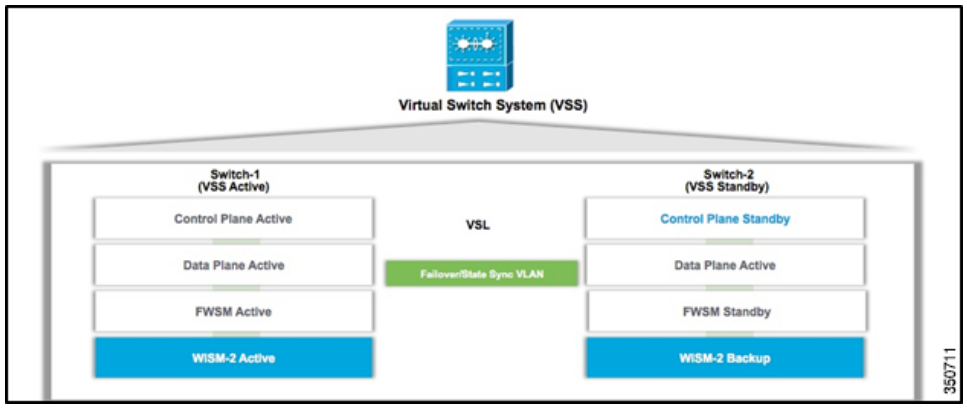


Figure 7 Active and Standby VSS Pair connected via VSL Link

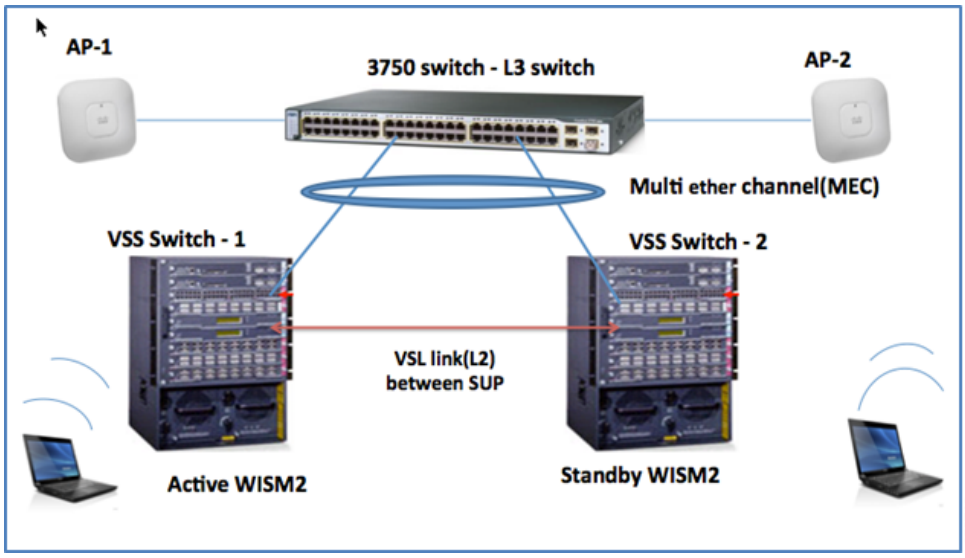
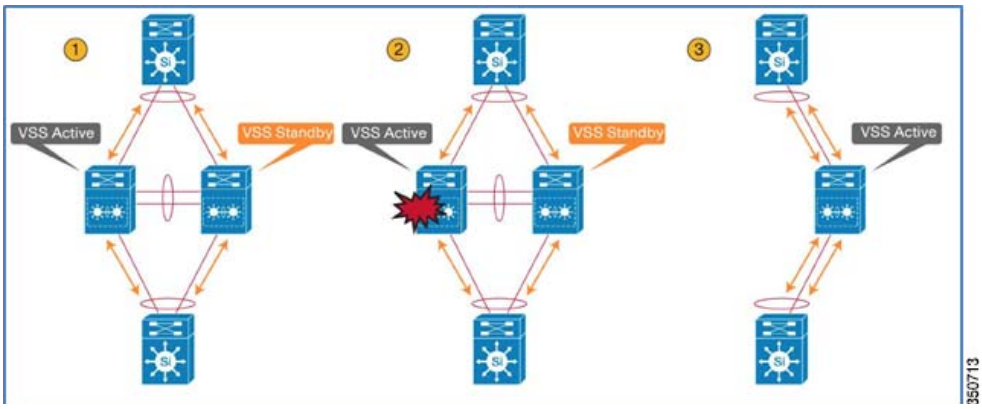


Figure 8 WiSM2 connectivity using VSS Pair



VSS Configuration

	Command	Purpose
Step 1	`Switch-1(config)#redundancy`	Enters redundancy configuration mode.
Step 2	`Switch-1(config-red)# mode sso`	Configures SSO. When this command is entered, the redundant supervisor engine is reloaded and begins to work in SSO mode.
Step 3	`Switch-1(config-red)# exit`	Exits redundancy configuration mode.
Step 4	`Switch-1(config)# router` *routing_protocol processID*	Enables routing, which places the router in router configuration mode.
Step 5	`Switch-1(config-router)#nsf`	Enables NSF operations for the routing protocol.
Step 6	`Switch-1(config-router)#end`	Exits to privileged EXEC mode.
Step 7	`Switch-1# show running-config`	Verifies that SSO and NSF are configured and enabled.
Step 8	`Switch-1# show redundancy states`	Displays the operating redundancy mode.

	Command	Purpose
Step 1	`Switch-1(config)# switch virtual domain 100`	Configures the virtual switch domain on Chassis A.
Step 2	`Switch-1(config-vs-domain)# switch 1`	Configures Chassis A as virtual switch number 1. For Chassis B config - Switch 2
Step 3	`Switch-1(config-vs-domain)# exit`	Exits config-vs-domain.

350714

Command	Purpose	
Step 1	`Switch-1(config)# interface port-channel 10`	Configures port channel 10 on Switch 1.
Step 2	`Switch-1(config-if)# switch virtual link 1`	Associates Switch 1 as owner of port channel 10.
Step 3	`Switch-1(config-if)# no shutdown`	Activates the port channel.
Step 4	`Switch-1(config-if)# exit`	Exits interface configuration.

	Command	Purpose
Step 1	`Switch-2(config)# interface port-channel 20`	Configures port channel 20 on Switch 2.
Step 2	`Switch-2(config-if)# switch virtual link 2`	Associates Switch 2 as owner of port channel 20.
Step 3	`Switch-2(config-if)# no shutdown`	Activates the port channel.
Step 4	`Switch-2(config-if)# exit`	Exits interface configuration mode.

Command	Purpose
`Switch-1# switch convert mode virtual`	Converts Switch 1 to virtual switch mode. After you enter the command, you are prompted to confirm the action. Enter **yes**. The system creates a converted configuration file, and saves the file to the RP bootflash.

350715

Recommendations

- Round trip latency on Redundancy Link should be less than or equal to 80 milliseconds.
- Preferred MTU on Redundancy Link is 1500 or above.
- Bandwidth on Redundancy Link should be 60 Mbps or more.
- If redundancy ports are connected via switches such that there is L2 adjacency between the two controllers, the RP VLAN should be excluded from the access VLAN configured on the switch for the management ports.
- For WiSM2 connectivity between two different chassis connected across the L2 network, the “redundancy-vlan” should be excluded from the access-VLAN configured on the switch for the management ports.
- It is highly recommended to use different sets of switches for the RP port connectivity and the management port traffic to avoid an Active-Active scenario.
- When deploying WiSM2 in VSS setup, it is recommended to set the peer search time to 180 seconds.

Client SSO (Client Stateful Switchover)

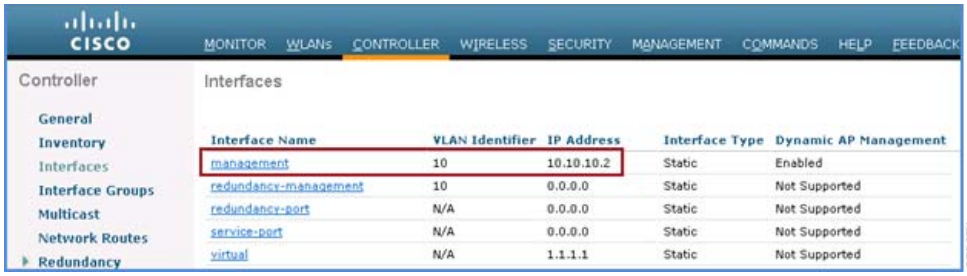
To support High Availability without impacting the service, there needs to be support for seamless transition of the clients and APs from the active controller to the standby controller. Release 7.5 supports Client Stateful Switch Over (Client SSO) in Wireless LAN controllers. Client SSO will be supported for clients, which have already completed the authentication and DHCP phase and have started passing traffic. With Client SSO, the client's information is synced to the Standby WLC when client associates or the client parameters change. Fully authenticated clients, i.e. ones in Run state, are synced to the Standby and thus, client re-association is avoided on switchover making the failover seamless for the AP as well as for the client.

- Client SSO will work with Anchor-Foreign mobility setup as well as Guest Anchor scenarios.
- L3 MGIDs are synced to the Standby Controller.
- The failover time varies from ~2-996 milliseconds depending on the category of box failover.
- The management gateway failover time is in the order of ~15 seconds, which is the time taken for 12 pings to the management gateway.
- The default RTT latency between the two WLCs is 80 milliseconds. RTT latency should be less than or equal to 80% of the Keepalive timer. The Keepalive timer is configurable in the range 100-400 milliseconds

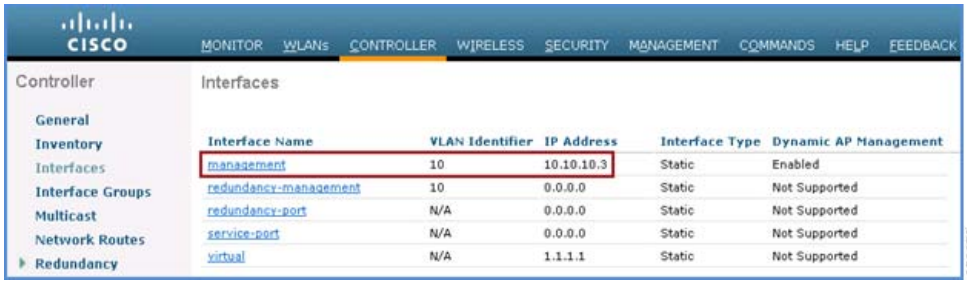
Configuration

1. Before configuring HA it is mandatory to have both the controllers' management interface in same subnet.

   WLC 1:



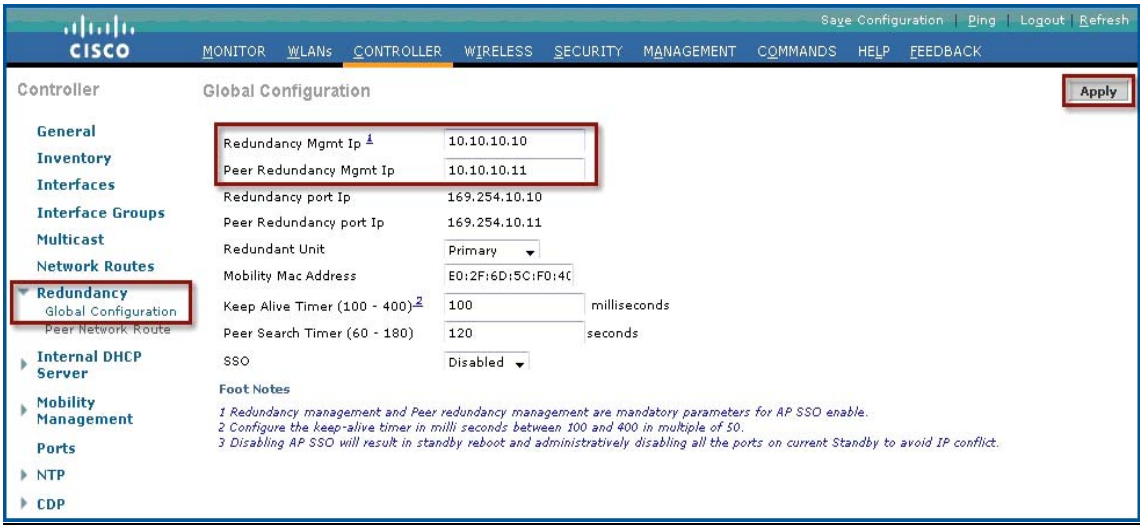
   WLC 2:



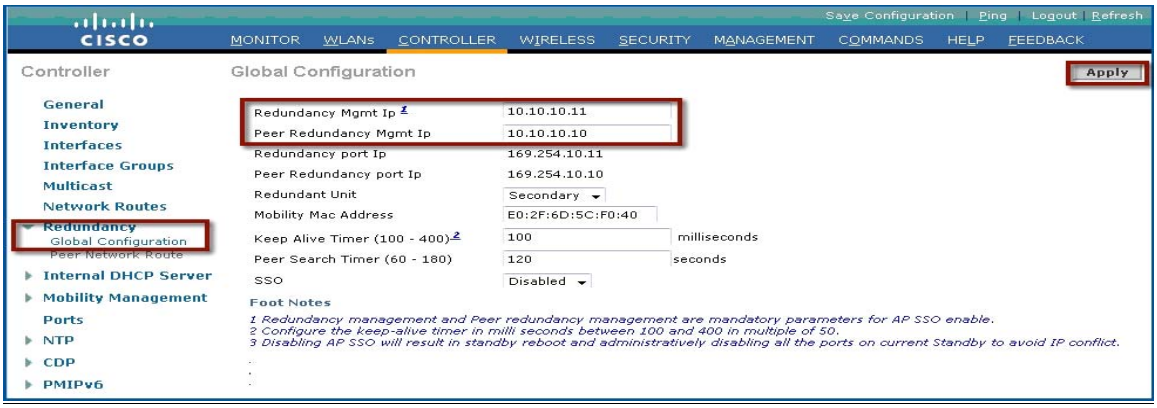
2. HA is disabled by default. Before enabling HA it is mandatory to configure Redundant Management IP address and Peer Redundant Management IP address. Both the interfaces should be in same subnet as Management Interface.

