High Availability Configuration Guide, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)

First Published: 0,

Last Modified: 0,

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-32316-01

CONTENTS

Preface

Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands and keywords and user-entered text appear in **bold** font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`Courier` font	Terminal sessions and information the system displays appear in `courier` font.
`Bold Courier` font	**`Bold Courier`** font indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x | y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Convention	Description
{x | y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document may use the following conventions for reader alerts:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means *the following information will help you solve a problem.*

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time.* You can save time by performing the action described in the paragraph.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Related Documentation

Note Before installing or upgrading the controller, refer to the controller release notes.

- Cisco 5700 Series Wireless Controller documentation, located at:

  http://www.cisco.com/go/wlc5700_sw

- Cisco Validated Designs documents, located at:

  http://www.cisco.com/go/designzone

- Error Message Decoder, located at:

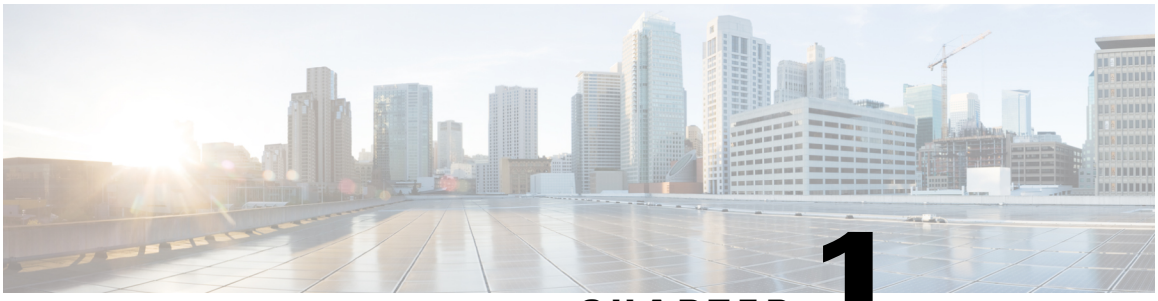
  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

Using the Command-Line Interface

Information About Using the Command-Line Interface

Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

You can start a CLI session through a console connection, through Telnet, a SSH, or by using the browser.

When you start a session, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the controller reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the controller reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

This table describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode.

Table 1: Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session using Telnet, SSH, or console.	`Controller>`	Enter **logout** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	While in user EXEC mode, enter the **enable** command.	`Controller#`	Enter **disable** to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode. Use this mode to execute privilege EXEC commands for access points. These commands are not part of the running config of the controller, they are sent to the IOS config of the access point.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	`Controller(config)#`	To exit to privileged EXEC mode, enter **exit** or **end**, or press **Ctrl-Z**.	Use this mode to configure parameters that apply to the entire controller. Use this mode to configure access point commands that are part of the running config of the controller.
VLAN configuration	While in global configuration mode, enter the **vlan** *vlan-id* command.	`Controller(config-vlan)#`		

Mode	Access Method	Prompt	Exit Method	About This Mode
			To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the controller startup configuration file.
Interface configuration	While in global configuration mode, enter the **interface** command (with a specific interface).	`Controller(config-if)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure parameters for the Ethernet ports.
Line configuration	While in global configuration mode, specify a line with the **line vty** or **line console** command.	`Controller(config-line)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure parameters for the terminal line.

Using the Help System

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command.

SUMMARY STEPS

1. **help**
2. *abbreviated-command-entry* **?**
3. *abbreviated-command-entry* <Tab>
4. **?**
5. *command* **?**
6. *command keyword* **?**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**help** **Example:** `Controller# help`	Obtains a brief description of the help system in any command mode.

Step 2	*abbreviated-command-entry* **?**
	
	Example:
	`Controller# di?`
	`dir disable disconnect`
		Obtains a list of commands that begin with a particular character string.

Step 3	*abbreviated-command-entry* <Tab>
	
	Example:
	`Controller# sh conf<tab>`
	`Controller# show configuration`
		Completes a partial command name.

Step 4	**?** **Example:** `Controller> ?`	Lists all commands available for a particular command mode.
Step 5	*command* **?** **Example:** `Controller> show ?`	Lists the associated keywords for a command.

Step 6	*command keyword* **?**
	
	Example:
	`Controller(config)# cdp holdtime ?`
	`<10-255> Length of time (in sec) that receiver must keep this packet`
		Lists the associated arguments for a keyword.

Understanding Abbreviated Commands

You need to enter only enough characters for the controller to recognize the command as unique.

This example shows how to enter the **show configuration** privileged EXEC command in an abbreviated form:

```
Controller# show conf
```

No and Default Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to reenable a disabled feature or to enable a feature that is disabled by default.

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command enables the command and sets variables to their default values.

CLI Error Messages

This table lists some error messages that you might encounter while using the CLI to configure your controller.

Table 2: Common CLI Error Messages

Error Message	Meaning	How to Get Help
`% Ambiguous command: "show con"`	You did not enter enough characters for your controller to recognize the command.	Reenter the command followed by a question mark (?) without any space between the command and the question mark. The possible keywords that you can enter with the command appear.
`% Incomplete command.`	You did not enter all of the keywords or values required by this command.	Reenter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
`% Invalid input detected at '^' marker.`	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all of the commands that are available in this command mode. The possible keywords that you can enter with the command appear.

