



Configuring High Availability

- [Finding Feature Information, page 1](#)
- [Information about High Availability, page 1](#)
- [Information About Redundancy, page 2](#)
- [Information about Access Point Stateful Switch Over , page 4](#)
- [Initiating Graceful Switchover, page 4](#)
- [Configuring EtherChannels for High Availability, page 5](#)
- [Configuring LACP, page 5](#)
- [Troubleshooting High Availability, page 6](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Information about High Availability

The high availability feature is enabled by default when the controllers are connected using the stack cable and the technology is enabled. You cannot disable it; however, you can initiate a manual graceful-switchover using the command line interface to use the high availability feature enabled in the controller.

In Cisco Wireless LAN Controllers, high availability is achieved with redundancy.

In Cisco Wireless LAN Controllers, redundancy is achieved in two ways— n+1 and AP SSO redundancy.

Keepalive messages are sent and received between the active and standby controllers.

- If the standby controller does not respond, a new standby controller is elected.
- If the active controller does not respond, the standby controller becomes the active controller.

In addition, hello messages are sent and received by all stack members.

- If a stack member does not respond, that member is removed from the stack.
- If the standby controller does not respond, a new standby controller is elected.
- If the active controller does not respond, the standby controller becomes the active controller.

Information About Redundancy

In case of n+1 redundancy, access points are configured with primary, secondary, and tertiary controllers. When the primary controller fails, depending upon the number of access points managed by a controller, the access point fails over to the secondary controller. In case of AP SSO redundancy, once the primary controller is unavailable, the access points re-discover the controller and reestablishes the CAPWAP tunnel with the secondary controller. However, all clients must disconnect and a re-authentication is performed to rejoin the controller.

You can configure primary, secondary, and tertiary controllers for a selected access point and a selected controller.

In an ideal high availability deployment, you can have access points connected to primary and secondary controllers and one controller can remain without connection to any access points. This way the controller that does not have any access points can take over when a failure occurs and resume services of active controller.

Configuring Redundancy in Access Points

You must use the commands explained in this section to configure primary, secondary, or tertiary controllers for a selected access point.

Before You Begin

SUMMARY STEPS

1. `conf t`
2. `ap capwap backup primary`
3. `ap capwap backup secondary`
4. `ap capwap backup tertiary`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>conf t</code> Example: <code>Controller # conf t</code>	Configures the terminal

	Command or Action	Purpose
Step 2	ap capwap backup primary Example: Controller # ap capwap backup primary WLAN-Controller-A	Configures the primary controller for the selected access point.
Step 3	ap capwap backup secondary Example: Controller # ap capwap backup secondary WLAN-Controller-B	Configures the secondary controller for the selected access point.
Step 4	ap capwap backup tertiary Example: Controller # ap capwap backup tertiary WLAN-Controller-C	Configures the tertiary controller for the selected access point.

What to Do Next

Once you complete configuration of the primary, secondary, and tertiary controllers for a selected access point, you must verify the configuration using the **show ap name** *AP-NAME* command. For more details on, **show ap name** *AP-NAME* command, see the Lightweight Access Point Configuration Guide for Cisco Wireless LAN Controller.

.

Configuring Heartbeat Messages

Heartbeat messages enable you to reduce the controller failure detection time. When a failure occurs, a switchover from active to hot standby happens after the controller waits for the heartbeat timer. If the controller does not function within the heartbeat time, then the standby takes over as then active controller. Ideally the access point generates three heartbeat messages within the time out value specified, and when the controller does not respond within the timeout value, the standby controller takes over as active. You can specify the timeout value depending on your network. Ideally the timer value is not a higher value as some chaos will occur while performing a switchover. This section explains on how to configure heartbeat interval between the controller and the access points using a timeout value to reduce the controller failure detection time.

Before You Begin

SUMMARY STEPS

1. conf t
2. ap capwap timers heartbeat-timeout

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>conf t</code> Example: <code>controller # conf t</code>	Configures the terminal.
Step 2	<code>ap capwap timers heartbeat-timeout</code> Example: <code>controller # ap capwap timers heartbeat-timeout</code>	Configures the heartbeat interval between the controller and access points. The timeout value ranges from 1 to 30.

Information about Access Point Stateful Switch Over

An Access Point Stateful Switch Over (AP SSO) implies that all the access point sessions are switched over state-fully and the user session information is maintained during a switchover, and access points continue to operate in network with no loss of sessions, providing improved network availability. The active controller in the stack is equipped to perform all network functions, including IP functions and routing information exchange. The controller supports 1000 access points and 12000 clients.

However, all the clients are de-authenticated and need to be re-associated with the new active controller except for the locally switched clients in FlexConnect mode when a switchover occurs.