To configure Redundant Management and Peer Redundant Management IP address click **Controller tab > Redundancy > Global Configuration** and enter IP address in both the fields and then click **Apply.**

WLC 1:

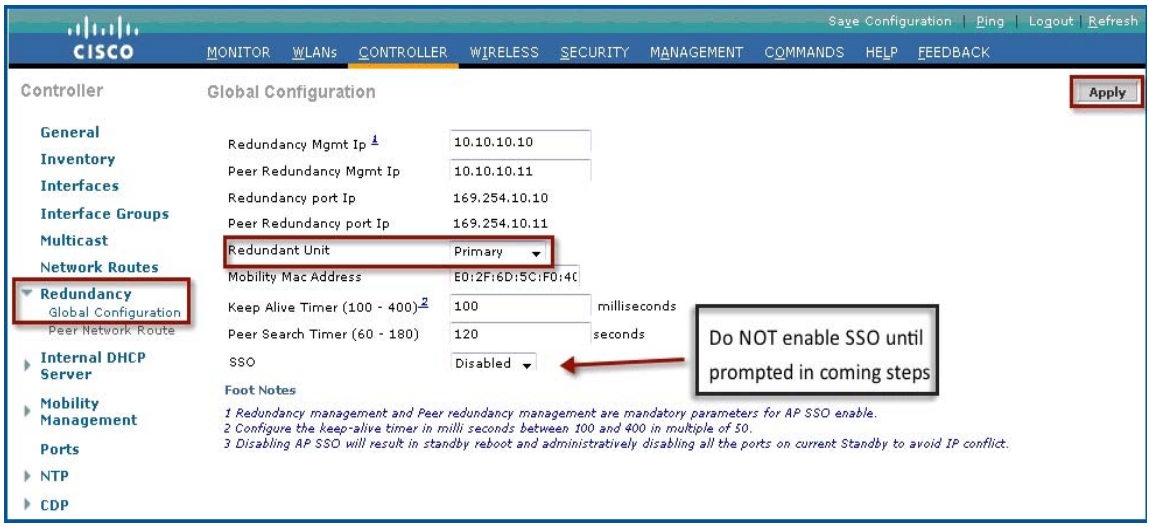


WLC 2:

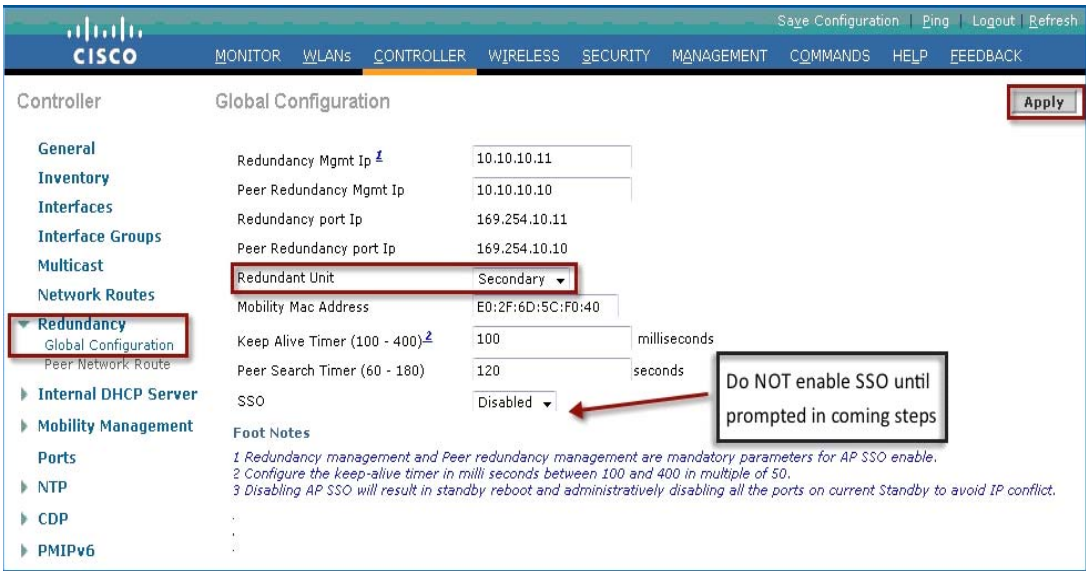


3. Now configure one controller as **Primary** and another controller as **Secondary** from Redundant Unit drop-down. In an example below WLC 1 is configured as **Primary Unit** and WLC 2 is configured as **Secondary Unit (will work as HA SKU UDI)**. While pairing, the controller that is configured as Primary will push its AP Count License to Standby WLC. To configure one controller as Primary unit and second controller as Secondary unit, click **Controller tab > Redundancy > Global Configuration** and select Primary/Secondary from Redundant Unit drop-down list and then click **Apply**.

WLC 1:



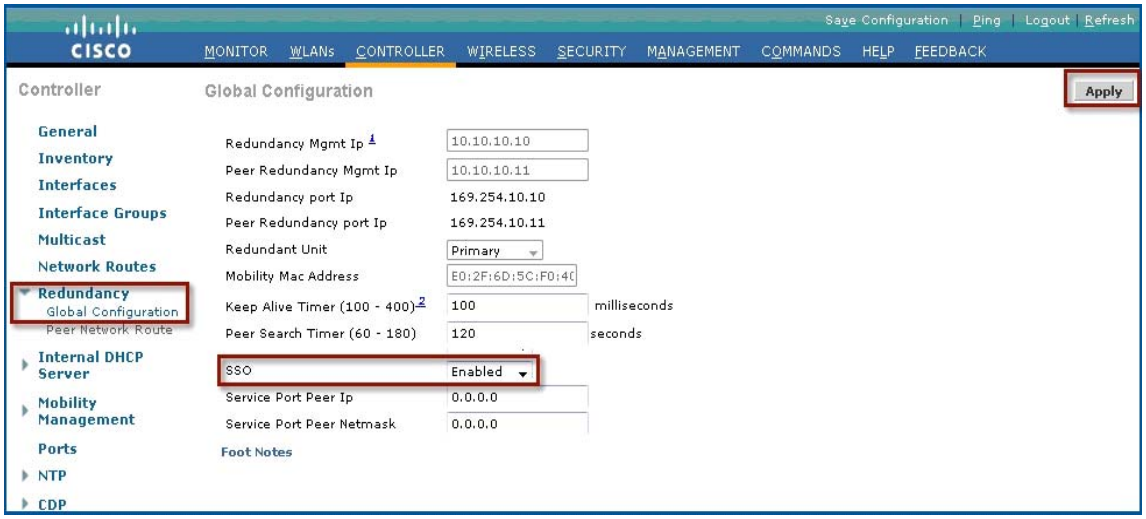
WLC 2:



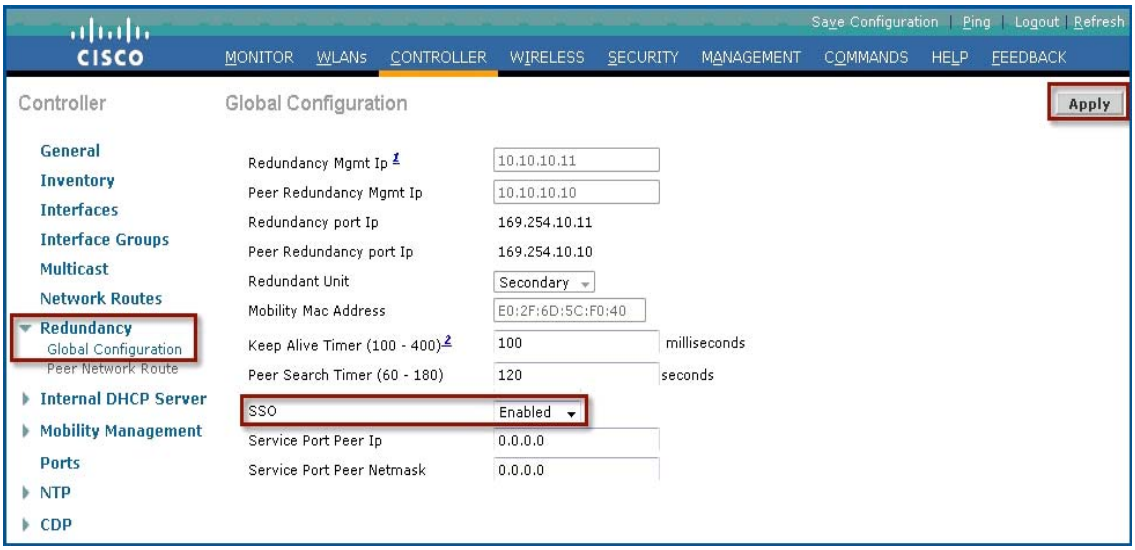
4. After controllers are configured with Redundant Management, Peer Redundant Management IP address and Redundant Units are configured, it is very important to make sure physical connection are up between both the controllers i.e. both the WLCs are connected via Redundant Port using Ethernet cable and uplink is also connected to infrastructure switch and gateway is reachable from both the WLCs. Initiate **ping** to management interface gateway IP Address from both the controllers and make sure reachability to management gateway is fine.

5. To enable SSO navigate to **Controller >Redundancy > Global Configuration** and select the **Enable** option from **SSO** drop-down list on both the WLCs and click **Apply**. This step will make controllers reboot.

WLC 1:



WLC 2:



6. Enabling SSO will reboot controllers to negotiate HA role as per configuration and once the role is determined, configuration is synced from Active to Standby WLC via the redundant port. Initially controller configured as Secondary will report XML mismatch after downloading the configuration from Active and reboot again. In next reboot after role determination it will validate the configuration again and will report no XML mismatch and will process further to establish itself as Standby WLC. Thus, controller configured as Primary will reboot once and controller configured as Secondary will reboot twice.

   WLC 1:

```
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...
ok
Starting LWAPP: ok
Starting CAPWAP: ok
Starting LOCP: ok
Starting Security Services: ok
```

350679

WLC 2 on first reboot after enabling SSO:

```
Starting VPN Services: ok
Starting DNS Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...

Standby started downloading configurations from Active...

Standby comparing its own configurations with the configurations downloaded from Active...


Startup XMLs are different, reboot required
Restarting system. Reason: rsyncmgrXferTrasport ..
Restarting system.
```

350680

WLC 2 on second reboot after downloading XML configuration from Active:

```
Starting VPN Services: ok
Starting DNS Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...
Standby started downloading configurations from Active...

Standby comparing its own configurations with the configurations downloaded from Active...


Startup XMLs are same, no reboot required
Standby continue...
ok
Starting LWAPP: ok
Starting CAPWAP: ok
```

350681

While WLC2 is booting up, no configuration change is allowed on WLC1:

```
(POD1-WLC) >
Blocked: Configurations blocked as standby WLC is still booting up.
         You will be notified once configurations are Unblocked

Unblocked: Configurations are allowed now...
```

350682

7. After SSO is enabled followed by controller reboots and XML configuration is synced, WLC 1 will transition its state as **Active** and WLC 2 will transition its state as **Standby HOT**. From this point onwards GUI/Telnet/SSH for WLC 2 on management interface will not work, as all the configurations should be done from the Active controller. Standby controller i.e. WLC 2 in this case if required can only be managed via Console or Service Port.