Configuration Logging

You can log and view changes to the controller configuration. You can use the Configuration Change Logging and Notification feature to track changes on a per-session and per-user basis. The logger tracks each configuration command that is applied, the user who entered the command, the time that the command was entered, and the parser return code for the command. This feature includes a mechanism for asynchronous notification to registered applications whenever the configuration changes. You can choose to have the notifications sent to the syslog.

Note Only CLI or HTTP changes are logged.

How to Use the CLI to Configure Features

Configuring the Command History

The software provides a history or record of commands that you have entered. The command history feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize this feature to suit your needs.

Changing the Command History Buffer Size

By default, the controller records ten command lines in its history buffer. You can alter this number for a current terminal session or for all sessions on a particular line. This procedure is optional.

SUMMARY STEPS

1. **terminal history** [**size** *number-of-lines*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**terminal history** [**size** *number-of-lines*] **Example:** `Controller# terminal history size 200`	Changes the number of command lines that the controller records during the current terminal session in privileged EXEC mode. You can configure the size from 0 to 256.

Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in this table. These actions are optional.

Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

SUMMARY STEPS

1. **Ctrl-P** or use the **up arrow** key
2. **Ctrl-N** or use the **down arrow** key
3. **show history**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**Ctrl-P** or use the **up arrow** key	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Step 2	**Ctrl-N** or use the **down arrow** key	Returns to more recent commands in the history buffer after recalling commands with **Ctrl-P** or the up arrow key. Repeat the key sequence to recall successively more recent commands.
Step 3	**show history** **Example:** `Controller# show history`	Lists the last several commands that you just entered in privileged EXEC mode. The number of commands that appear is controlled by the setting of the **terminal history** global configuration command and the **history** line configuration command.

Disabling the Command History Feature

The command history feature is automatically enabled. You can disable it for the current terminal session or for the command line. This procedure is optional.

SUMMARY STEPS

1. **terminal no history**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**terminal no history** **Example:** `Controller# terminal no history`	Disables the feature during the current terminal session in privileged EXEC mode.

Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it and reenable it.

SUMMARY STEPS

1. **terminal editing**
2. **terminal no editing**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**terminal editing** **Example:** `Controller# terminal editing`	Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.
Step 2	**terminal no editing** **Example:** `Controller# terminal no editing`	Disables the enhanced editing mode for the current terminal session in privileged EXEC mode.

Editing Commands Through Keystrokes

The keystrokes help you to edit the command lines. These keystrokes are optional.

Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

Table 3: Editing Commands

Editing Commands	Description

Ctrl-B or use the **left arrow** key	Moves the cursor back one character.
Ctrl-F or use the **right arrow** key	Moves the cursor forward one character.
Ctrl-A	Moves the cursor to the beginning of the command line.
Ctrl-E	Moves the cursor to the end of the command line.
Esc B	Moves the cursor back one word.
Esc F	Moves the cursor forward one word.
Ctrl-T	Transposes the character to the left of the cursor with the character located at the cursor.
Delete or **Backspace** key	Erases the character to the left of the cursor.
Ctrl-D	Deletes the character at the cursor.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.
Ctrl-U or **Ctrl-X**	Deletes all characters from the cursor to the beginning of the command line.
Ctrl-W	Deletes the word to the left of the cursor.
Esc D	Deletes from the cursor to the end of the word.
Esc C	Capitalizes at the cursor.
Esc L	Changes the word at the cursor to lowercase.
Esc U	Capitalizes letters from the cursor to the end of the word.
Ctrl-V or **Esc Q**	Designates a particular keystroke as an executable command, perhaps as a shortcut.
Return key	Scrolls down a line or screen on displays that are longer than the terminal screen can display. **Note** The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including **show** command output. You can use the **Return** and **Space** bar keystrokes whenever you see the More prompt.
Space bar	Scrolls down one screen.

Ctrl-L or **Ctrl-R**	Redisplays the current command line if the controller suddenly sends a message to your screen.

Editing Command Lines That Wrap

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command. The keystroke actions are optional.

To scroll back to the beginning of the command entry, press **Ctrl-B** or the left arrow key repeatedly. You can also press **Ctrl-A** to immediately move to the beginning of the line.

Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

The following example shows how to wrap a command line that extends beyond a single line on the screen.

SUMMARY STEPS

1. **access-list**
2. **Ctrl-A**
3. **Return** key

DETAILED STEPS

	Command or Action	Purpose

Step 1	**access-list**
	
	Example:
	`Controller(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35`
	`Controller(config)# $ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25`
	`Controller(config)# $t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq`
	`Controller(config)# $15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45`
		Displays the global configuration command entry that extends beyond one line.
		
		When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign ($) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.

Step 2	**Ctrl-A** **Example:** `Controller(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2$`	Checks the complete syntax. The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right.
Step 3	**Return** key	Execute the commands.

	Command or Action	Purpose
		The software assumes that you have a terminal screen that is 80 columns wide. If you have a different width, use the **terminal width** privileged EXEC command to set the width of your terminal. Use line wrapping with the command history feature to recall and modify previous complex command entries.

Searching and Filtering Output of show and more Commands

You can search and filter the output for **show** and **more** commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see. Using these commands is optional.