Once a redundancy pair is formed while in a stack, high availability is enabled, which includes that access points continue to remain connected during an active-to-standby switchover.

**Note**

You can not disable AP SSO while in a controller stack once the controllers form a redundant pair.

Initiating Graceful Switchover

To perform a manual switchover and to use the high availability feature enabled in the controller, execute the **redundancy force-switchover** command. This command initiates a graceful switchover from the active to the standby controller.

```
Controller# redundancy force-switchover
System configuration has been modified. Save ? [yes/no] : yes
Building configuration ...
Preparing for switchover ...
Compressed configuration from 14977 bytes to 6592 bytes[OK]This will reload the active unit
and force switchover to standby[confirm] : y
```

Configuring EtherChannels for High Availability

The LAG, or an EtherChannel, bundles all the existing ports in both the standby and active units into a single logical port to provide an aggregate bandwidth of 60 Gbps. The creation of an EtherChannel enables protection against failures. The EtherChannels or LAGs created are used for link redundancy to ensure high availability of access points.

For more details on configuring EtherChannel, and Etherchannel modes, see the [Layer 2 \(Link Aggregation\) Configuration Guide, Cisco IOS XE Release 3SE \(Cisco WLC 5700 Series\)](#)

-
- | | |
|---------------|---|
| Step 1 | Connect two controllers that are in powered down state using the stack cable. |
| Step 2 | Power up and perform a boot on both controllers simultaneously or power and boot one controller. The controllers boot up successfully, and form a high availability pair. |
| Step 3 | Configure EtherChannel or LAG on the units. |
| Step 4 | Use the show etherchannel summary command to view the status of the configured EtherChannel. On successful configuration, all the specified ports will be bundled in a single channel and listed in the command output of show etherchannel summary . |
| Step 5 | Execute the show ap uptime command to verify the connected access points. |
-

Configuring LACP

SUMMARY STEPS

1. **configure terminal**
2. **interface port-channel** *number*
3. **lacp max-bundle** *number*
4. **lacp port-priority** *number*
5. **switchport backup interface** *po2*
6. **end**
7. **show etherchannel summary**
8. **show interfaces switchport backup**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.
	Example: Controller# configure terminal	

	Command or Action	Purpose
Step 2	interface port-channel <i>number</i> Example: Controller(config)# interface Port-channel Po2	Enters port-channel interface configuration mode.
Step 3	lacp max-bundle <i>number</i> Example: Controller(config-if)# lacp max-bundle 6	Defines the maximum number of active bundled LACP ports allowed in a port channel. The value ranges from 1 to 8.
Step 4	lacp port-priority <i>number</i> Example: Controller(config-if)# lacp port-priority 4	Specifies port priority to be configured on the port using LACP. The value ranges from 0 to 65535.
Step 5	switchport backup interface <i>po2</i> Example: Controller(config-if)# switchport backup interface Po2	Specifies an interface as the backup interface.
Step 6	end	Exits the interface and configuration mode.
Step 7	show etherchannel summary Example: Controller# show etherchannel summary	Displays a summary of EtherChannel properties.
Step 8	show interfaces switchport backup Example: Controller# show interfaces switchport backup	Displays summary of backup EtherChannel properties.

Troubleshooting High Availability

Access the Standby Console

You can only access the console of the active controller in a stack. To access the standby controller, use the following commands.

Before You Begin

Use this functionality only under supervision of Cisco Support.

SUMMARY STEPS

1. **configure terminal**
2. **service internal**
3. **redundancy**
4. **main-cpu**
5. **standby console enable**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Controller# configure terminal	Enters global configuration mode.
Step 2	service internal Example: Controller(config)# service internal	Enables Cisco IOS debug commands.
Step 3	redundancy Example: Controller(config)# redundancy	Enters redundancy configuration mode.
Step 4	main-cpu Example: Controller(config)# main-cpu	Enters the redundancy main configuration submenu.
Step 5	standby console enable Example: Controller(config)# standby console enable	Enables the standby console.
Step 6	exit Example: Controller(config)# exit	Exits the configuration mode.

Before a Switchover

A switchover happens when the active controller fails; however, while performing a manual switchover, you can execute these commands to initiate a successful switchover:

SUMMARY STEPS

1. show redundancy states
2. show switch detail
3. show platform ses states
4. show ap summary
5. show capwap detail
6. show dtls database-brief
7. show power inline

DETAILED STEPS

	Command or Action	Purpose
Step 1	show redundancy states Example: Controller# <code>show redundancy states</code>	Displays the high availability role of the active and standby controllers.
Step 2	show switch detail Example: Controller# <code>show switch detail</code>	Display physical property of the stack. Verify if the physical states of the stacks are "Ready" or "Port".
Step 3	show platform ses states Example: Controller# <code>show platform ses states</code>	Displays the sequences of the stack manager.
Step 4	show ap summary Example: Controller# <code>show ap summary</code>	Displays all the access points in the active and standby controllers.
Step 5	show capwap detail Example: Controller# <code>show capwap detail</code>	Displays the details of the CAPWAP tunnel in the active and standby controllers.
Step 6	show dtls database-brief Example: Controller# <code>show dtls database-brief</code>	Displays DTLS details in the active and standby controllers.
Step 7	show power inline Example: Controller# <code>show power inline</code>	Displays the power on Ethernet power state. Note When a failover occurs, the standby controller must be in a standby-hot state and the redundant port in a terminal state in SSO for successful switchover to occur.