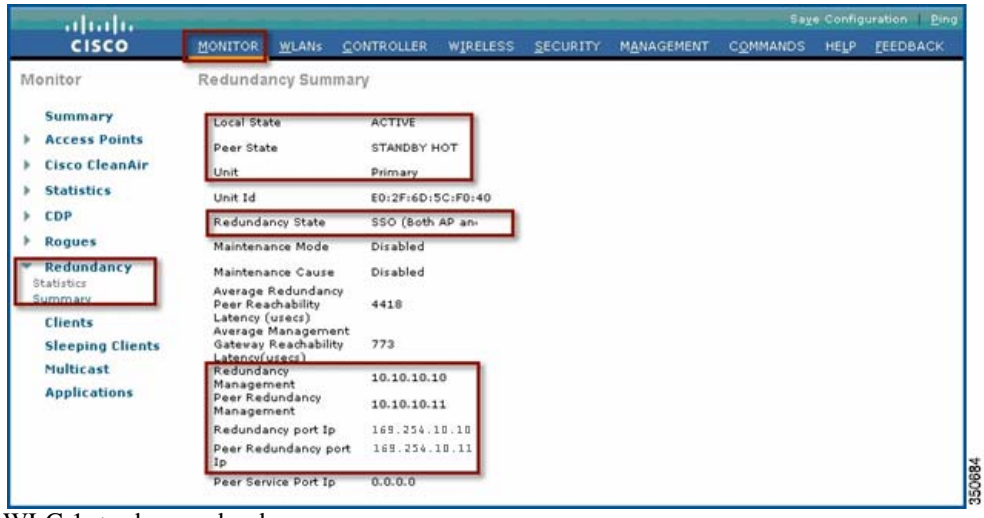
   Also once Peer WLC transitions to **Standby Hot** state, **-Standby** keyword is automatically appended to Standby WLC's prompt name.

```
User: admin
Password:********
(POD1-WLC-Standby) >
```

350683

8. To check the redundancy status

   WLC 1 -> Click **Monitor > Redundancy > Summary:**



WLC 1 -> show redundancy summary:

```
(POD1-WLC) >show redundancy summary
            Redundancy Mode = SSO ENABLED
                Local State = ACTIVE
                 Peer State = STANDBY HOT
                       Unit = Primary
                    Unit ID = E0:2F:6D:5C:F0:40
          Redundancy State = SSO (Both AP and Client SSO)
              Mobility MAC = E0:2F:6D:5C:F0:40
Management Gateway Failover = ENABLED (Management GW failover would be operational in few moments)
           Link Encryption = DISABLED

Redundancy Management IP Address.................. 10.10.10.10
Peer Redundancy Management IP Address............. 10.10.10.11
Redundancy Port IP Address........................ 169.254.10.10
Peer Redundancy Port IP Address................... 169.254.10.11
Peer Service Port IP Address...................... 0.0.0.0
```

350685

WLC 2 -> show redundancy summary:

```
(POD1-WLC-Standby) >show redundancy summary
            Redundancy Mode = SSO ENABLED
                Local State = STANDBY HOT
                 Peer State = ACTIVE
                       Unit = Secondary - HA SKU (Inherited AP License Count = 62)
                    Unit ID = E0:2F:6D:5C:EE:A0
          Redundancy State = SSO (Both AP and Client SSO)
              Mobility MAC = E0:2F:6D:5C:F0:40

Average Redundancy Peer Reachability Latency = 1452 usecs
Average Management Gateway Reachability Latency = 750 usecs

Redundancy Management IP Address.................. 10.10.10.11
Peer Redundancy Management IP Address............. 10.10.10.10
Redundancy Port IP Address........................ 169.254.10.11
Peer Redundancy Port IP Address................... 169.254.10.10
```

350686

AP And Client State Sync

1. At this stage both the controllers are paired up in HA setup. Any configuration done on Active will be synced to Standby controller via redundant port. Check the WLAN summary and Interface summary on standby WLC from console connection.
2. In High Availability setup, APs' CAPWAP state in maintained on Active as well as Standby controller (only for APs which are in Run state) i.e. UP time and Associated UP time is synced from the active to the standby controller. In an example below WLC 1 is an Active state and serving the network and WLC 2 is in Standby state monitoring active controller. Although WLC 2 is in standby state it still maintains CAPWAP state of AP.

   WLC 1->Console Connection:

```
(POD1-WLC) >show ap uptime

Number of APs.................................... 2
Global AP User Name.............................. Not Configured
Global AP Dot1x User Name........................ Not Configured

AP Name             Ethernet MAC       AP Up Time              Association Up Time
-----------------   ----------------   ---------------------   ---------------------
POD1-AP1            6c:20:56:e1:50:09  0 days, 03 h 45 m 58 s  0 days, 00 h 24 m 11 s
POD1-AP2            44:d3:ca:42:31:57  0 days, 15 h 46 m 37 s  0 days, 00 h 24 m 07 s
```


   Observe the AP UP Time and Association UP Time on Active WLC

   WLC 2->Console Connection:

```
(POD1-WLC-Standby) >show ap uptime

Number of APs.................................... 2
Global AP User Name.............................. Not Configured
Global AP Dot1x User Name........................ Not Configured

AP Name             Ethernet MAC       AP Up Time              Association Up Time
-----------------   ----------------   ---------------------   ---------------------
POD1-AP1            6c:20:56:e1:50:09  0 days, 03 h 46 m 11 s  0 days, 00 h 24 m 24 s
POD1-AP2            44:d3:ca:42:31:57  0 days, 15 h 46 m 50 s  0 days, 00 h 24 m 20 s
```


   Observe the AP Uptime and Association UP Time on Standby WLC will be in sync with active WLC.
3. In case of Box Failover i.e. Active controller crashes / system hang / manual reset / force switchover direct command is sent from Active controller via Redundant Port as well as from Redundant Management Interface to Standby controller to take over the network. Failover may take ~2-360 millisecond depending on number of APs/Clients on the active controller. In case of power failure on Active WLC or some crash where direct command for switchover cannot be sent to the standby controller, it may take ~360 – 990 msec depending upon number of APs/Clients on the active controller and the Keepalive timer configured. The default Keepalive timer is 100 milliseconds. Make sure that default RTT latency is less than or equal to 80 msec.
4. With release 7.5 as part of Client SSO, the client database is also synced to standby WLC so Run state client entries will be present on Standby WLC.

   WLC 1-> Console/Telnet/SSH Connection:

```
(POD1-WLC) >show client summary

Number of Clients................................ 2

Number of PMIPV6 Clients......................... 0

                                                 GLAN/
                                                 RLAN/
MAC Address       AP Name           Slot Status       WLAN  Auth Protocol         Port Wired PMIPV6 Role
----------------- ----------------- ---- ------------ ----- ---- ---------------- ---- ----- ------ ----------
24:77:03:11:59:38 POD1-AP1           1   Associated     1    Yes  802.11n(5 GHz)   1    No    No     Local
28:e7:cf:ec:e9:50 POD1-AP2           1   Associated     2    Yes  802.11n(5 GHz)   1    No    No     Local
```

350689

```
(POD1-WLC) >show client detail 28:e7:cf:ec:e9:50
Client MAC Address.............................. 28:e7:cf:ec:e9:50
Client Username ................................ N/A
AP MAC Address.................................. 64:d9:89:42:34:70
AP Name......................................... POD1-AP2
AP radio slot Id................................ 1
Client State.................................... Associated
Client NAC OOB State............................ Access
Wireless LAN Id................................. 2
Hotspot (802.11u)............................... Not Supported
BSSID........................................... 64:d9:89:42:34:7e
Connected For .................................. 252 secs
Channel......................................... 149
IP Address...................................... 10.10.11.76
Gateway Address................................. 10.10.11.1
Netmask......................................... 255.255.255.0
IPv6 Address.................................... fe80::2ae7:cfff:feec:e950
Association Id.................................. 1
Authentication Algorithm........................ Open System
Reason Code..................................... 1
Status Code..................................... 0
Session Timeout................................. 1800
Client CCX version.............................. No CCX support
```

350690

Client entry is present on Active WLC.

WLC2-> Console Connection:

```
(POD1-WLC-Standby) >show client summary

Number of Clients................................ 2

Number of PMIPV6 Clients......................... 0

                                                 GLAN/
                                                 RLAN/
MAC Address       AP Name           Slot Status       WLAN  Auth Protocol         Port Wired PMIPV6 Role
----------------- ----------------- ---- ------------ ----- ---- ---------------- ---- ----- ------ ----------
24:77:03:11:59:38 POD1-AP1           1   Associated     1    Yes  802.11n(5 GHz)   1    No    No     Local
28:e7:cf:ec:e9:50 POD1-AP2           1   Associated     2    Yes  802.11n(5 GHz)   1    No    No     Local
```

350691

```
(POD1-WLC-Standby) >show client detail 28:e7:cf:ec:e9:50
Client MAC Address.............................. 28:e7:cf:ec:e9:50
Client Username ................................ N/A
AP MAC Address.................................. 64:d9:89:42:34:70
AP Name......................................... POD1-AP2
AP radio slot Id................................ 1
Client State.................................... Associated
Client NAC OOB State............................ Access
Wireless LAN Id................................. 2
Hotspot (802.11u)............................... Not Supported
BSSID........................................... 64:d9:89:42:34:7e
Connected For .................................. 262 secs
Channel......................................... 149
IP Address...................................... 10.10.11.76
Gateway Address................................. 10.10.11.1
Netmask......................................... 255.255.255.0
IPv6 Address.................................... fe80::2ae7:cfff:feec:e950
Association Id.................................. 1
Authentication Algorithm........................ Open System
Reason Code..................................... 1
Status Code..................................... 0
Session Timeout................................. 1800
Client CCX version.............................. No CCX support
```

350692

Client entry is present on Standby WLC.

5. PMK cache is also synced between the two controllers

   WLC 1:

```
(POD1-WLC) >show pmk-cache all

Number of PMK Cache Entries: 2

PMK-CCKM Cache

                          Entry
Type        Station       Lifetime   VLAN Override        IP Override          Audit-Session-ID
------  ---------------   --------   ------------------   ---------------      ----------------
RSN     28:e7:cf:ec:e9:50  83725                          0.0.0.0
RSN     70:de:e2:0e:ce:05  83725                          0.0.0.0
```

   WLC 2:

```
(POD1-WLC-Standby) >show pmk-cache all
Number of PMK Cache Entries: 2

PMK-CCKM Cache

                          Entry
Type        Station       Lifetime   VLAN Override        IP Override          Audit-Session-ID
------  ---------------   --------   ------------------   ---------------      ----------------
RSN     28:e7:cf:ec:e9:50  83725                          0.0.0.0
RSN     70:de:e2:0e:ce:05  83725                          0.0.0.0
```

350694

Failover Process

1. Issue a command **redundancy force-switchover** on Active controller. This command will trigger manual switchover where Active controller will reboot and Standby controller will take over the network. In this case Run state client on Active WLC will not be de-authenticated. The command **save config** is initiated before **redundancy force-switchover** command.

   WLC 1-> Console Connection:

```
(POD1-WLC) >redundancy force-switchover

Warning: Saving configuration change causes all the configurations to be saved on Flash.
If this is not what you intend to do, do not type 'y' below.

The system has unsaved changes.
Would you like to save them now? (y/N) y


Configuration Saved!Restarting system.
```

350695

   WLC 2-> Console Connection:

```
(POD1-WLC-Standby) >
HA completed successfully, WLC switch over detection time : 2 msec and APs switch over time : 0 msec

(POD1-WLC) >show client detail 28:e7:cf:ec:e9:50
Client MAC Address.............................. 28:e7:cf:ec:e9:50
Client Username ................................ N/A
AP MAC Address.................................. 64:d9:89:42:34:70
AP Name......................................... POD1-AP2
AP radio slot Id................................ 1
Client State.................................... Associated
Client NAC OOB State............................ Access
Wireless LAN Id................................. 2
Hotspot (802.11u)............................... Not Supported
BSSID........................................... 64:d9:89:42:34:7e
Connected For .................................. 284 secs
Channel......................................... 149
IP Address...................................... 10.10.11.76
Gateway Address................................. 10.10.11.1
Netmask......................................... 255.255.255.0
IPv6 Address.................................... fe80::2ae7:cfff:feec:e950
Association Id.................................. 1
Authentication Algorithm........................ Open System
Reason Code..................................... 1
Status Code..................................... 0
Session Timeout................................. 1800
Client CCX version.............................. No CCX support
```

350696

   Observe the change in prompt in above screen capture.

