# High Availability

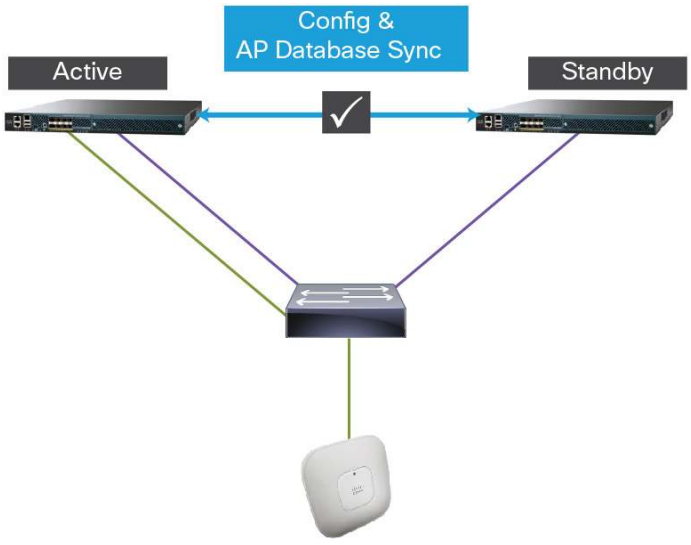
**Q.** In Cisco® Unified Wireless Network Software Release 7.3, what are the enhancements in the area of high availability (HA) of wireless LAN controllers?

**A.** Before Release 7.3 in a Cisco Unified Wireless Network deployment, an access point could be configured with primary, secondary, and sometimes even tertiary controllers. When the primary controller failed, depending upon the number of access points managed by a controller, the access point may be down for tens to hundreds of seconds before failing over to the secondary controller. Once it detected that the primary controller was unavailable, the access point would have to rediscover the controller and reestablish the Control and Provisioning of Wireless Access Points (CAPWAP) tunnel to the secondary controller. In addition, the client would need to reauthenticate with the access point and reestablish any session-sensitive applications such as Telnet or Citrix.

With Release 7.3, a controller can be configured as a hot standby controller to another controller designated as the active controller. The redundancy ports of these two controllers are connected with an Ethernet cable. This connection is used to exchange configurations and keep the databases in sync. The standby controller maintains the CAPWAP states of the access points connected to the active controller. This is why a subsecond failover can be achieved from the active controller to the standby.

The standby controller also syncs the pairwise master key (PMK) key cache from the active controller. In this way, when the client reassociates with the access point, there is no need for the controller to reauthenticate with the RADIUS server (Figure 1).

**Figure 1.** Fast Access Point Failover Between Primary and Standby Controllers



**Q.** What actions can trigger access points to fail over to the standby controller?

**A.** The following scenarios are supported:

- Failure of the controller appliance: Downtime before failover occurs is reduced to less than 1 second. Note that it is not possible to achieve hitless software upgrade of a controller.
- Network failure (for example, a network issue that prevents the active controller from reaching the gateway): Downtime of up to 12-15 seconds.

**Q.** How often is the keep-alive check done between the active and standby controllers?

**A.** Every 100 ms, a keep-alive is sent by the standby to the active controller to check the status. In case of the Cisco 5508 Wireless Controller, Cisco Flex 7500 Series Wireless Controllers, and Cisco 8500 Series Wireless Controllers, this is done on the redundancy port. In the case of the Cisco Wireless Services Module 2 (WiSM2) blade server, the keep-alive is sent over a redundancy VLAN.

**Note:** The redundancy vlan need to be configured on the Supervisor.
e.g CLI - wism redundancy-vlan 169

**Q.** If a user is on an active voice call during a failure, what impact will he or she experience?

**A.** Cisco Unified Wireless Network Releases 7.3 and 7.4 support only single sign-on for access points. With the enhancements in high availability, the client may have to reestablish the connection with the access point. Assuming no change in IP address, the user will most likely experience a few seconds of jitter when the switchover occurs.

In 7.5 - The Clients session should be maintained upon switchovers.