After a Switchover

This section defines the steps that you must perform to ensure that successful switchover from the active to standby controller is performed. On successful switchover of the standby controller as active, all access points connected to the active need to re-join the standby (then active) controller.

SUMMARY STEPS

1. `show ap uptime`
2. `show wireless summary`
3. `show wcdb database all`
4. `show power inline`

DETAILED STEPS

	Command or Action	Purpose
Step 1	show ap uptime Example: Controller# <code>show ap uptime</code>	Verify if the uptime of the access point after the switchover is large enough.
Step 2	show wireless summary Example: Controller# <code>show wireless summary</code>	Display the clients connected in the active controller.
Step 3	show wcdb database all Example: Controller# <code>show wcdb database all</code>	Display if the client has reached the uptime.
Step 4	show power inline Example: Controller# <code>show power inline</code>	Display the power over Ethernet power state.

Viewing Redundancy Switchover History (GUI)

Step 1

Click **Monitor > Controller > Redundancy > States**.

The Redundancy States page is displayed. The values for the following parameters are displayed in the page:

Parameter	Description
Index	Displays the index number of the of the redundant unit.

Parameter	Description
Previous Active	Displays the Controllers that was active before.
Current Active	Displays the Controllers that is currently active.
Switch Over Time	Displays the system time when the switchover occurs.
Switch Over Reason	Displays the cause of the switchover.

Step 2 Click **Apply**.

Viewing Switchover States (GUI)

Step 1 Click **Monitor > Controller > Redundancy > States**.
The Redundancy States page is displayed. The values for the following parameters are displayed in the page:

Parameter	Description
My State	Shows the state of the active CPU Controller module. Values are as follows: <ul style="list-style-type: none"> • Active • Standby HOT • Disable
Peer State	Displays the state of the peer (or standby) CPU Controller module. Values are as follows: <ul style="list-style-type: none"> • Standby HOT • Disable
Mode	Displays the current state of the redundancy peer. Values are as follows: <ul style="list-style-type: none"> • Simplex— Single CPU switch module • Duplex— Two CPU switch modules
Unit ID	Displays the unit ID of the CPU switch module.
Redundancy Mode (Operational)	Displays the current operational redundancy mode supported on the unit.
Redundancy Mode (Configured)	Displays the current configured redundancy mode supported on the unit.

Parameter	Description
Redundancy State	Displays the current functioning redundancy state of the unit. Values are as follows: <ul style="list-style-type: none"> • SSP • Not Redundant
Manual SWACT	Displays whether manual switchovers have been enabled without the force option.
Communications	Displays whether communications are up or down between the two CPU Controller modules.
Client Count	Displays the number of redundancy subsystems that are registered as RF clients.
Client Notification TMR	Displays, in milliseconds, the time that an internal RF timer has for notifying RF client subsystems.
Keep Alive TMR	Displays, in milliseconds, the time interval the RF manager has for sending keep-alive messages to its peer on the standby CPU switch module.
Keep Alive Count	Displays the number of keep-alive messages sent without receiving a response from the standby CPU Controller module.
Keep Alive Threshold	Displays the threshold for declaring that interprocessor communications are down when keep-alive messages have been enabled (which is the default).
RF Debug Mask	Displays an internal mask used by the RF to keep track of which debug modes are on.

Step 2 Click **Apply**.

Monitoring the Controller Stack

Table 1: Commands for Displaying Stack Information

Command	Description
show switch	Displays summary information about the stack, including the status of provisioned switches and switches in version-mismatch mode.
show switch <i>stack-member-number</i>	Displays information about a specific member.
show switch detail	Displays detailed information about the stack.
show switch neighbors	Displays the stack neighbors.
show switch stack-ports	Displays port information for the stack.

Command	Description
show redundancy	Displays the redundant system and the current processor information. The redundant system information includes the system uptime, standby failures, switchover reason, hardware, configured and operating redundancy mode. The current processor information displayed includes the active location, the software state, the uptime in the current state and so on.
show redundancy state	Displays all the redundancy states of the active and standby controllers.