   WLC 2->Console Connection:

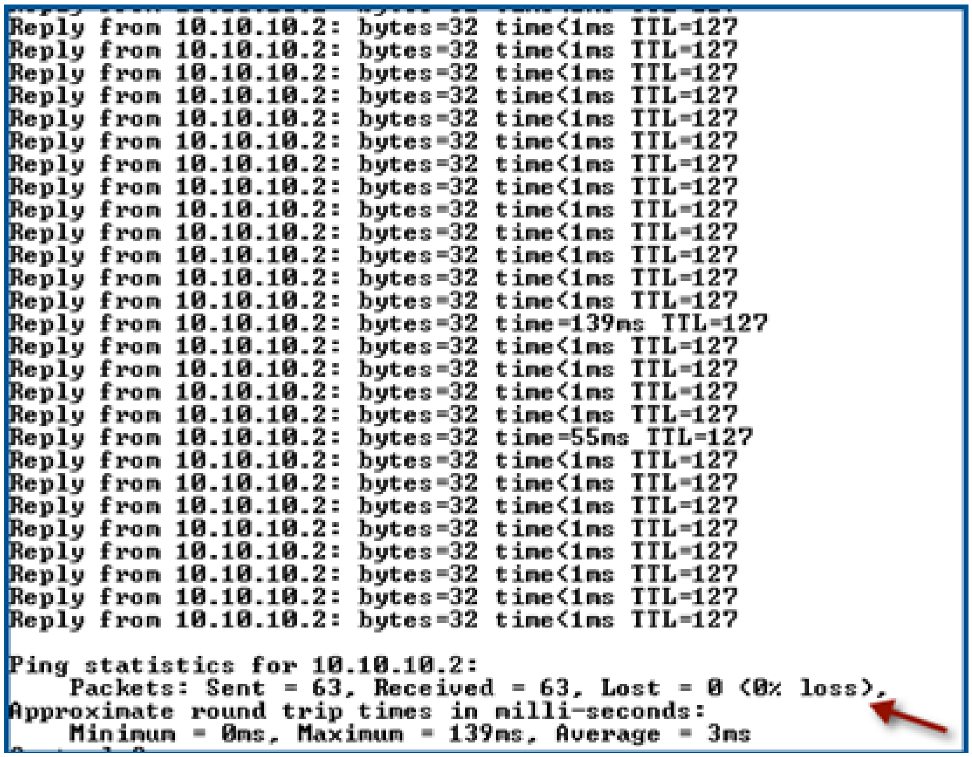
```
(POD1-WLC) >show ap uptime

Number of APs.................................... 2
Global AP User Name.............................. Not Configured
Global AP Dot1x User Name........................ Not Configured

AP Name             Ethernet MAC       AP Up Time                Association Up Time
------------------  -----------------  ------------------------  ------------------------
POD1-AP1            6c:20:56:e1:50:09  0 days, 03 h 57 m 13 s    0 days, 00 h 35 m 26 s
POD1-AP2            44:d3:ca:42:31:57  0 days, 15 h 57 m 52 s    0 days, 00 h 35 m 22 s
```

350697

Observe the AP CAPWAP State on WLC 2 which was standby initially and is Active now after switchover. AP uptime as well as Association UP Time is maintained and AP did not go in discovery state.

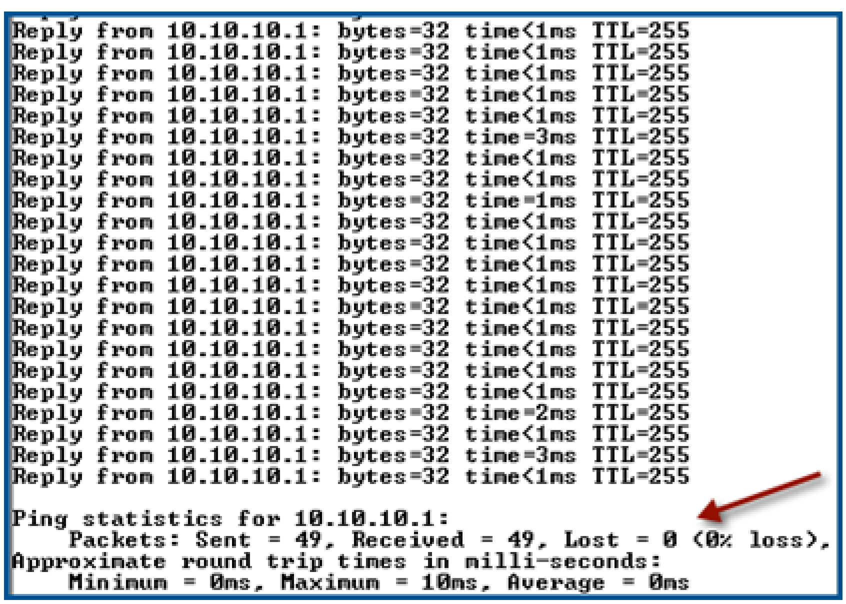
2. Also notice client connectivity when switchover is initiated. Client will be not be de-authenticated.

   Ping from wireless client to its gateway IP Address and management IP Address during switchover shows minimal loss.



```
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time=139ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time=55ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127

Ping statistics for 10.10.10.2:
    Packets: Sent = 63, Received = 63, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 139ms, Average = 3ms
```

350698



```
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=3ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=2ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=3ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.10.1:
    Packets: Sent = 49, Received = 49, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 0ms
```

350699

3. To check the redundancy status

WLC 1 -> Console connection issue a command **show redundancy summary:**

```
(POD1-WLC) >show redundancy summary
            Redundancy Mode = SSO ENABLED
                Local State = ACTIVE
                 Peer State = STANDBY HOT
                       Unit = Secondary - HA SKU (Inherited AP License Count = 62)
                    Unit ID = E0:2F:6D:5C:EE:A0
          Redundancy State = SSO (Both AP and Client SSO)
              Mobility MAC = E0:2F:6D:5C:F0:40

Average Redundancy Peer Reachability Latency = 2660 usecs
Average Management Gateway Reachability Latency = 751 usecs

Redundancy Management IP Address.................. 10.10.10.11
Peer Redundancy Management IP Address............. 10.10.10.10
Redundancy Port IP Address........................ 169.254.10.11
Peer Redundancy Port IP Address................... 169.254.10.10
Peer Service Port IP Address...................... 0.0.0.0

Switchover History[1]:
Previous Active = 10.10.10.10, Current Active = 10.10.10.11
Switchover Reason = User initiated, Switchover Time = Wed Apr  3 02:01:21 2013
```

350700

WLC 2 -> Console connection issue a command **show redundancy summary:**

```
(POD1-WLC-Standby) >show redundancy summary
            Redundancy Mode = SSO ENABLED
                Local State = STANDBY HOT
                 Peer State = ACTIVE
                       Unit = Primary
                    Unit ID = E0:2F:6D:5C:F0:40
          Redundancy State = SSO (Both AP and Client SSO)
              Mobility MAC = E0:2F:6D:5C:F0:40

Average Redundancy Peer Reachability Latency = 1347 usecs
Average Management Gateway Reachability Latency = 763 usecs

Redundancy Management IP Address.................. 10.10.10.10
Peer Redundancy Management IP Address............. 10.10.10.11
Redundancy Port IP Address........................ 169.254.10.10
Peer Redundancy Port IP Address................... 169.254.10.11

Switchover History[1]:
Previous Active = 10.10.10.10, Current Active = 10.10.10.11
Switchover Reason = User initiated, Switchover Time = Wed Apr  3 02:01:21 2013
```

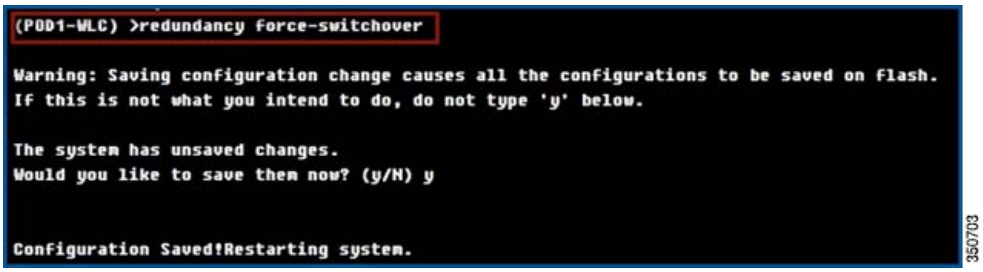
350701

WLC 2-> Click on **Monitor > Redundancy > Summary:**

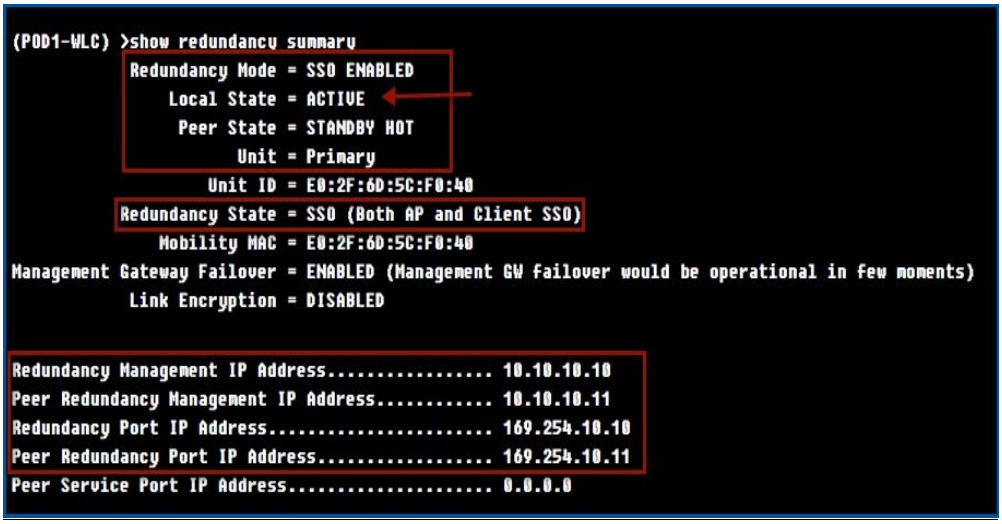
4. Initiate a force switchover again on current active WLC.

   WLC, which was configured as Primary Unit, should now be active and WLC, which was configured as Secondary Unit i.e., WLC 2 should be in Hot Standby State.

   WLC 2:



   WLC 1: Make sure Local state should be Active and Unit should be Primary on WLC 1 after switchover:



Observe the switchover history. WLC maintains 10 switchover histories with switchover reason.

```
Switchover History[1]:
Previous Active = 10.10.10.10, Current Active = 10.10.10.11
Switchover Reason = User initiated, Switchover Time = Wed Apr  3 02:01:21 2013
```

350705

Client SSO Behavior and Limitations

- The Bonjour dynamic database comprising of the services and service providers associated with a service and the domain name database is synced to standby.
- Only clients that are in Run state are synced between the Active and Standby WLC. Client SSO does not support seamless transitions for clients that are in the process of associating/joining the controller. The clients in the transition phase will be de-authenticated after switchover and will need to rejoin the controller.
- Posture and NAC OOB are not supported if the client is not in Run state.
- WGB and the clients associated to the WGB need to be re-associated post switchover.
- CCX based applications need to be re-started post Switchover.
- New mobility is not supported.

	New Mobility		Old/Flat Mobility	
	7.3.112.0	7.5	7.3.112.0	7.5
APSSO	Yes	Yes	Yes	Yes
Client SSO	No	No	No	Yes

- Client statistics are not synced.
- PMIPv6, NBAR, SIP static CAC tree are not synced, need to be re-learned after SSO.
- OEAP (600) clients are not supported.
- Passive clients need to be re-associated after SSO.
- Device and root certificates are not automatically synced to the Standby controller.
- AP and Client Rogue information is not synced to the Standby controller and needs to be re-learnt when the hot standby becomes the active controller.
- Sleeping client information is not synced to the standby controller.
- NBAR statistics are not synced to the secondary controller.
- Native Profiling data is not synced to the secondary controller, therefore, clients will be re-profiled after switchover.
- The below table captures the behavior w.r.t SSO with MAPs and RAPs.

	AP SSO	Client SSO
RAP	Supported	Not supported
MAP	Not Supported	Not supported

High Availability in Release 8.0

High Availability in release 8.0 introduces enhancements and improvements to the High Availability feature-set. The following enhancements are captured in this section:

- Bulk sync status
- Enhanced debugs and serviceability for HA
- Configurable keep-alive timer/retries and peer-search timer value
- Peer RMI ICMP ping replaced with UDP messages
- Standby WLC on-the-fly maintenance mode
- Default gateway reachability check enhancement
- Faster HA Pair up

High Availability in release 8.0 also introduces new features enabling SSO such as:

- Internal DHCP server support for SSO enabled controllers
- AP radio CAC statistics sync
- SSO support for sleeping client feature
- SSO support for OEAP 600 APs

Enhancements and Improvements

Bulk Sync Status

Currently, the controller does not provide any indication for the completion of Bulk Sync configuration once it is initiated. The Bulk Sync can be verified only by user observation and by manually checking the number of clients synced to the standby WLC. As part of this feature, a mechanism is provided to convey the status of Bulk Sync (both AP and client sync) when standby WLC comes up.

