Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)

First Published: October 07, 2013

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-28845-01

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 **Means *reader be warned.* In this situation, you might perform an action that could result in bodily injury.**

Related Documentation

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

- Cisco Catalyst 3650 Switch documentation, located at:

  http://www.cisco.com/go/cat3650_docs

- Cisco SFP and SFP+ modules documentation, including compatibility matrixes, located at:

  http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html

- Error Message Decoder, located at:

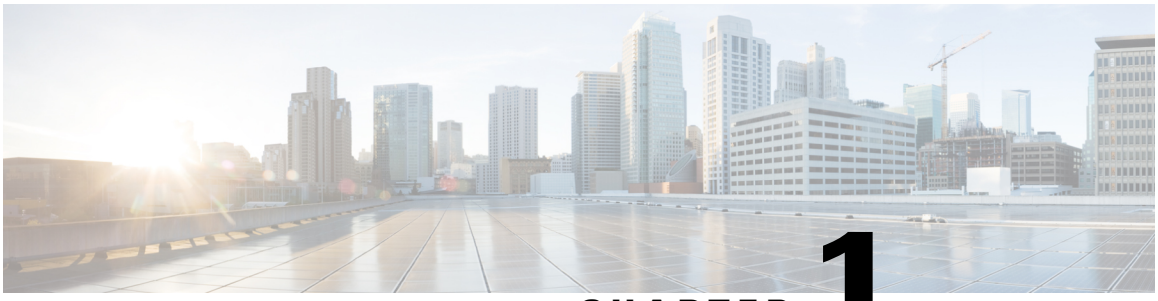
  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

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/en/US/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 switch 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 switch 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.	`Switch>`	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.	`Switch#`	Enter **disable** to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	`Switch(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 switch.
VLAN configuration	While in global configuration mode, enter the **vlan** *vlan-id* command.	`Switch(config-vlan)#`	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 switch startup configuration file.
Interface configuration	While in global configuration mode, enter the **interface** command (with a specific interface).	`Switch(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.

Mode	Access Method	Prompt	Exit Method	About This Mode
Line configuration	While in global configuration mode, specify a line with the **line vty** or **line console** command.	`Switch(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:** `Switch# help`	Obtains a brief description of the help system in any command mode.

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

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

	Command or Action	Purpose
Step 4	**?** **Example:** `Switch> ?`	Lists all commands available for a particular command mode.
Step 5	*command* **?** **Example:** `Switch> show ?`	Lists the associated keywords for a command.

Step 6	*command keyword* **?**
	
	Example:
	`Switch(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 switch to recognize the command as unique.