SUMMARY STEPS

1. {**show** | **more**} *command* | {**begin** | **include** | **exclude**} *regular-expression*

DETAILED STEPS

	Command or Action	Purpose
Step 1	{**show**	**more**} *command*	{**begin**	**include**	**exclude**} *regular-expression* **Example:** `Controller# show interfaces	include protocol` `Vlan1 is up, line protocol is up` `Vlan10 is up, line protocol is down` `GigabitEthernet1/0/1 is up, line protocol is down` `GigabitEthernet1/0/2 is up, line protocol is up`	Searches and filters the output. Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain **output** are not displayed, but the lines that contain **output** appear.

Accessing the CLI Through a Console Connection or Through Telnet

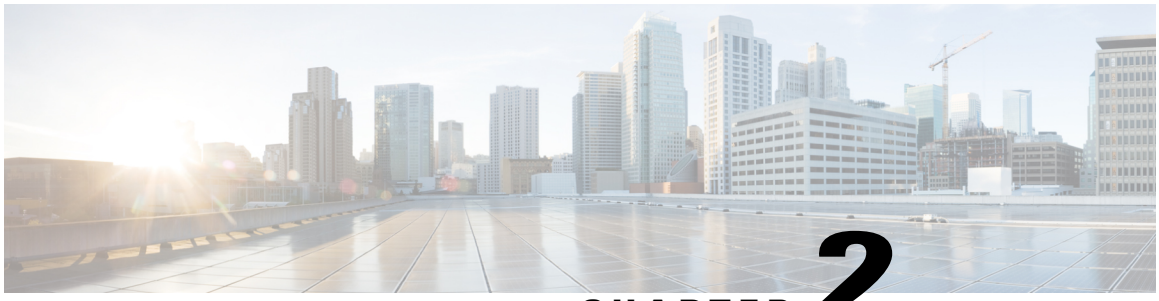
Before you can access the CLI, you must connect a terminal or a PC to the controller console or connect a PC to the Ethernet management port and then power on the controller, as described in the hardware installation guide that shipped with your controller.

If your controller is already configured, you can access the CLI through a local console connection or through a remote Telnet session, but your controller must first be configured for this type of access.

You can use one of these methods to establish a connection with the controller:

- Connect the controller console port to a management station or dial-up modem, or connect the Ethernet management port to a PC. For information about connecting to the console or Ethernet management port, see the controller hardware installation guide.
- Use any Telnet TCP/IP or encrypted Secure Shell (SSH) package from a remote management station. The controller must have network connectivity with the Telnet or SSH client, and the controller must have an enable secret password configured.
    - The controller supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.
    - The controller supports up to five simultaneous secure SSH sessions.

  After you connect through the console port, through the Ethernet management port, through a Telnet session or through an SSH session, the user EXEC prompt appears on the management station.



CHAPTER 2

Using the Web Graphical User Interface

Prerequisites for Using the Web GUI

- The GUI must be used on a PC running Windows 7, Windows XP SP1 (or later releases), or Windows 2000 SP4 (or later releases).
- The controller GUI is compatible with Microsoft Internet Explorer version 10.x, Mozilla Firefox 20.x, or Google Chrome 26.x.

Information About Using The Web GUI

A web browser, or graphical user interface (GUI), is built into each controller.

You can use either the service port interface or the management interface to access the GUI. We recommend that you use the service-port interface. Click Help at the top of any page in the GUI to display online help. You might need to disable your browser's pop-up blocker to view the online help.

Web GUI Features

The controller web GUI supports the following:

The Configuration Wizard—After initial configuration of the IP address and the local username/password or auth via the authentication server (privilege 15 needed), the wizard provides a method to complete the initial

wireless configuration. Start the wizard through Configuration -> Wizard and follow the nine-step process to configure the following:

- Admin Users
- SNMP System Summary
- Management Port
- Wireless Management
- RF Mobility and Country code
- Mobility configuration
- WLANs
- 802.11 Configuration
- Set Time

The Monitor tab:

- Displays summary details of controller, clients, and access points.
- Displays all radio and AP join statistics.
- Displays air quality on access points.
- Displays list of all Cisco Discovery Protocol (CDP) neighbors on all interfaces and the CDP traffic information.
- Displays all rogue access points based on their classification-friendly, malicious, ad hoc, classified, and unclassified.

The Configuration tab:

- Enables you to configure the controller for all initial operation using the web Configuration Wizard. The wizard allows you to configure user details, management interface, and so on.
- Enables you to configure the system, internal DHCP server, management, and mobility management parameters.
- Enables you to configure the controller, WLAN, and radios.
- Enables you to configure and set security policies on your controller.
- Enables you to access the controller operating system software management commands.

The Administration tab enables you to configure system logs.

Connecting the Console Port of the Controller

Before You Begin

Before you can configure the controller for basic operations, you need to connect it to a PC that uses a VT-100 terminal emulation program (such as HyperTerminal, ProComm, Minicom, or Tip).

Step 1 Connect one end of a null-modem serial cable to the controller's RJ-45 console port and the other end to your PC's serial port.