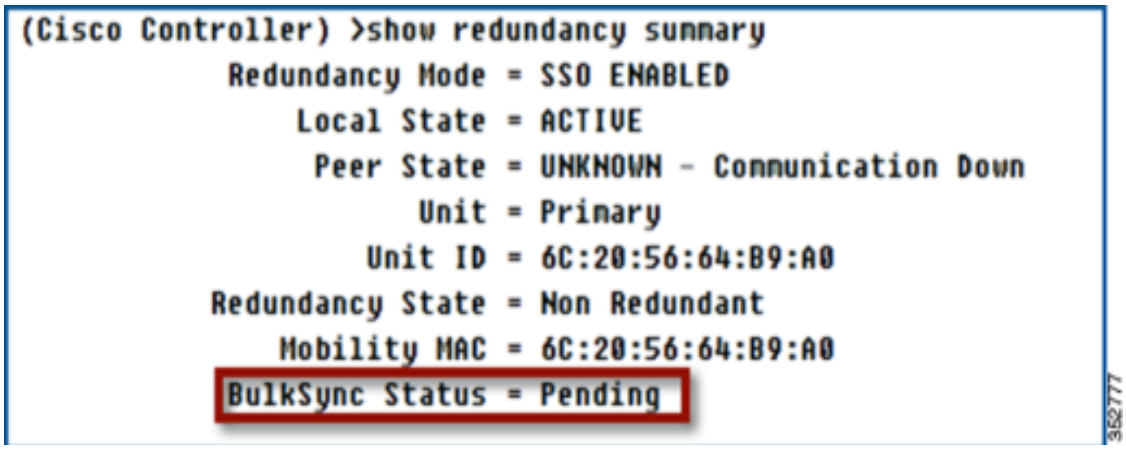
A new field called **BulkSync Status** is added in the GUI under **Controller > Redundancy > Summary**. This field points to the status of the bulk sync to the standby WLC and the status can be Pending/In-progress/Complete.

Figure 9 BulkSync Status GUI

The output of the CLI command **`show redundancy summary`** also displays the Bulk Sync status, which can be Pending/In-progress/Complete as shown below while pairing with the standby controller.

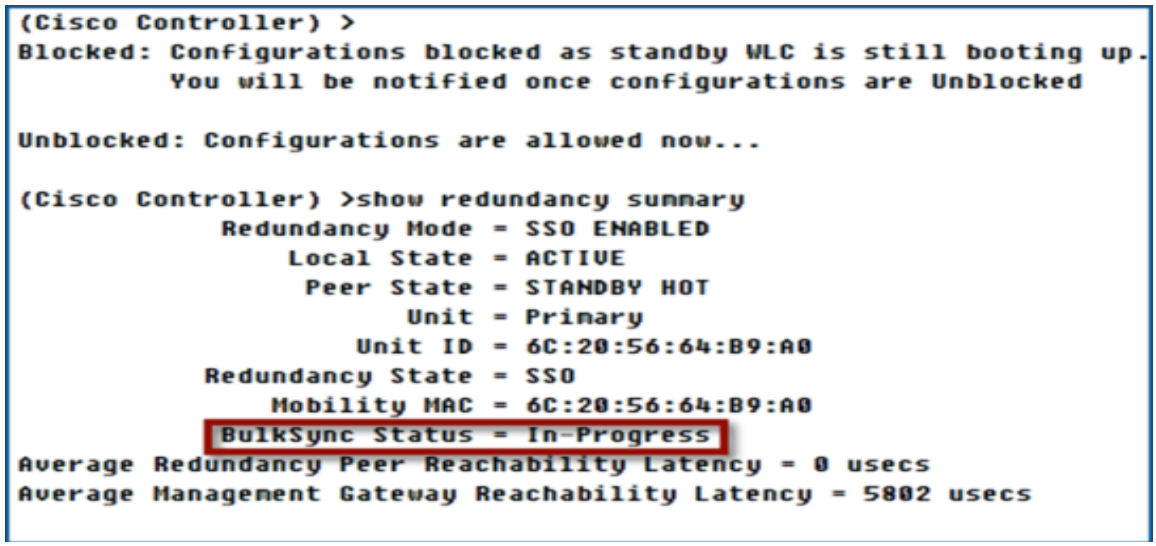
When the standby controller is booting up, the **BulkSync** status shows **Pending**.

Figure 10 BulkSync Status—Pending



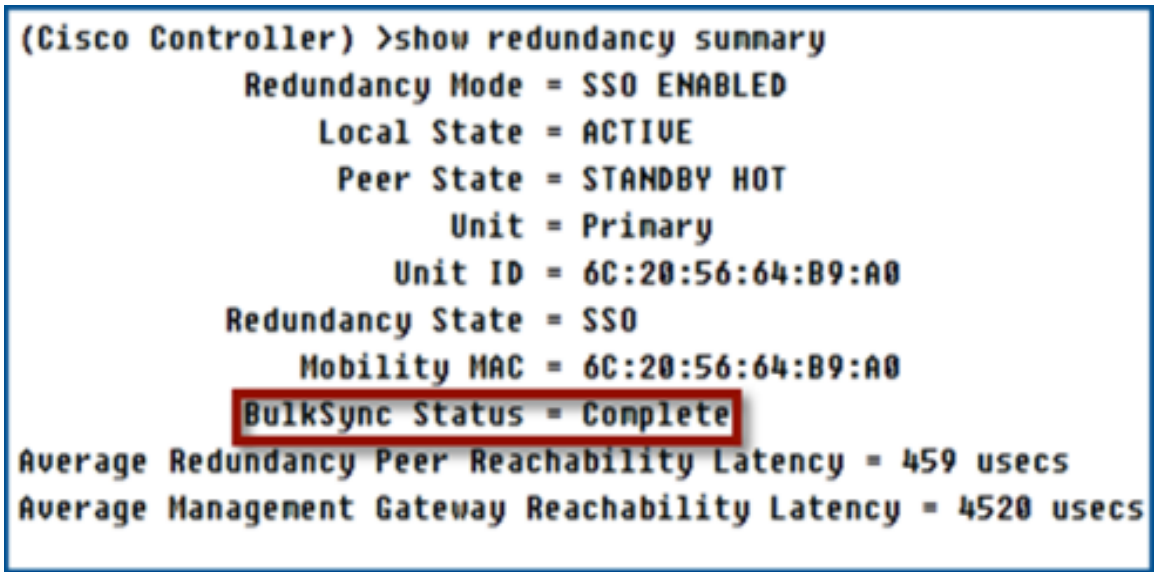
Once the standby controller completes, the boot-up process and the bulk sync starts, the status changes to **In-Progress**.

Figure 11 BulkSync Status—In-Progress



When the bulk sync process is complete, the **BulkSync** status changes to **Complete**.

Figure 12 BulkSync Status—Complete



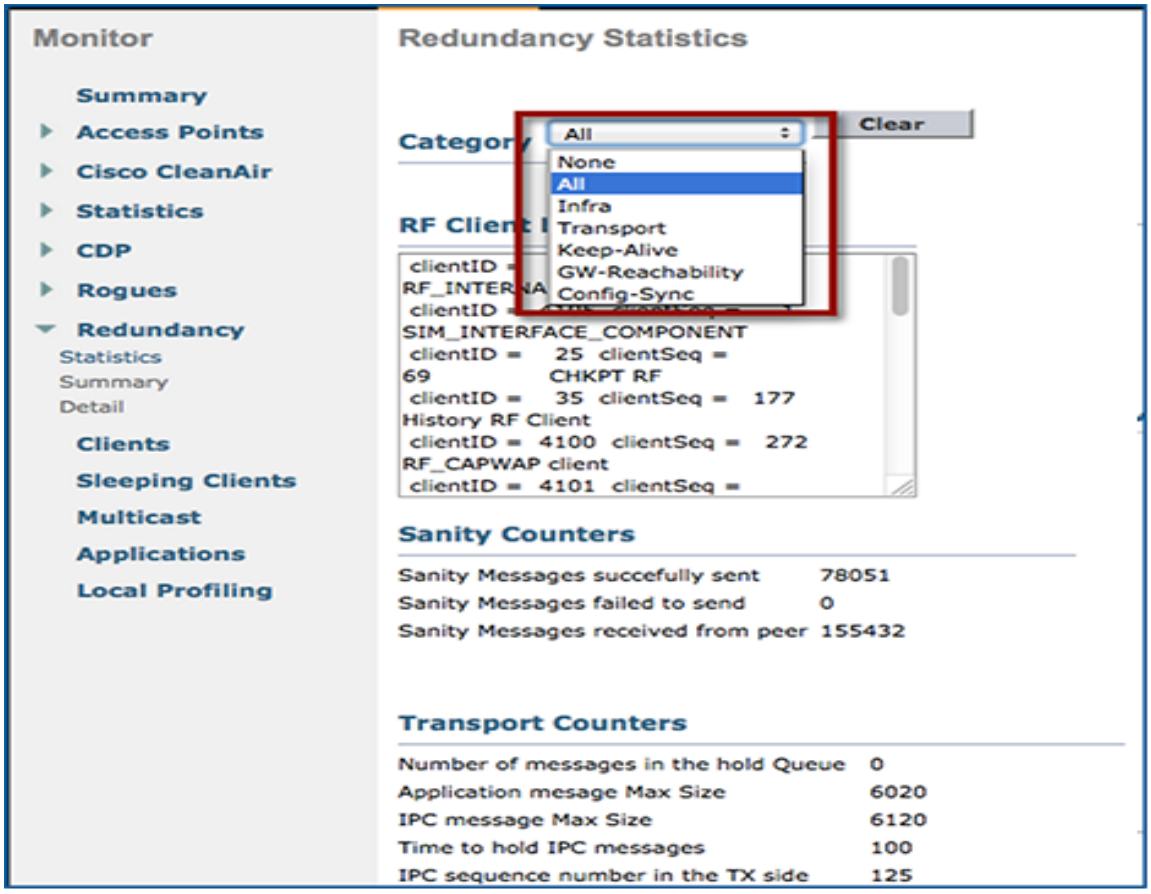
Debug/Show Command Enhancements

As HA plays a major role in avoiding network outage, it should also be pertinent to be able to debug the state changes on the boxes at the time of SSO or at a later point in time.

The following new categories of statistics are introduced under **Monitor > Redundancy > Statistics:**

a. All
b. Infra
c. Transport
d. Keep-Alive
e. GW-Reachability
f. Config-Sync

Figure 13 Redundancy Statistics GUI



The Infra statistics contain RF Client details and Sanity Counters as shown in Figure 14.