LACP Configuration: Example

This example shows how to configure LACP and to verify creation of the LACP bundle and the status:

```

Controller(config)# !
interface TenGigabitEthernet1/0/1
  switchport mode trunk
  channel-group 1 mode active
  lacp port-priority 10
  ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/2
  switchport mode trunk
  channel-group 1 mode active
  lacp port-priority 10
  ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/3
  switchport mode trunk
  channel-group 1 mode active
  lacp port-priority 10
  ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/4
  switchport mode trunk
  channel-group 1 mode active
  ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/5
  switchport mode trunk
  channel-group 1 mode active
  ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/6
  switchport mode trunk
  channel-group 1 mode active
  ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/1
  switchport mode trunk
  channel-group 1 mode active
  lacp port-priority 10
  ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/2
  switchport mode trunk
  channel-group 1 mode active
  lacp port-priority 10

```

```

ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/3
 switchport mode trunk
 channel-group 1 mode active
 lacp port-priority 10
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/4
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/5
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/6
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface Vlan1
 no ip address
 ip igmp version 1
 shutdown
!

```

Controller# **show etherchannel summary**

```

Flags:  D - down          P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3        S - Layer2
        U - in use        f - failed to allocate aggregator

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

```

```

Number of channel-groups in use: 1
Number of aggregators:          1

```

Group	Port-channel	Protocol	Ports
1	Pol (SU)	LACP	Te1/0/1 (P) Te1/0/2 (P) Te1/0/3 (P) Te1/0/4 (H) Te1/0/5 (H) Te1/0/6 (H) Te2/0/1 (P) Te2/0/2 (P) Te2/0/3 (P) Te2/0/4 (H) Te2/0/5 (H) Te2/0/6 (H)

This example shows the switch backup interface pairs:

Controller# show interfaces switchport backup

Switch Backup Interface Pairs:

Active Interface	Backup Interface	State
Port-channel1	Port-channel2	Active Standby/Backup Up

This example shows the summary of the EtherChannel configured in the controller:

Controller# show ethernet summary

```

Flags:  D - down          P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3        S - Layer2
        U - in use        f - failed to allocate aggregator

```

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

Number of channel-groups in use: 2
 Number of aggregators: 2

Group	Port-channel	Protocol	Ports		
1	Po1 (SU)	LACP	Te1/0/1 (P)	Te1/0/2 (P)	Te1/0/3 (P)
			Te1/0/4 (P)	Te1/0/5 (P)	Te1/0/6 (P)
2	Po2 (SU)	LACP	Te2/0/1 (P)	Te2/0/2 (P)	Te2/0/3 (P)
			Te2/0/4 (P)	Te2/0/5 (P)	Te2/0/6 (P)

Flex Link Configuration: Example

This example shows how to configure flex link and to verify creation and the status of the created link:

```

Controller(config)# !
interface Port-channel1
  description Ports 1-6 connected to NW-55-SW
  switchport mode trunk
  switchport backup interface Po2
  switchport backup interface Po2 preempt mode forced
  switchport backup interface Po2 preempt delay 1
  ip dhcp snooping trust
!
interface Port-channel2
  description Ports 7-12connected to NW-55-SW
  switchport mode trunk
  ip dhcp snooping trust
!
interface GigabitEthernet0/0
  vrf forwarding Mgmt-vrf
  no ip address
  negotiation auto
!
interface TenGigabitEthernet1/0/1
  switchport mode trunk
  channel-group 1 mode on
  ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/2
  switchport mode trunk
  channel-group 1 mode on
  ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/3
  switchport mode trunk
  channel-group 1 mode on
  ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/4
  switchport mode trunk
  channel-group 1 mode on
  ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/5
  switchport mode trunk
  channel-group 1 mode on
  ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/6
  switchport mode trunk
  channel-group 1 mode on
  ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/1

```

```

switchport mode trunk
channel-group 2 mode on
ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/2
switchport mode trunk
channel-group 2 mode on
ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/3
switchport mode trunk
channel-group 2 mode on
ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/4
switchport mode trunk
channel-group 2 mode on
ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/5
switchport mode trunk
channel-group 2 mode on
ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/6
switchport mode trunk
channel-group 2 mode on
ip dhcp snooping trust
!
interface Vlan1
no ip address

```

Controller# **show etherchannel summary**

```

Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator

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

```

```

Number of channel-groups in use: 2
Number of aggregators:          2

```

Group	Port-channel	Protocol	Ports
1	Po1 (SU)	-	Te1/0/1 (P) Te1/0/2 (P) Te1/0/3 (P) Te1/0/4 (P) Te1/0/5 (P) Te1/0/6 (P)
2	Po2 (SU)	-	Te2/0/1 (P) Te2/0/2 (P) Te2/0/3 (D) Te2/0/4 (P) Te2/0/5 (P) Te2/0/6 (P)