Step 2 Plug the AC power cord into the controller and a grounded 100 to 240 VAC, 50/60-Hz electrical outlet. Turn on the power supply. The bootup script displays operating system software initialization (code download and power-on self-test verification) and basic configuration. If the controller passes the power-on self-test, the bootup script runs the configuration wizard, which prompts you for basic configuration input.

Step 3 Enter **yes**. Proceed with basic initial setup configuration parameters in the CLI setup wizard. Specify the IP address for the service port which is the gigabitethernet 0/0 interface.
After entering the configuration parameters in the configuration wizard, you can access the Web GUI. Now, the controller is configured with the IP address for service port.

Logging On to the Web GUI

Step 1 Enter the controller IP address in your browser's address bar. For a secure connection, enter https://**ip-address**. For a less secure connection, enter http://**ip-address**.

Step 2 When prompted, enter a valid username and password, and click **OK**.
The **Summary** page is displayed.

Note The administrative username and password that you created in the configuration wizard are case sensitive. The default username is admin, and the default password is admin.

Step 3 When prompted, enter a valid username and password and click **OK**.

Note The administrative username and password that you created in the configuration wizard are case sensitive. The default username is admin, and the default password is cisco.

The Accessing page appears.

Enabling Web and Secure Web Modes

Step 1 Choose **Configuration** > **Controller** > **Management** > **Protocol Management** > **HTTP-HTTPS**.

The **HTTP-HTTPS Configuration** page appears.

Step 2 To enable web mode, which allows users to access the controller GUI using "http://ip-address," choose Enabled from the HTTP Access drop-down list. Otherwise, choose Disabled. Web mode (HTTP) is not a secure connection.

Step 3 To enable secure web mode, which allows users to access the controller GUI using "https://ip-address," choose Enabled from the HTTPS Access drop-down list. Otherwise, choose Disabled. Secure web mode (HTTPS) is a secure connection.

Step 4 Choose to track the device in the IP Device Tracking check box.

Step 5 Choose to enable the trust point in the Enable check box.

Step 6 Choose the trustpoints from the Trustpoints drop-down list.

Step 7 Enter the amount of time, in seconds, before the web session times out due to inactivity in the HTTP Timeout-policy (1 to 600 sec) text box.
The valid range is from 1 to 600 seconds.

Step 8 Enter the server life time in the Server Life Time (1 to 86400 sec) text box.
The valid range is from1 to 86400 seconds.

Step 9 Enter the maximum number of connection requests that the server can accept in the Maximum number of Requests (1 to 86400) text box.
The valid range is from 1 to 86400 connections.

Step 10 Click **Apply**.

Step 11 Click **Save Configuration**.

Configuring the Controller Web GUI

The configuration wizard enables you to configure basic settings on the controller. You can run the wizard after you receive the controller from the factory or after the controller has been reset to factory defaults. The configuration wizard is available in both GUI and CLI formats.

Step 1 Connect your PC to the service port and configure an IPv4 address to use the same subnet as the controller. The controller is loaded with IOS XE image and the service port interface is configured as gigabitethernet 0/0.

Step 2 Start Internet Explorer 10 (or later), Firefox 2.0.0.11 (or later), or Google Chrome on your PC and enter the management interface IP address on the browser window. The management interface IP address is same as the gigabitethernet 0/0 (also known as service port interface). When you log in for the first time, you need to enter HTTP username and password. By default, the username is **admin** and the password is **cisco**.
You can use both HTTP and HTTPS when using the service port interface. HTTPS is enabled by default and HTTP can also be enabled.

When you log in for the first time, the **Accessing Cisco Controller <Model Number> <Hostname>** page appears.

Step 3 On the **Accessing Cisco Controller** page, click the **Wireless Web GUI** link to access controller web GUI **Home** page.

Step 4 Choose **Configuration** > **Wizard** to perform all steps that you need to configure the controller initially.

The **Admin Users** page appears.

Step 5 On the **Admin Users** page, enter the administrative username to be assigned to this controller in the User Name text box and the administrative password to be assigned to this controller in the Password and Confirm Password text boxes. Click **Next**.
The default username is **admin** and the default password is **cisco**. You can also create a new administrator user for the controller. You can enter up to 24 ASCII characters for username and password.

The **SNMP System Summary** page appears.

Step 6 On the **SNMP System Summary** page, enter the following SNMP system parameters for the controller, and click **Next**:

- Customer-definable controller location in the Location text box.
- Customer-definable contact details such as phone number with names in the Contact text box.
- Choose **enabled** to send SNMP notifications for various SNMP traps or **disabled** not to send SNMP notifications for various SNMP traps from the SNMP Global Trap drop-down list.
- Choose **enabled** to send system log messages or **disabled** not to send system log messages from the SNMP Logging drop-down list.

Note The SNMP trap server, must be reachable through the distribution ports (and not through the gigabitethernet0/0 service or management interface).

The **Management Port** page appears.

Step 7 In the **Management Port** page, enter the following parameters for the management port interface (gigabitethernet 0/0) and click **Next**.

- Interface IP address that you assigned for the service port in the IP Address text box.
- Network mask address of the management port interface in the Netmask text box.
- The IPv4 Dynamic Host Configuration Protocol (DHCP) address for the selected port in the IPv4 DHCP Server text box.

The **Wireless Management** page appears.