Figure 14 Redundancy Statistics—Infra

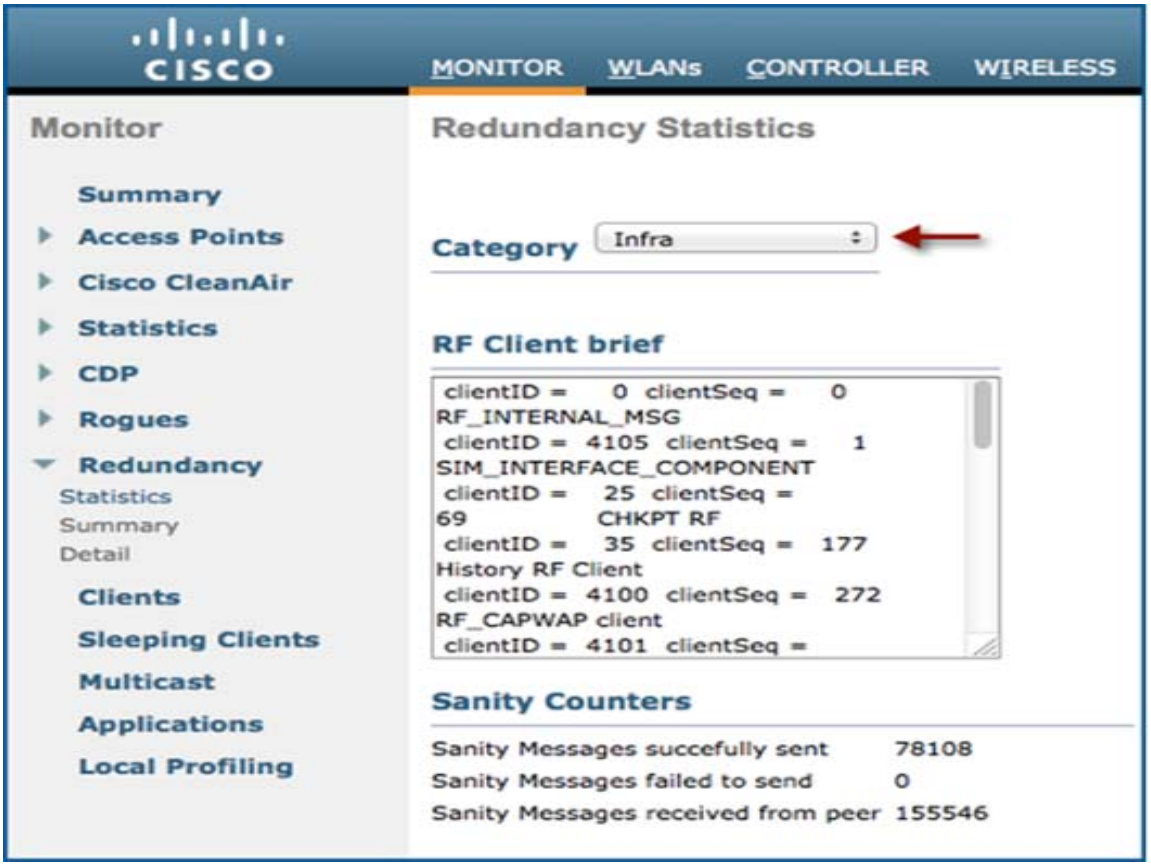
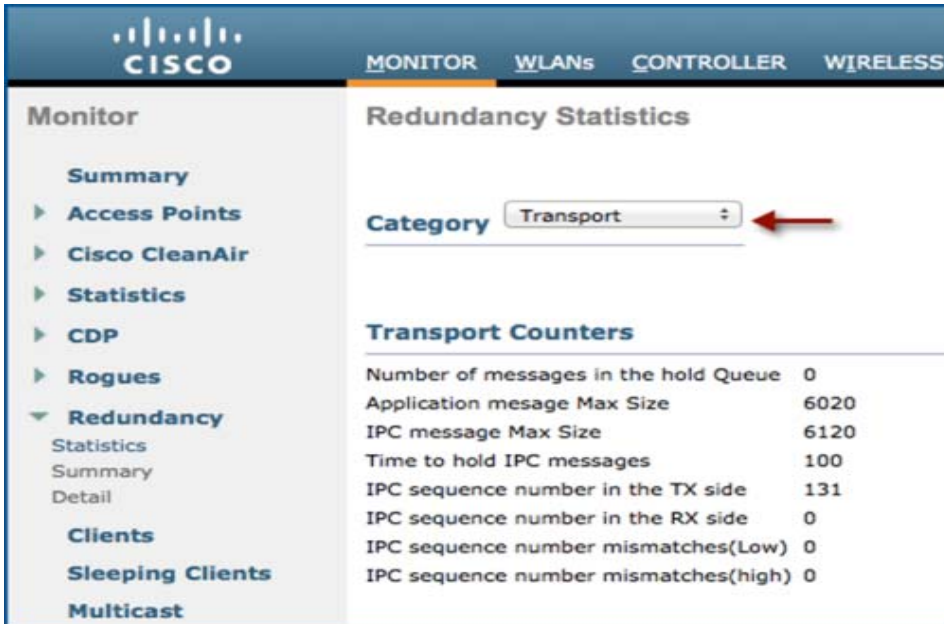
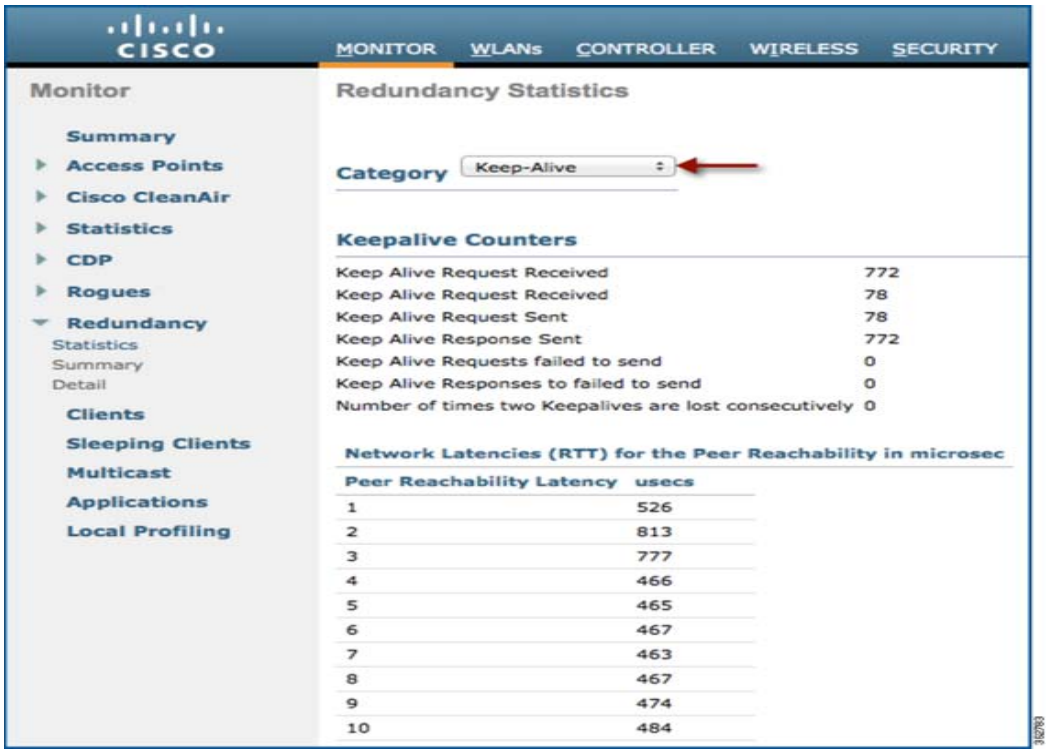


Figure 15 Redundancy Statistics —Transport



The Heartbeat debugs include events of reception of heartbeats, loss of heartbeats, and subsequent actions related to them.

Figure 16 Redundancy Keep-alive Statistics



The HA system monitors management gateway reachability to reduce network outage.

On the Standby controller, serviceability debugs related to the gateway reachability of the active controller and standby controller, their health states, and actions taken based on this information is reported. While on the active controller, the reachability of active WLC to the gateway alone is reported.

Figure 17 Redundancy GW-Reachability Statistics

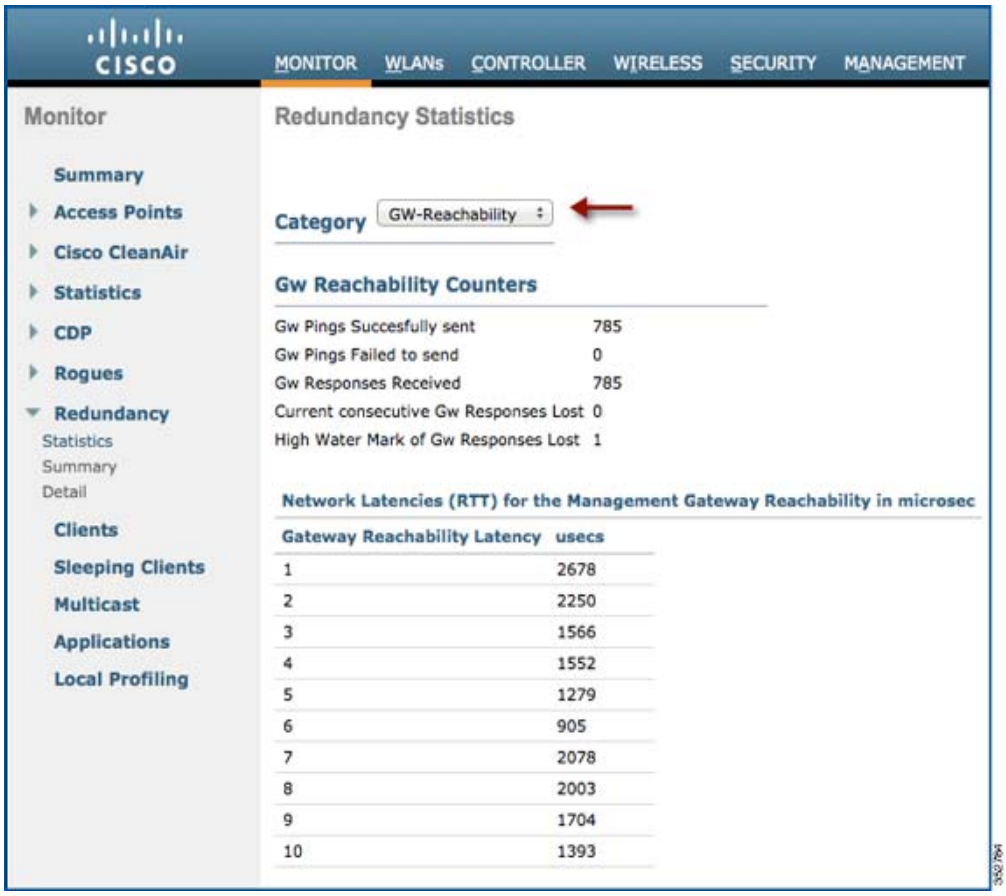


Figure 18 Redundancy Config-Sync Statistics

The following debug/show CLI commands are introduced for this feature:

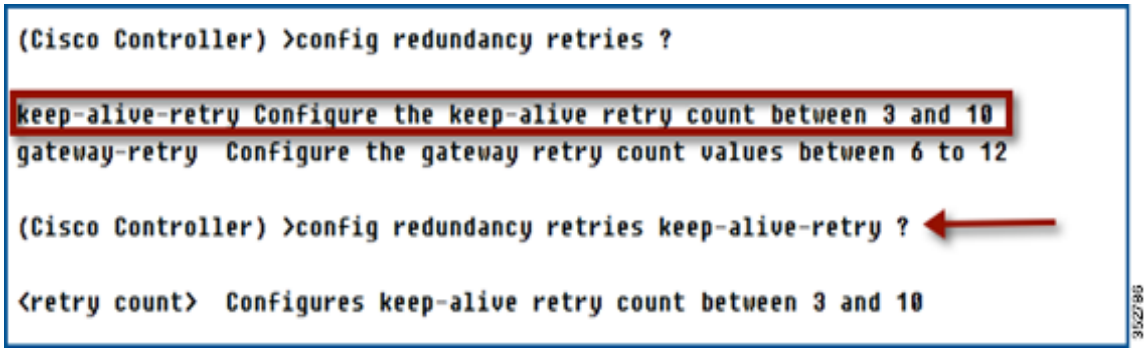
1. `debug redundancy infra detail/errors/event`
2. `debug redundancy transport detail/errors/events/packet`
3. `debug redundancy keepalive detail/errors/events`
4. `debug redundancy gw-reachability detail/errors/events`
5. `debug redundancy config-sync errors/events/detail`
6. `debug redundancy ap-sync errors/events/detail`
7. `debug redundancy client-sync errors/events/detail`
8. `debug redundancy mobility events/errors/detail`
9. `show redundancy infra statistics`
10. `show redundancy transport statistics`
11. `show redundancy keepalive statistics`
12. `show redundancy gw-reachability statistics`
13. `show redundancy config-sync statistics`
14. `show redundancy ap-sync statistics`
15. `show redundancy client-sync statistics`

Configurable Keep-alive and Peer-Search Parameters

To address the variable network latencies in different customer deployment scenarios, keep-alive and peer-search parameters are made configurable. As part of this enhancement, the maximum number of Keepalives between active and standby controllers to trigger a failover is now configurable. Also, peer-search timer and keep-alive timer are modified to support an extended range.

The following new CLI command is added to configure the number of redundancy keep-alive retries in the range of 3 to 10.

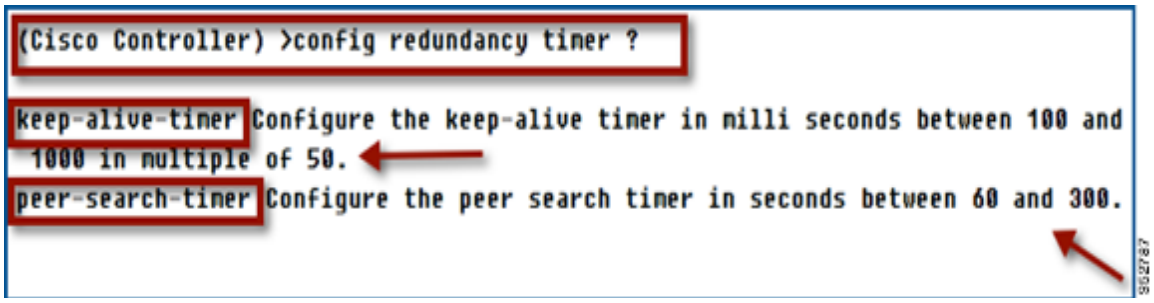
Figure 19 **`Redundancy retries` *CLI Command***



The existing CLI command **`config redundancy timer keep-alive-timer`** of keep-alive timer is modified to support keep-alive timer from 100 to 1000 msecs.