**Q.** Do my active and standby controllers share the IP address or operate as separate devices?

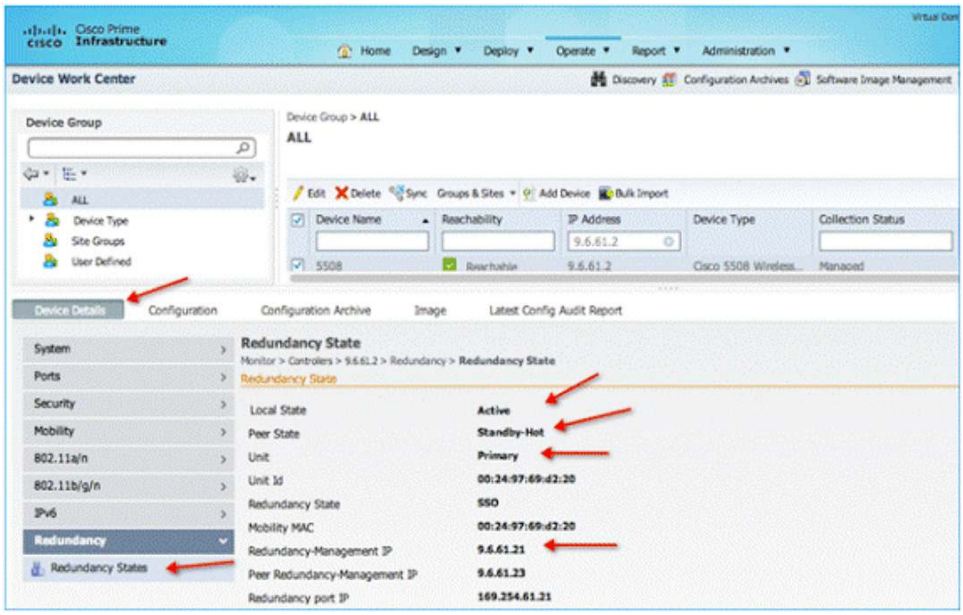
**A.** The two controllers operate as separate devices but do share the same IP address. The entire configuration is exactly the same, except for the redundancy management IP and redundant port IP.

**Q.** How do I know if my two wireless LAN controllers (WLCs) have properly paired up?

**A.** To check the redundancy state of the active WLC from the Cisco Prime™ Network Control System (NCS), go to Device Details > Redundancy > Redundancy States (Figure 2).

In CLI - The pair up details will be seen under - “show redundancy summary”.

**Figure 2.** NCS GUI Showing the Standby Controller




**Q.** Which controller models also provide the -HA SKU, and which support the stateful switchover (SSO) functionality?

**A.** Table 1 lists the controller models and indicates whether they support -HA and SSO.

**Table 1.** Controller Support for -HA and Stateful Switchover

| Controller Model | SKU | Supports N+1 | Supports SSO |
|---|---|---|---|
| **5508** | AIR-CT5508-HA-K9 | Yes | Yes |
| **WiSM2** | WS-SVC-WISM2HA-K9=<br>WS-SVC-WISM2-HA-K9 | Yes | Yes |
| **Flex 7500** | AIR-CT7510-HA-K9 | Yes | Yes |
| **8500** | AIR-CT8510-HA-K9 | Yes | Yes |
| **2500** | AIR-CT2504-HA-K9 | Yes | No |
| **UC blade on ISR G2** | No | Yes | No |
| **Virtual controller** | No | Yes | No |

**Q.** Can the primary and standby controller operating in stateful switchover be two different models?

**A.** No. The primary and standby controller both need to belong to the same product family (for example, the 5508) and be running the same software version. You can have a different controller model be the N+1 backup controller to the primary. For example, a Cisco 8500 Series controller can act as the N+1 controller to multiple Cisco 5500 Series controllers in the branch offices.

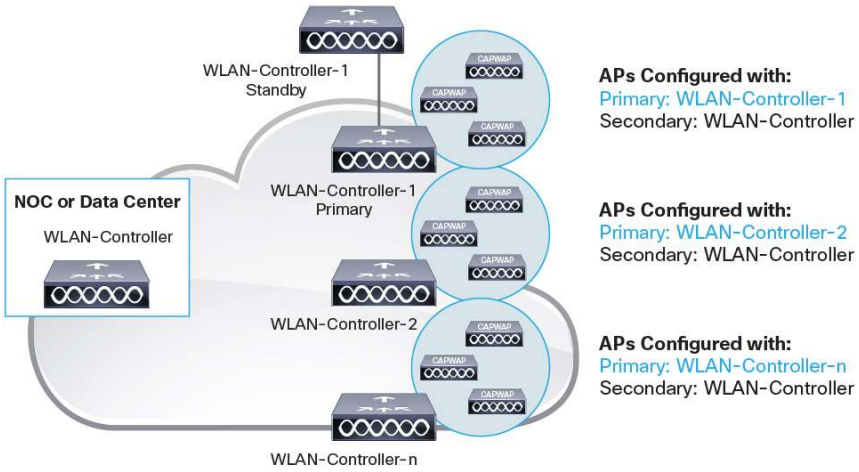
**Q.** Can my access points managed by the controllers connected in stateful switchover be operating in centralized, Cisco FlexConnect™, or mesh modes?