Step 8 In the **Wireless Management** page, enter the following wireless interface management details, and click **Next**.

- Choose the interface—VLAN, or Ten Gigabit Ethernet from the Select Interface drop-down list.
- VLAN tag identifier, or 0 for no VLAN tag in the VLAN id text box.
- IP address of wireless management interface where access points are connected in the IP Address text box.
- Network mask address of the wireless management interface in the Netmask text box.
- DHCP IPv4 IP address in the IPv4 DHCP Server text box.

When selecting VLAN as interface, you can specify the ports as –Trunk or Access ports from the selected list displayed in the Switch Port Configuration text box.

The **RF Mobility and Country Code** page appears.

Step 9 In the **RF Mobility and Country Code** page, enter the RF mobility domain name in the RF Mobility text box, choose current country code from the Country Code drop-down list, and click **Next**. From the GUI, you can select only one country code.

Note Before configuring RF grouping parameters and mobility configuration, ensure that you refer to the relevant conceptual content and then proceed with the configuration.

The **Mobility Configuration** page with mobility global configuration settings appears.

Step 10 In the **Mobility Configuration** page, view and enter the following mobility global configuration settings, and click **Next**.

- Displays Mobility Controller in the Mobility Role text box.
- Displays mobility protocol port number in the Mobility Protocol Port text box.
- Displays the mobility group name in the Mobility Group Name text box.
- Displays whether DTLS is enabled in the DTLS Mode text box.

  DTLS is a standards-track Internet Engineering Task Force (IETF) protocol based on TLS.
- Displays mobility domain identifier for 802.11 radios in the Mobility Domain ID for 802.11 radios text box.
- Displays the number of members configured on the controller in the Mobility Domain Member Count text box.
- To enable the controller as a Mobility Oracle, select the Mobility Oracle Enabled check box.

  Note Only the controller can be configured as Mobility Oracle. You cannot configure the switch as Mobility Oracle.

  The Mobility Oracle is optional, it maintains the client database under one complete mobility domain.
- The amount of time (in seconds) between each ping request sent to an peer controller in the Mobility Keepalive Interval (1-30)sec text box.

  Valid range is from 1 to 30 seconds, and the default value is 10 seconds.
- Number of times a ping request is sent to an peer controller before the peer is considered to be unreachable in the Mobility Keepalive Count (3-20) text box.

  The valid range is from 3 to 20, and the default value is 3.
- The DSCP value that you can set for the mobility controller in the Mobility Control Message DSCP Value (0-63) text box.

  The valid range is 0 to 63, and the default value is 0.

The **WLANs** page appears.

Step 11 In the **WLANs** page, enter the following WLAN configuration parameters, and click **Next**.

- WLAN identifier in the WLAN ID text box.
- SSID of the WLAN that the client is associated with in the SSID text box.
- Name of the WLAN used by the client in the Profile Name text box.

The **802.11 Configuration** page appears.

Step 12 In the **802.11 Configuration** page, check either one or both 802.11a/n/ac and 802.11b/g/n check boxes to enable the 802.11 radios, and click **Next**.
The **Set Time** page appears.

Step 13 In the **Set Time** page, you can configure the time and date on the controller based on the following parameters, and click **Next**.

- Displays current timestamp on the controller in the Current Time text box.

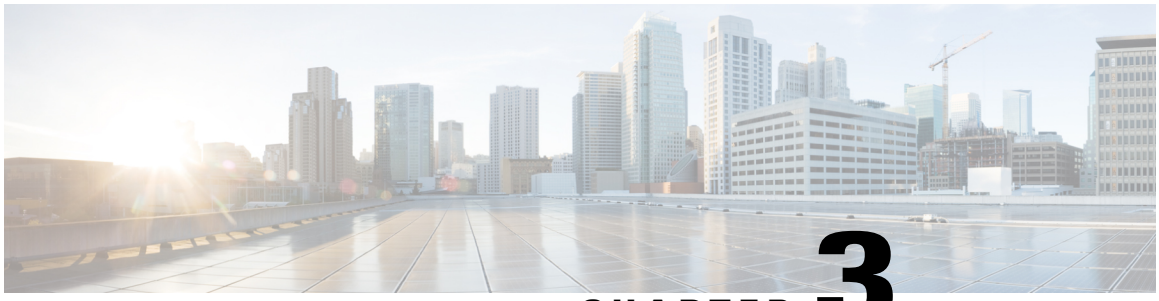
- Choose either Manual or NTP from the Mode drop-down list.

  On using the NTP server, all access points connected to the controller, synchronizes its time based on the NTP server settings available.

- Choose date on the controller from the Year, Month, and Day drop-down list.
- Choose time from the Hours, Minutes, and Seconds drop-down list.
- Enter the time zone in the Zone text box and select the off setting required when compared to the current time configured on the controller from the Offset drop-down list.

The **Save Wizard** page appears.

Step 14 In the **Save Wizard** page, you can review the configuration settings performed on the controller using these steps, and if you wish to change any configuration value, click **Previous** and navigate to that page.
You can save the controller configuration created using the wizard only if a success message is displayed for all the wizards. If the **Save Wizard** page displays errors, you must recreate the wizard for initial configuration of the controller.



CHAPTER 3

Managing Controller Stacks

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.