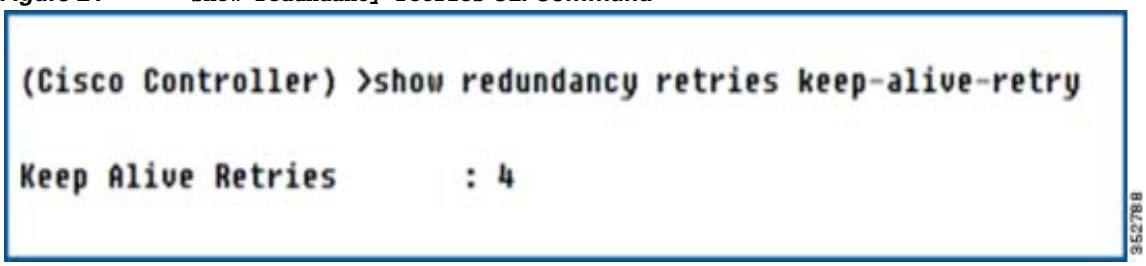
The existing CLI command **`config redundancy timer peer-search-timer`** of peer-search timer is modified to support peer-search timer from 60 to 300 secs.

Figure 20 **`Redundancy timer` *CLI Command***



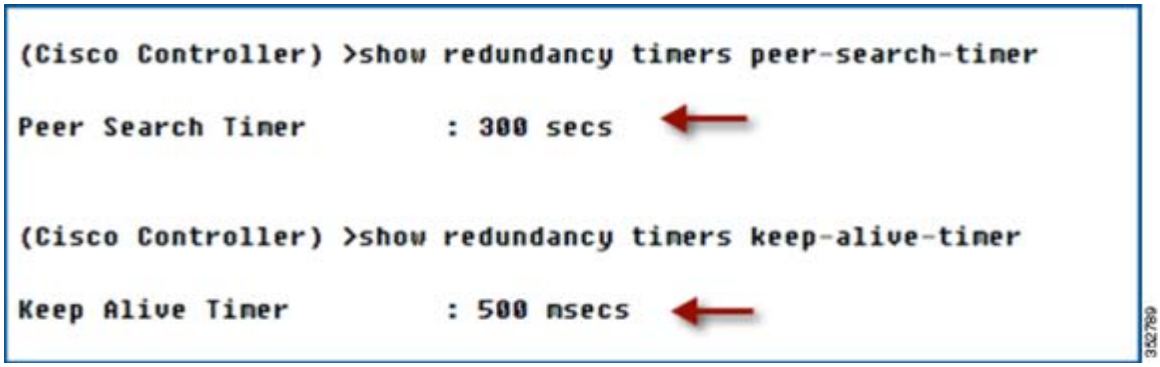
The following CLI is introduced to view the redundancy keep-alive-retry value.

Figure 21 **`Show redundancy retries` *CLI Command***



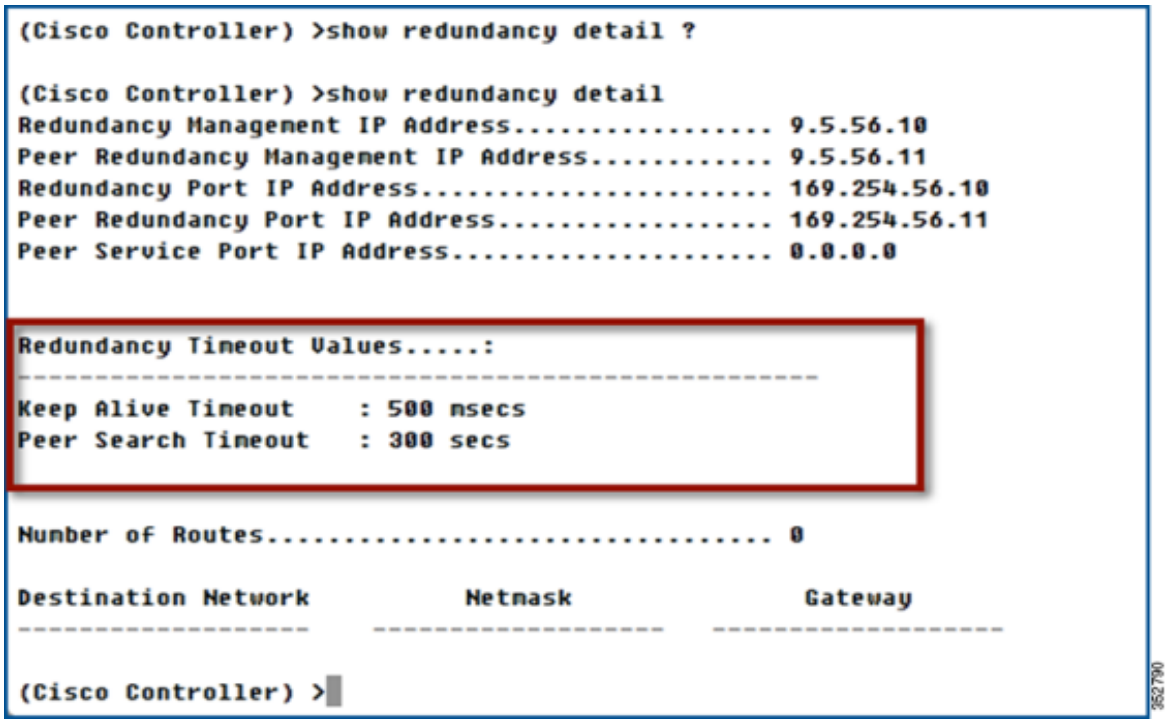
Use the **show redundancy timers** command to view the peer-search-timer and keep-alive-timer values.

Figure 22 **Show redundancy timers** ***CLI Command***



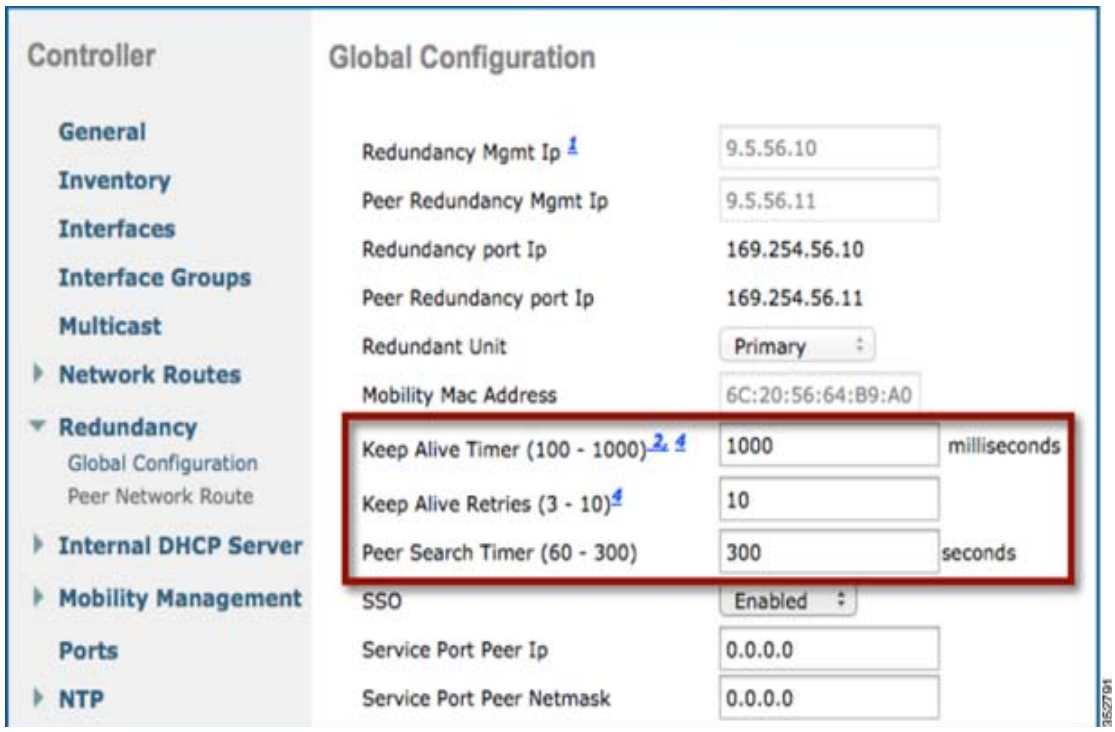
Use the **show redundancy detail** command to display the keep-alive and peer-search timeout values.

Figure 23 **Show redundancy detail** ***CLI Command***



The keep-alive timer, keep-alive retries, and peer-search timer can also be configured and viewed from the **Controller > Redundancy > Global Configuration** page in the GUI.

Figure 24 Redundancy Global Configuration GUI



Peer RMI ICMP Ping Replaced with UDP Messages

Prior to release 8.0, ICMP ping is used to heart-beat with the peer WLC over the Redundancy Management Interface. As part of this feature for release 8.0, ICMP ping is replaced with a UDP message.

This will benefit due to the following factors:

- ICMP ping packets might get discarded under heavy loads.
- Any other device with the same IP might also reply to the ping.

It is recommended to tag the RMI and management interfaces to avoid false Switchovers. Tagging of the RMI and management interfaces is now mandatory in release 8.0 to pair WLCs in SSO mode.

Standby WLC On-the-Fly Maintenance Mode (MTC)

Prior to release 8.0 when the standby controller looses reachability to the “Default Gateway” or “Peer RP”, the controller reboots and checks that condition while booting up and enters into the MTC mode. With this feature, the standby WLC will enter into the MTC mode “on-the-fly” without rebooting when such error scenarios occur. Once Peer-RP and the default gateway reachability is restored, the MTC mode auto-recovery mechanism introduced in release 7.6, will reboot the WLC and pair it with the active WLC. This mechanism is applicable only to the standby WLC. The active controller will still reboot before going to MTC mode.

Default Gateway Reachability Check Enhancement

As part of this enhancement, the gateway (GW) reachability check mechanism is modified to avoid false positives and it is also modified for the ideal time to start checking for gateway reachability once the controller boots up.

Prior to release 8.0, the “GW reachability check” is performed during Role negotiation. In release 8.0 and later, during Role negotiation, GW reachability check is not performed and is initiated only after the HA Pair-Up is complete.

Also, it is observed that certain Switch/Router configurations rate limits ICMP ping packets or drop them altogether. To avoid such conditions triggering false-positives, the new design ensures not to take switchover decisions purely based on ICMP ping losses. By the modified logic, upon 6 consecutive ping drops, an ARP request is sent to the GW IP address. A successful response to this request is considered as the GW being reachable.

Faster HA Pair Up

Currently during the HA pairing process, once the active-standby role is determined, the configuration is synced from the active WLC to the standby WLC via the Redundancy Port. If the configuration is different, the secondary WLC reports XML mismatch and downloads the configuration from the active controller and reboots again. In the next reboot after role determination, it validates the configuration again, reports no XML mismatch, and process further in order to establish itself as the Standby WLC.

With this feature enhancement, the XMLs are sent from the **to-be-Active** to **to-be-Standby** controller at the time of initialization, just before the validation of the XMLs. This avoids the extra step of comparison and reboot since no other modules are initialized yet, resulting in faster pair up of Active and Standby WLCs.

As seen in the boot logs below, there are no comparison of XMLs and no reboot of standby WLC.