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

```
Switch# 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 switch.

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 switch 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 switch 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 switch 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:** `Switch# terminal history size 200`	Changes the number of command lines that the switch 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.

	Command or Action	Purpose
Step 3	**show history** **Example:** `Switch# 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:** `Switch# 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:** `Switch# terminal editing`	Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.

	Command or Action	Purpose
Step 2	**terminal no editing** **Example:** `Switch# 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 switch 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:
	`Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35`
	`Switch(config)# $ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25`
	`Switch(config)# $t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq`
	`Switch(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:** `Switch(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. 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*	Searches and filters the output.

	Command or Action	Purpose

	Example:
	`Switch# 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`
		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 on a Switch Stack

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

You manage the switch stack and the stack member interfaces through the . You cannot manage stack members on an individual switch basis. You can connect to the through the console port or the Ethernet management port of one or more stack members. Be careful with using multiple CLI sessions on the . Commands that you enter in one session are not displayed in the other sessions. Therefore, it is possible to lose track of the session from which you entered commands.

Note We recommend using one CLI session when managing the switch stack.

If you want to configure a specific stack member port, you must include the stack member number in the CLI command interface notation.

Accessing the CLI Through a Console Connection or Through Telnet

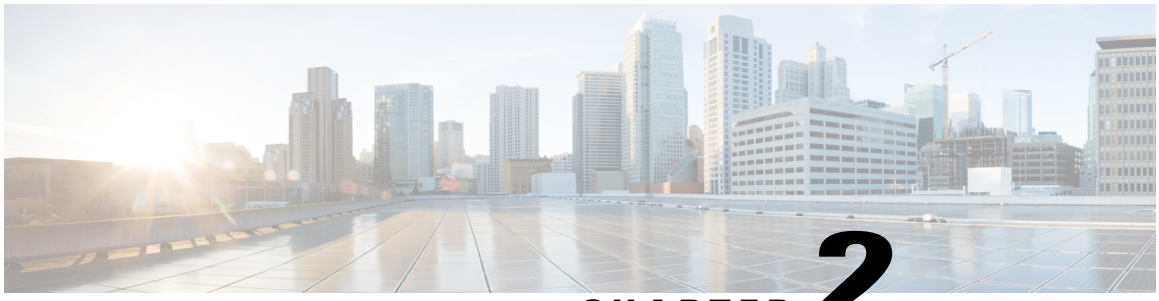
Before you can access the CLI, you must connect a terminal or a PC to the switch console or connect a PC to the Ethernet management port and then power on the switch, as described in the hardware installation guide that shipped with your switch.

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

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

- Connect the switch 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 switch hardware installation guide.
- Use any Telnet TCP/IP or encrypted Secure Shell (SSH) package from a remote management station. The switch must have network connectivity with the Telnet or SSH client, and the switch must have an enable secret password configured.
    - The switch supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.
    - The switch 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 switch 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 switch.

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 switch 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 switch, 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 switch 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 switch, WLAN, and radios.
- Enables you to configure and set security policies on your switch.
- Enables you to access the switch operating system software management commands.

The Administration tab enables you to configure system logs.

Connecting the Console Port of the Switch

Before You Begin

Before you can configure the switch 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 switch's RJ-45 console port and the other end to your PC's serial port.

Step 2 Plug the AC power cord into the switch 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 switch 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 switch is configured with the IP address for service port.

Logging On to the Web GUI

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

Step 2 The Accessing Cisco AIR-CT3650 page appears.

Enabling Web and Secure Web Modes

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

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

Step 2 To enable web mode, which allows users to access the switch 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 switch 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 Switch Web GUI

The configuration wizard enables you to configure basic settings on the switch. You can run the wizard after you receive the switch from the factory or after the switch 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 switch. The switch 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 Switch <Model Number> <Hostname>** page appears.

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

Step 4 Choose **Configuration** > **Wizard** to perform all steps that you need to configure the switch initially.
The **Admin Users** page appears.

Step 5 On the **Admin Users** page, enter the administrative username to be assigned to this switch in the User Name text box and the administrative password to be assigned to this switch 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 switch. 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 switch, and click **Next**:

- Customer-definable switch 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**.