Pre-requisites for Configuring Controller Stack

You must ensure the following before stacking controllers:

- Ensure that the controllers are connected using the stack cable. For more details on stack cables used, see the Information on Controller stack section.
- Only one controller other than the active unit is available to be stacked.
- Identify which controller needs to be in active and standby state based on your priorities.
- You must verify that the controllers in the stack run on Cisco IOS Software release 3.3 and later.
- You must verify that the licenses of the controllers in the stack; for more details, see the Cisco 5700 Series Wireless Controller Installation Guide.

- Verify the license used by the controllers in the stack. Ideally, the active controller must posses a valid license and the standby controller can either posses a valid license or a HA SKU license. For more details on controller licenses, see the hardware guide-

.

Restrictions for Configuring Controller Stack

You must ensure that the controllers in the stack are configured with the same Cisco IOS Software Release version and licenses.

When you reboot the controller while on stack, you must ensure that you deactivate the already existing licenses configured on the controllers. This is because while you perform a reboot, the controller uses the highest activated (EULA accepted) license level as the reboot license while on stack.

-

Information on Controller Stack

A controller stack can have one stacking-capable controller connected through their StackWise-480 ports; which implies that the stack has two members- an active and a standby controller. The stack member work together as a unified system using the use the StackWise-480 technology. If the active controller becomes unavailable, the standby controller assumes the role of the active switch, and continues to the keep the stack operational.

The active controller contains the saved and running configuration files for the controller stack. The configuration files include the system-level settings for the controller stack and the interface-level settings the stack member. The stack member has a current copy of all these files for back-up purposes. The controllers in the stack use Cisco StackWise-480 technology which provides a robust distributed forwarding architecture through each stack member switch and a unified, fully centralized control and management plane to simplify operation in a large-scale network design.

In the stack, all configuration in the active unit is synced to the standby unit once standby unit changes its state from member to the hot standby state. Thus, all the start-up configuration available in the unit prior to synchronization is lost. If you would need the start-up configuration of the standby unit again, you must save the startup configuration of the unit in secondary memory- Flash memory to reuse the configurations later.

You must use the following Cisco StackWise-480 and Cisco StackPower cables to connect the units in the stack.

Stack Cable	Description
STACK-T1-50CM	Cisco StackWise-480 50cm stacking cable spare
STACK-T1-1M	Cisco StackWise-480 1m stacking cable spare
STACK-T1-3M	Cisco StackWise-480 3m stacking cable spare
CAB-SPWR-30CM	Cisco Catalyst 3850 StackPower cable 30cm spare
CAB-SPWR-150CM	Cisco Catalyst 3850 StackPower cable 150cm spare

When you reboot the controller while on stack, you must ensure that you deactivate the already existing licenses configured on the controllers. This is because while you perform a reboot, the controller uses the highest activated (EULA accepted) license level as the reboot license while on stack.

In the stack, all configuration in the active unit is synced to the standby unit once standby unit changes its state from member to the hot standby state. Thus, all the start-up configuration available in the unit prior to synchronization is lost. If you would need the start-up configuration of the standby unit again, you must save the startup configuration of the unit in secondary memory- Flash memory to reuse the configurations later.

When you use the controller stack, all the six controller ports of both the controllers are combined hence providing an availability of 12 ports for usage. The bandwidth of a controller port is a 10 gig ethernet port; however on combination of 12 ports the controller, a throughput of 60 Gbps is only available for use. These ports can be combined to form an Etherchannel, a flex link, or a Link Aggregation Group (LAG).

Configuring Controller Stack

SUMMARY STEPS

1. Connect two controllers that are up and running using the stack cable.
2. Power up and perform a boot on both controllers simultaneously or power and boot one controller.
3. Configure Etherchannel or LAG on the units. The deployment type of Etherchannel, LAG, and LACP is based on your network design.
4. Execute the command **show etherchannel summary** to view status of the configured Etherchannel.
5. Configure LACP .
6. Execute the commands defined for displaying stack information on the console of the active controller to verify that the redundancy high availability pair exists.

DETAILED STEPS

Step 1 Connect two controllers that are up and running 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 forms a high availability pair.

Step 3 Configure Etherchannel or LAG on the units. The deployment type of Etherchannel, LAG, and LACP is based on your network design.

Step 4 Execute the command **show etherchannel summary** to view 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 Configure LACP .

Step 6 Execute the commands defined for displaying stack information on the console of the active controller to verify that the redundancy high availability pair exists.

Switch Stack Membership

A standalone switch is a switch stack with one stack member that also operates as the active switch. You can connect one standalone switch to another to create a switch stack containing two stack members, with one of them as the active switch. You can connect standalone switches to an existing switch stack to increase the stack membership.

Stack Member Numbers

A new, out-of-the-box switch (one that has not joined a switch stack or has not been manually assigned a stack member number) ships with a default stack member number of 1. When it joins a switch stack, its default stack member number changes to the lowest available member number in the stack.

Stack members in the same switch stack cannot have the same stack member number. Every stack member, including a standalone switch, retains its member number until you manually change the number or unless the number is already being used by another member in the stack.