**A.** Yes. The access points managed by controllers in SSO can operate in any of these modes. In the case of mesh mode, only access point SSO functionality is supported, because the access point CAPWAP states are copied over. However, synchronization of underlying technologies such as Adaptive Wireless Path Protocol (AWPP) is not supported.

**Q.** Can we support additional redundancy by configuring a third controller configured with an N+1 model in addition to the two controllers in active-standby mode?

**A.** Yes, it is possible to have the active controller be a part of an N+1 design, as shown in Figure 3.

**Figure 3.** Additional N+1 Redundancy




## Standby Controller Licensing

**Q.** Do I need to buy access point licenses on my standby controller?

**A.** No. When the active controller is unavailable, the standby controller will adopt the licenses from the primary controller. It is expected that the customer will be able to get the primary controller back online within 90 days. After 90 days, the customer will get a daily reminder to switch back to the primary controller.

**Q.** I already have a spare controller. Can I convert that controller to the standby controller?

**A.** Yes. Customers need to upgrade their controller software to Release 7.3. They can then convert the spare to a standby controller using the command-line interface or GUI.

It is important to note that on the Cisco 5508, the controller needs to have at least 50 access point licenses in order to be able to convert the controller to the standby controller for the wireless LAN.

**Q.** Can I transfer the licenses from the spare controller to another controller?

**A.** The following link provides information on how to transfer “Adder” licenses from one WLC to another: http://www.cisco.com/en/US/docs/wireless/controller/7.0/configuration/guide/c70ccfg.html#wp1880270.

It is not possible to transfer the base licenses (that come installed along with the purchase of the controller) to another controller. For further details about the Cisco Flex 7500 Series and Cisco 8500 Series platforms that support Right to Use (RTU) licensing, see the RTU Q&A.

**Q.** What new capabilities are introduced starting with Release 7.4 in high-availability licensing?

**A.** Starting with Release 7.4, the -HA SKU can be used in N+1 mode. After 90 days, a daily reminder about reconnecting the primary controller will be sent to the network administrator.

**Q.** Can I convert the HA SKU for use as a primary controller and add licenses on the primary controller once converted?

**A.** Yes. Starting 7.6, customers can convert -HA those as SKU to primary via issuing the command "config redundancy unit primary" followed by adding licenses to this controller.

**Q.** Can the -HA SKU that has been deployed as an N+1 mode geographically separate from the primary be redeployed to support client stateful switchover?

**A.** Yes. You need to redeploy the standby controller physically adjacent to the primary and support the full “no SSID outage.”

**Q.** What is the difference in functionality between an -HA SKU operating as the N+1 controller and a fully licensed controller operating as an N+1 controller?

**A.** An -HA SKU operates only as a standby controller. This implies that it gets activated only when one or more primary controllers go down. Customers that intend to load-balance need to purchase fully licensed controllers.