Figure 25 Standby WLC bootup log

```
Starting Management Frame Protection: ok
Starting Certificate Database: ok
Starting VPN Services: ok
Starting DNS Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 300 seconds

Initiate Role Negotiation Message to peer

Found the Peer. Starting Role Determination...
ok
Starting LWAPP: ok
Starting CAPWAP: ok
Starting LOCP: ok
Starting Security Services: ok
Starting Policy Manager: ok
Starting Authentication Engine: ok
Starting Mobility Management: ok
Starting Capwap Ping Component: ok
Starting AVC Services: ok
Starting Virtual AP Services: ok
Starting AireWave Director: ok
Starting Network Time Services: ok
```

352792

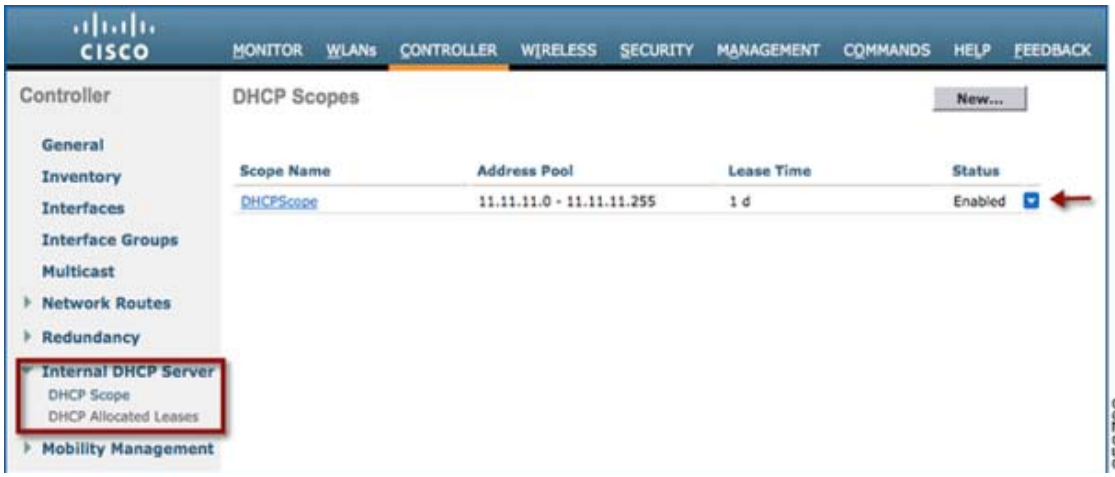
New Features Support in SSO

SSO Support for Internal DHCP Server

Prior to release 8.0, configuration of "Internal DHCP Server" is not allowed on HA enabled controllers because the internal DHCP server data is not synced to the standby WLC. In release 8.0 and later, "Internal DHCP Server" is configured on HA enabled controllers and this data is synced to the standby WLC so that soon after a switchover, the "Internal DHCP Server" on the new active controller starts serving clients.

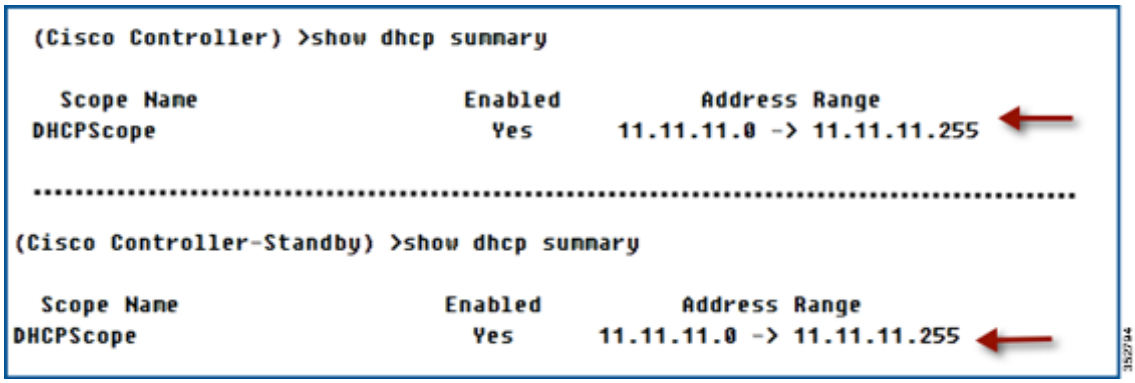
To configure the Internal DHCP server using the GUI, navigate to **Controller > Internal DHCP Server**

Figure 26 Internal DHCP Server GUI



The same is synced to the standby controller and is verified by executing the CLI command **`show dhcp summary`**

Figure 27 `show dhcp summary` on Active and Standby WLC



AP Radio CAC Statistics Sync

As part of this enhancement, Static CAC method bandwidth allocation parameters for Voice and Video and Call Statistics are synced to the Standby WLC, so that soon after a switchover, respective information is available on the new active controller that will be used for call admission control.

SSO Support for Sleeping Clients

Release 7.5 did not provide SSO support for sleeping clients. The sleeping client database was not synced to the standby controller, which caused the sleeping clients to re-authenticate after a switchover occurred. With this release, sleeping client database is synced to the standby controller, allowing sleeping clients to avoid web re-authentication if they wake up within the sleeping client timeout interval.

The CLI command **`show custom-web sleep-client summary`** is used to verify the sleeping client database sync between the active and standby WLC.

Figure 28 Sleeping Client Database on Primary WLC

```
(Cisco Controller) >show custon-web sleep-client summary

Active Sleep-Client entries.............1
Max Sleep-Client entries supported.....1000


MAC Address of Client             UserName        Time Renaining
---------------------             --------        --------------

7c:d1:c3:86:7e:dc                 cisco            12 hours 0 mins
```

352795

Figure 29 Sleeping Client Database on Standby WLC

```
(Cisco Controller-Standby) >show custon-web sleep-client summary

Active Sleep-Client entries.............1
Max Sleep-Client entries supported.....1000


MAC Address of Client             UserName        Time Renaining
---------------------             --------        --------------

7c:d1:c3:86:7e:dc                 cisco            12 hours 0 mins
```

352796

Figure 30 Sleeping Client Details on Active and Standby WLC

```
(Cisco Controller) >show custom-web sleep-client detail 7c:d1:c3:86:7e:dc
Mac               : 7c:d1:c3:86:7e:dc
Username          : cisco
Time Left         : 11 hours 40 min
WLAN(SSID)        : enjoy-WebAuth

(Cisco Controller-Standby) >show custom-web sleep-client detail 7c:d1:c3:86:7e:dc
Mac               : 7c:d1:c3:86:7e:dc
Username          : cisco
Time Left         : 11 hours 40 min
WLAN(SSID)        : enjoy-WebAuth
```

352797

SSO Support for OEAP 600 APs

Prior to release 8.0, when a switchover occurs on an HA pair, OEAP 600 APs restarts the CAPWAP tunnel and joins back the new active controller, and all the connected clients are de-authenticated. As a part of this feature, OEAP 600 APs ensure not to reset their CAPWAP tunnel. Also, clients continue their connection with the new active controller in a seamless manner.

As shown below, the output of **`show ap summary`** and **`show client summary`** command on the active and standby controllers displays the AP and client database sync.

Figure 31 OEAP 600 AP on Active WLC

```
(Cisco Controller) >show ap summary

Number of APs.................................... 1

Global AP User Name.............................. Not Configured
Global AP Dot1x User Name........................ Not Configured

AP Name             Slots  AP Model             Ethernet MAC      Location          Country     IP Address
------------------  -----  -------------------  ----------------  ----------------  ----------  -----------
-
OEAP600              3     AIR-OEAP602I-N-K9    ec:c8:82:b9:6c:60  default location IN       9.5.56.107
```

352798

Figure 32 OEAP 600 AP Sync to Standby WLC

```
(Cisco Controller-Standby) >show ap summary

Number of APs.................................... 1

Global AP User Name.............................. Not Configured
Global AP Dot1x User Name........................ Not Configured

AP Name             Slots  AP Model             Ethernet MAC      Location          Country     IP Address
------------------  -----  -------------------  ----------------  ----------------  ----------  -----------
OEAP600              3     AIR-OEAP602I-N-K9    ec:c8:82:b9:6c:60  default location IN       9.5.56.107
```

352799

Figure 33 Clients on Active WLC

```
(Cisco Controller) >show client summary

Number of Clients................................ 1

Number of PMIPV6 Clients......................... 0

                                                  GLAN/
                                                  RLAN/
MAC Address       AP Name           Slot Status       WLAN  Auth Protocol         Port Wired PMIPV6  Role
----------------- ----------------- ---- ------------ ----- ---- ---------------- ---- ----- ------- -------
7c:d1:c3:86:7e:dc OEAP600            1   Associated     1    Yes  802.11n(5 GHz)   1    No    No      Local
```

Figure 34 Client Sync to Standby WLC

```
(Cisco Controller-Standby) >show client summary

Number of Clients................................ 1

Number of PMIPV6 Clients......................... 0

                                                  GLAN/
                                                  RLAN/
MAC Address       AP Name           Slot Status       WLAN  Auth Protocol         Port Wired PMIPV6  Role
----------------- ----------------- ---- ------------ ----- ---- ---------------- ---- ----- ------- ------
7c:d1:c3:86:7e:dc OEAP600            1   Associated     1    Yes  802.11n(5 GHz)   1    No    No      Local
```

Web Links

- Cisco WLAN Controller Information:
  http://www.cisco.com/c/en/us/products/wireless/4400-series-wireless-lan-controllers/index.html
  http://www.cisco.com/c/en/us/products/wireless/2000-series-wireless-lan-controllers/index.html
- Cisco NCS Management Software Information:
  http://www.cisco.com/c/en/us/products/wireless/prime-network-control-system-series-appliances/index.html
- Cisco MSE Information:
  http://www.cisco.com/c/en/us/products/wireless/mobility-services-engine/index.html
- Cisco LAP Documentation:
  http://www.cisco.com/c/en/us/products/wireless/aironet-3500-series/index.html

Terminology

- APM—AP Manager Interface
- Dyn—Dynamic Interface
- Management—Management Interface
- Port—Physical Gbps port
- WiSM-2—Wireless Service Module
- AP—Access Point
- LAG—Link Aggregation
- SPAN—Switch Port Analyzer
- RSPAN—Remote SPAN
- VACL—VLAN Access Control List
- DEC—Distributed Etherchannel
- DFC—Distributed Forwarding Card
- OIR—Online Insertion and Removal
- VSL—Virtual Switch Link
- ISSU—In Service Software Upgrade
- MEC—Multichassis Ether Channel
- VSS—Virtual Switch System
- WCS—Wireless Control System
- NAM—Network Analysis Module
- IDSM—Intrusion Detection Service Module
- FWSM—Firewall Service Module
- STP—Spanning Tree Protocol
- VLAN—Virtual LAN
- SSO—Stateful Switchover

- WCP—Wireless Control Protocol
- WiSM-2—Wireless Service Module-2

Glossary

A

AP SSO Access Point State Full Switchover where CAPWAP state for each AP is maintained on Active and Standby WLC and CAPWAP state is retained after switchover to Standby WLC. AP need not go through CAPWAP discovery and join process after failover.

Active WLC This is the WLC which is currently active in HA pair and taking care of the wireless network. APs establish single CAPWAP tunnel with Active WLC.

C

Client SSO Wireless Client State Full Switchover where client state is also maintained on Active and Standby WLC and wireless clients are not de-authenticated after switchover. Will be supported in future release.

K

Keep-Alive-Timer Standby WLC in HA setup sends keep-alive packets on redundancy port to check the health of active WLC. With no acknowledgment of three keep-alive packets from active WLC, standby declares active as dead and takes over the network.

M

Maintenance Mode When Standby WLC cannot communicate to gateway or cannot discover peer WLC i.e. active WLC via redundant port it goes in Maintenance mode. In this mode WLC cannot communicate to infra network and will not participate in HA process. Because WLC in maintenance mode does not participate in HA process it need to be manually rebooted to bring it out of maintenance mode and make participate in HA process again.

Mobility MAC Unique MAC address shared between peers in HA setup. This mac address should be used to form a mobility pair between HA setup and another WLCs in HA setup or with independent controllers. By default active WLC mac address is shared as mobility mac address but mobility mac can also be manually configured on active WLC using a CLI, which will be shared between peers in HA setup.

P

Peer AP SSO is box-to-box redundancy i.e. 1:1 so both the WLCs (Active and Standby) in HA setup are peer to each other.

Primary Unit	In AP SSO deployment controller running higher permanent count licenses should be configured as primary unit. Primary Unit is the WLC, which will take the role of Active WLC first time it forms HA pair. Primary Unit sends the lic count information to its peer via redundant port.
Peer-Search-Timer	While booting, standby WLC waits for peer search timer (default 2 minutes) to discover the peer. If WLC cannot discover its peer within this time it will transition its state to maintenance mode.

R

Redundancy Port	Physical Port on 5500/7500/8500 WLC for HA role negotiation, configuration sync and redundancy messages between Active and Standby WLC.
Redundancy Vlan	Vlan created on Cat6500 Sup for WiSM-2 Redundancy Port that is connected to Cat6k backplane to exchange configuration and redundancy messages including HA role negotiation between Active and Standby WLC.
Redundancy Management Interface	A parallel interface to management interface on both the WLC in HA setup. Should be in same subnet as management interface. This interface let standby WLC interact with infra network and also exchange some redundancy messages over infra network between Active and Standby WLC.

S

Standby WLC	This is the WLC that is monitoring active controller in HA pair and ready to take over the wireless network in event of Active WLC failure.
Secondary Unit	In AP SSO deployment controller running lower or equal permanent count lic should be configured as secondary unit OR controller with HA SKU UDI (zero AP count lic) is shipped default as secondary unit. Secondary Unit is the WLC, which will take the role of Standby WLC first time it forms HA pair. Secondary unit inherit the lic count information from its peer i.e. Active WLC via redundant port.

Related Information

- Technical Support & Documentation - Cisco Systems