- If you manually change the stack member number by using the **switch** *current-stack-member-number* **renumber** *new-stack-member-number* command, the new number goes into effect after that stack member resets (or after you use the **reload slot** *stack-member-number* privileged EXEC command) and only if that number is not already assigned to any other members in the stack. Another way to change the stack member number is by changing the SWITCH_NUMBER environment variable.

  If the number is being used by another member in the stack, the switch selects the lowest available number in the stack.

  If you manually change the number of a stack member and no interface-level configuration is associated with that new member number, that stack member resets to its default configuration.

  You cannot use the **switch** *current-stack-member-number* **renumber** *new-stack-member-number* command on a provisioned switch. If you do, the command is rejected.

- If you move a stack member to a different switch stack, the stack member retains its number only if the number is not being used by another member in the stack. If it is being used, the switch selects the lowest available number in the stack.

- If you merge switch stacks, the switches that join the switch stack of a new active switch select the lowest available numbers in the stack.

As described in the hardware installation guide, you can use the switch port LEDs in Stack mode to visually determine the stack member number of each stack member.

Stack Member Priority Values

A higher priority value for a stack member increases the probability of it being elected active switch and retaining its stack member number. The priority value can be 1 to 15. The default priority value is 1. You can display the stack member priority value by using the **show switch** EXEC command.

Note We recommend assigning the highest priority value to the switch that you prefer to be the active switch. This ensures that the switch is reelected as the active switch if a reelection occurs.

To change the priority value for a stack member, use the **switch** *stack-member-number* **priority** *new priority-value* command.

The new priority value takes effect immediately but does not affect the current active switch. The new priority value helps determine which stack member is elected as the new active switch when the current active switch or the switch stack resets.

Active and Standby Switch Election and Reelection

The active switch is elected or reelected based on one of these factors and in the order listed:

1. The switch that is currently the active switch.
2. The switch with the highest stack member priority value.

Note We recommend assigning the highest priority value to the switch that you prefer to be the active switch. This ensures that the switch is reelected as active switch if a reelection occurs.

3. The switch with the lowest MAC address.

Enabling the Persistent MAC Address Feature

This procedure is optional.

Note When you enter the command to configure this feature, a warning message appears with the consequences of your configuration. You should use this feature cautiously. Using the old active switch MAC address elsewhere in the same domain could result in lost traffic.

SUMMARY STEPS

1. **configure terminal**
2. **stack-mac persistent timer** [**0** | *time-value*]
3. **end**
4. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global configuration mode.
Step 2	**stack-mac persistent timer** [**0** | *time-value*] **Example:** `Controller(config)# stack-mac persistent timer 7`	Enables a time delay after a stack-master change before the stack MAC address changes to that of the new stack master. If the previous stack master rejoins the stack during this period, the stack uses that MAC address as the stack MAC address. You can configure the time period as 0 to 60 minutes. • Enter the command with no value to set the default delay of approximately 4 minutes. We recommend that you always enter a value. If the command is entered without a value, the time delay appears in the running-config file with an explicit timer value of 4 minutes. • Enter **0** to continue using the MAC address of the current stack master indefinitely. The stack MAC address of the previous stack master is used until you enter the **no stack-mac persistent timer** command, which immediately changes the stack MAC address to that of the current stack master. • Enter a *time-value* from 1 to 60 minutes to configure the time period before the stack MAC address changes to the new stack master. The stack MAC address of the previous stack master is used until the configured time period expires or until you enter the **no stack-mac persistent timer** command. **Note** If you enter the **no stack-mac persistent timer** command after a new stack master takes over, before the time expires, the switch stack moves to the current stack master MAC address.
Step 3	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 4	**copy running-config startup-config** **Example:** `Controller# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Assigning a Stack Member Number

This optional task is available only from the active switch.

SUMMARY STEPS

1. **switch** *current-stack-member-number* **renumber** *new-stack-member-number*
2. **reload slot** *stack-member-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**switch** *current-stack-member-number* **renumber** *new-stack-member-number* **Example:** `Controller(config)# switch 3 renumber 4`	Specifies the current stack member number and the new member number for the stack member. The range is 1 to 2. You can display the current stack member number by using the **show switch** user EXEC command.
Step 2	**reload slot** *stack-member-number* **Example:** `Controller# reload slot 4`	Resets the stack member.

Setting the Stack Member Priority Value

This optional task is available only from the active switch.

SUMMARY STEPS

1. **switch** *stack-member-number* **priority** *new-priority-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**switch** *stack-member-number* **priority** *new-priority-number* **Example:** `Controller(config)# switch 3 priority 2`	You can display the current priority value by using the **show switch** user EXEC command. The new priority value takes effect immediately but does not affect the current active switch. The new priority value helps determine which stack member is elected as the new active switch when the current active switch or switch stack resets.

Displaying Incompatible Switches in the Switch Stack

SUMMARY STEPS

1. **show switch**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show switch** **Example:** `Controller# show switch`	Displays any incompatible switches in the switch stack (indicated by a 'Current State' of 'V-Mismatch'). The V-Mismatch state identifies the switches with incompatible software. The output displays Lic-Mismatch for switches that are not running the same license level as the active switch. For information about managing license levels, see the *System Management Configuration Guide (Cisco WLC 5700 Series)* .