**Q.** What is the capacity of the N+1 standby controller when an -HA SKU is used in N+1 mode?

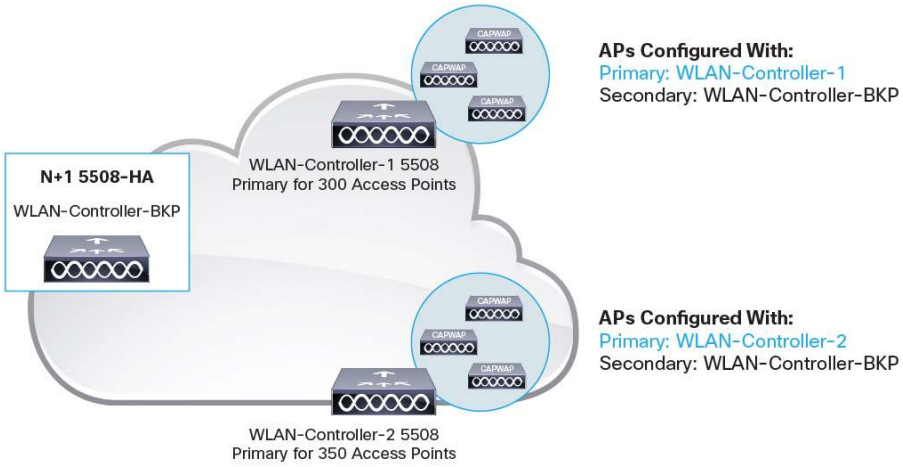
**A.** Whether the customer purchases an -HA controller SKU or converts an existing controller to the HA SKU, the HA SKU can support the full capacity of the model (see Table 2).

**Table 2.** Models and Access Point Counts

| Model | Access Point Count |
|---|---|
| **Cisco 5500 Wireless Controller** | 500 |
| **Cisco Wireless Services Module 2 (WiSM2)** | 1000 |
| **Cisco Flex 7500 Series Wireless Controller** | 6000 |
| **Cisco 8500 Series Wireless Controller** | 6000 |
| **Cisco 2500 Series Wireless Controller** | 75 |

Consider the scenario in Figure 4, in which two controllers fail over to a single N+1 standby controller.

**Figure 4.** Two Controllers Failing Over to a Single N+1 Standby Controller




The first primary controller is a 5508 with support for 300 access points, while the second primary controller is a 5508 with support for another 350 access points.

Both of them are backed up by a single 5508-HA, which supports a capacity of 500 access points.

If the first controller fails, all 300 of the access points will fail over to the N+1 standby controller. This means a capacity of 500 - 300 = 200 is left on the -HA SKU.

If the second primary controller also fails over, only 200 of the Cisco Aironet® 350 Series Access Points connected to the second controller will fail over to the N+1 controller. Note that you can prioritize the access points that fail over in a manner similar to the existing mechanism described at http://www.cisco.com/en/US/docs/wireless/controller/7.3/configuration/guide/b_wlc-cg_chapter_01000.html#ID3096.

**Q.** Can the N+1 standby controller be a different model of controller than the primary?

**A.** Yes. The N+1 standby can be the same or a different model of wireless LAN controller. For example, the primary can be a Cisco 5508, while the N+1 standby is a Cisco 8510 Wireless Controller. Note that in such a scenario you do not get the access point stateful failover functionality.

**Q.** How does client SSO, available with Release 7.5, enhance the user experience with high availability?

**A.** Releases 7.3 and 7.4 support 1:1 active-standby access point SSO, which ensures that no Service Set Identifier (SSID) outage occurs. In other words, if the active controller fails for some reason, the access points fail over in less than a second from the active to the standby (new active) controller. Each client needs to reauthenticate against the currently active controller. At the rate of several tens of simultaneous authentications per second on the controller, it can take anywhere from zero to a few hundred seconds for the tens of thousands of clients to associate that may be connected per controller. The 1:1 active-standby client SSO in Release 7.5 helps ensure that even the clients do not need to reauthenticate, and the time for clients to reconnect to the standby controller goes down to less than a second. This means that users will experience downtime of only the 2 to 3 seconds it takes for the specific application (such as voice or Citrix) to recover after the failover.

**Q.** Can my secondary wireless LAN controller for stateful switchover be placed in another data center?

**A.** The 7.5 release allows you to deploy the secondary controller in the Layer 2 adjacent separated environment from the primary controller so that they share the management IP address.

The following topologies are supported:

- Two 5508, 7500, or 8500 models connected via back-to-back route processor (RP) port in the same data center (similar to releases 7.3 and 7.4)
- Two 5508, 7500, or 8500 models connected via the RP port over Layer 2 VLAN/fiber in the same or different data centers
- Two 5508, 7500, or 8500 models connected to a virtual switching system (VSS) pair.

**Note:** If supervisor failover in VSS is triggered, it is recommended that you configure peer search time on the active HA pair controllers to 180 seconds. This is because it takes about 120 to 130 seconds for the line card to come up after a supervisor failover in VSS.