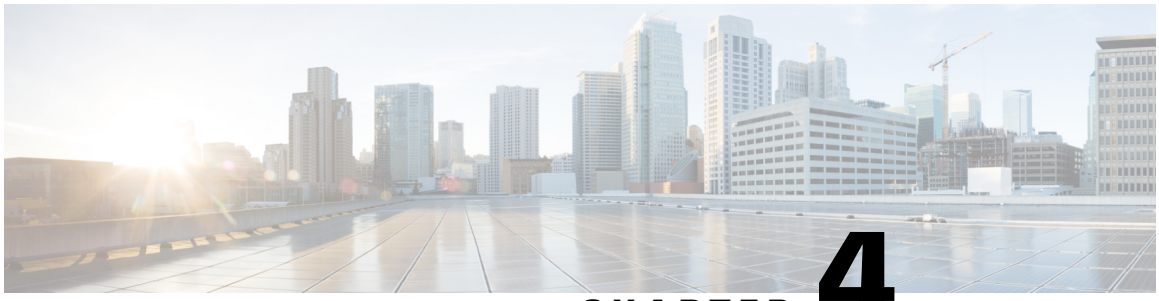
Upgrading an Incompatible Switch in the Switch Stack

SUMMARY STEPS

1. **software auto-upgrade**
2. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**software auto-upgrade** **Example:** `Controller# software auto-upgrade`	Upgrades incompatible switches in the switch stack, or changes switches in bundle mode to installed mode.
Step 2	**copy running-config startup-config** **Example:** `Controller# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.



CHAPTER 4

Configuring High AvailabilityConfiguring Wireless High Availability

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.

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-discovers 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 with out 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	conf t **Example:** `Controller # conf t`	Configures the terminal
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.

	Command or Action	Purpose
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

Hearbeat 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	conf t **Example:** `controller # conf t`	Configures the terminal.

	Command or Action	Purpose
Step 2	ap capwap timers heartbeat-timeout **Example:** `controller # ap capwap timers heartbeat-timeout`	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

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.

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** **Example:** `Controller# configure terminal`	Enters global configuration mode.
Step 2	**interface port-channel** *number* **Example:** `Controller(config)# interface Port-channel Po2`	Enters port-channel interface configuration mode.

	Command or Action	Purpose
Step 3	**lacp max-bundle** *number* **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** *number* **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** *po2* **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 submode.
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# show redundancy states`	Displays the high availability role of the active and standby controllers.
Step 2	**show switch detail** **Example:** `Controller# show switch detail`	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# show platform ses states`	Displays the sequences of the stack manager.
Step 4	**show ap summary** **Example:** `Controller# show ap summary`	Displays all the access points in the active and standby controllers.
Step 5	**show capwap detail** **Example:** `Controller# show capwap detail`	Displays the details of the CAPWAP tunnel in the active and standby controllers.
Step 6	**show dtls database-brief** **Example:** `Controller# show dtls database-brief`	Displays DTLS details in the active and standby controllers.
Step 7	**show power inline** **Example:** `Controller# show power inline`	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# show ap uptime`	Verify if the uptime of the access point after the switchover is large enough.
Step 2	**show wireless summary** **Example:** `Controller# show wireless summary`	Display the clients connected in the active controller.
Step 3	**show wcdb database all** **Example:** `Controller# show wcdb database all`	Display if the client has reached the uptime.
Step 4	**show power inline** **Example:** `Controller# show power inline`	Display the power over Ethernet power state.

Monitoring the Controller Stack

Table 4: 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.

Command	Description
show switch *stack-member-number*	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.
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      Po1(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 preemption mode forced
 switchport backup interface Po2 preemption 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)
```

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.
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**.

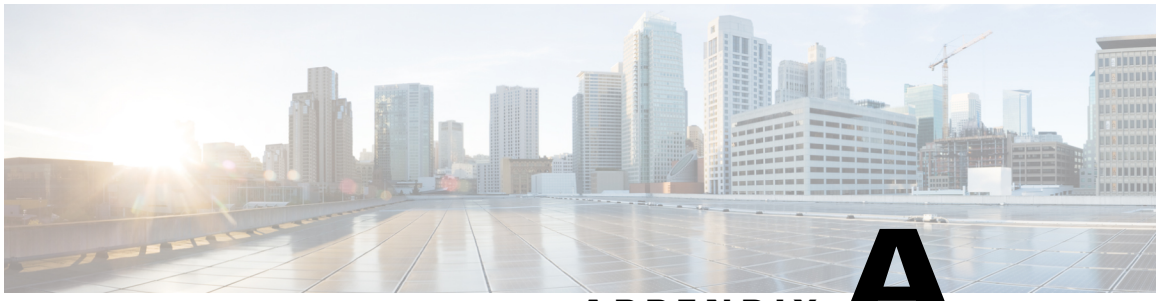
Viewing Switchover States (GUI)

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: • Active • Standby HOT • Disable
Peer State	Displays the state of the peer (or standby) CPU Controller module. Values are as follows: • Standby HOT • Disable

Parameter	Description
Mode	Displays the current state of the redundancy peer. Values are as follows: • 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.
Redundancy State	Displays the current functioning redundancy state of the unit. Values are as follows: • 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**.



APPENDIX A

Reference wrapper Appendix topic here

INDEX