For WiSM2, the following three topologies are supported (similar to releases 7.3 and 7.4):

- Two WiSM-2 on the same chassis
- Two WiSM-2 on different chassis with redundancy VLAN extended over the Layer 2 network

- Two WiSM-2 on different chassis in VSS mode

**Note:** When Supervisor 2T is used, the access point has been seen to enter into discover mode after a switchover. The issue has been root caused, and the fix is available in the MK1 release of Cisco IOS® Software. If the IOS image (MK1) is not yet loaded on the Supervisor 2T, the workaround is to configure fixed hashing for the port channel globally and adaptive hashing for other port channels. For example:

Globally configure fixed hash distribution:

```
Router(config)#port-channel hash-distribution fixed.
```

Then configure adaptive hash distribution for other port channels if required:

```
Router(config)#int port-channel 10
Router(config-if)#port-channel port hash-distribution adaptive
```

The above configuration will ensure that port channel 10 will use adaptive hash distribution and all other port channels will use fixed hash distribution (including port channels that will be created for WiSM2).

**Q.** Can one secondary controller serve as the redundancy pair for multiple primary controllers?

**A.** No. The secondary controller can support only one primary for 1:1 active-standby redundancy.

**Q.** What steps need to be followed if my -HA SKU has a hardware problem and needs to be returned under a return materials authorization (RMA)?

**A.** Any customer that suffers from hardware failure on their wireless LAN controller and has to undergo RMA will receive the -CA SKU in return. Thus, if your -HA SKU needs an RMA, you need to convert the -CA SKU to the -HA SKU using the command “config redundancy unit secondary.” For customers that select the Cisco 5508, please work with the account team to get 50 permanent licenses to enable converting the controller to the -HA SKU.

**Q.** In an environment in which the customer has converted a 5508-50 (or higher) to the -HA SKU, how can we see the original number of licenses?

**A.** There is currently no way to view the number of licenses on a converted -HA unit.

**Q.** What are the recommendations for the network between the primary and secondary controllers connected via RP over Layer 2 VLAN/fiber to achieve client SSO?

**A.** The Layer 2 network for RP connectivity needs to follow these recommendations to ensure appropriate performance in case of a switchover:

- Round-trip time (RTT) latency on the redundancy link: 80 ms or less for the default keep-alive timeout or 80 percent of the configured keep-alive timeout
- Preferred maximum transmission unit (MTU) on the redundancy link: 1500 or above
- Bandwidth on the redundancy link: 60 Mbps or more

**Q.** What types of clients are supported with the subsecond failover?

**A.** Any clients that are successfully authenticated will fail over successfully to the standby controller.

The following information will **not** be copied over from the active to the standby controller, and therefore subsecond stateful failover is **not** supported:

- Proxy Mobil IP (PMIP) v6
- Network Based Application Recognition (NBAR) 2 flow information
- Session Initiation Protocol (SIP) static call admission control (CAC)
- Workgroup Bridge (WGB) and wired/wireless clients associated with it
- OfficeExtend Access Point (OEAP) 600 clients
- Passive clients
- Subsecond failover of mobility anchors to the mobility controller with new mobility is not supported
- Sleeping clients are not supported

**Q.** What is the experience when the primary controller comes back online - will the access points automatically fail over from the standby (which is currently active) to the original active?

**A.** No. The access points will not fail over from the standby (which is currently active) to the original active controller. Customers can move the access points back to the primary whenever their schedule permits, using the force switchover command from the currently active controller.

**Q.** What happens if my access points are connected to the secondary controller for more than 90 days?

**A.** Both in the client SSO as well as the N+1 mode, access points will continue to stay connected, with the user getting daily reminders to move the access points back to the primary.

**Q.** Is there a way to see how many days are left until the 90-day timer expires?

**A.** There is currently no way to see that information.

**Q.** What behavior can I get with the -HA SKU on the Cisco 2504 Wireless Controller (CT2504)?

**A.** Starting 7.5, the HA SKU on the Cisco 2504 can operate only in N+1 mode. It does not support access point or client SSO.

**Q.** Can I rehost licensing from a Cisco 5508 to a Cisco 8510? My customer is pursuing network consolidation.

**A.** Transfer of licenses between two controllers of different models is not supported. The only exception is transfer of licenses between the Cisco IOS based 3850 and 5760 controllers, as described in the separate Q&A: http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps12598/qa_c67-726397.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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



Printed in USA C67-714540-04 2/14