- Choose **Mobility Controller** or **Mobility Agent** from the Mobility Role drop-down list:

- If Mobility Agent is chosen, enter the mobility controller IP address in the Mobility Controller IP Address text box and mobility controller IP address in the Mobility Controller Public IP Address text box.
- If Mobility Controller is chosen, then the mobility controller IP address and mobility controller public IP address are displayed in the respective text boxes.

- Displays mobility protocol port number in the Mobility Protocol Port text box.
- Displays the mobility switch peer group name in the Mobility Switch Peer 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.
- The amount of time (in seconds) between each ping request sent to an peer switch 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 switch 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 switch in the Mobility Control Message DSCP Value (0-63) text box.

  The valid range is 0 to 63, and the default value is 0.
- Displays the number of mobility switch peer group member configured in the Switch Peer Group Members Configured text box.

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 switch based on the following parameters, and click **Next**.

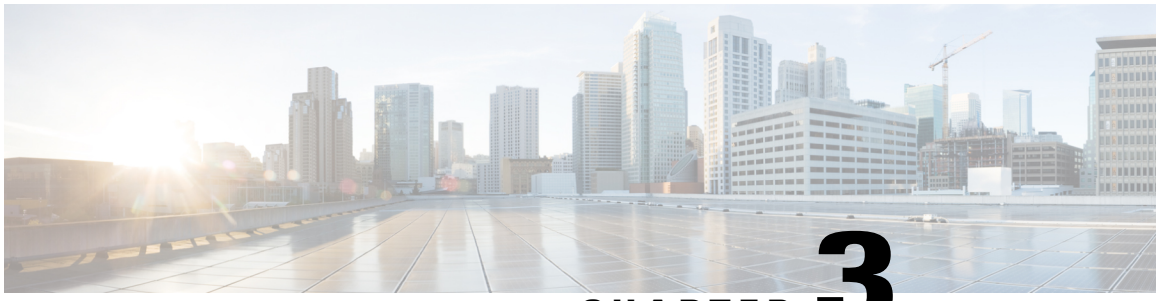
- Displays current timestamp on the switch in the Current Time text box.
- Choose either Manual or NTP from the Mode drop-down list.

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

- Choose date on the switch 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 switch 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 switch using these steps, and if you wish to change any configuration value, click **Previous** and navigate to that page.
You can save the switch 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 switch.



CHAPTER 3

Information About Mobility

Overview

The switch delivers more services at access layer other than merely providing increased speeds and feeds. Wireless services is now integrated with the switch, which ensures that the access layer switch terminates the wireless users data plane, thereby delivering on the promise of Cisco's unified architecture. Unification implies that mobility services are provided to both wireless and wired stations.

The switch provides seamless roaming, which requires transparency of the network configuration and deployment options to the client.

From the end user's perspective, any mobility event must not change its IP address, its default router or DHCP server. This means that as stations roam, they must be able to

- Send an ARP to their default router, or
- Transmit a DHCP request to the server that had previously assigned their address.

From the infrastructure's perspective, as mobility events occur, the station's traffic must follow its current point of attachment, which can either be a mobility agent (MA) or mobility controller (MC). This must be true regardless of whether the station has moved to a network that is configured for a different subnet. The period from which the station is not receiving traffic following its mobility event must be as short as possible, even below 40 ms whenever possible, which includes any authentication procedures that are required.

From the infrastructure's perspective, the mobility management solution must have four main components, and all of these functions must be performed within the constraints of roaming:

- Initial Association—This function is used to identify the user's new point of attachment in the network.
- Context Transfer—This function is used to transfer state information associated with the station. This ensures that the station's static and real-time policies, including security and application ACLs, and services, remain the same across handoffs.
- Handoff—This function is used to signal that the station's point of attachment has changed, and control of the station should be relinquished by the previous access switch.
- Data Plane—This function is typically tied to the handoff process, and ensures that the station's traffic continues to be delivered and received from the station without any noticeable performance degradation.

Wired and Wireless Mobility

One of the key features of the Converged access solution (applicable to both the Cisco Catalyst 3850 Switch and Cisco WLC 5700 Series Controller) is its ability to provide a device with an IP address and maintain its session persistence, across mobility events from ethernet connections to wireless and vice-versa. This feature allows users to remain on an ethernet network when possible, and make use of the freedom of mobility associated with wireless when necessary.

This feature leverages support from both the client and the infrastructure and uses the two factor authentication-device and user. The device authentication credentials is cached in the mobility controller (MC). When a device transitions across link layers, the device credentials is validated, and if a match is found, the MC ensures that the same IP address is assigned to the new interface.

Features of Mobility

- Mobility Controller (MC)—The controller provides mobility management services for inter-peer group roaming events. The MC provides a central point of contact for management and policy based control protocols, such as RADIUS. This eliminates the need for the infrastructure servers to maintain a user's location as it transitions throughout the network. The MC sends the configuration to all the mobility agents under its sub-domain of their mobility configuration, peer group membership and list of members. A sub-domain is synonymous to the MC that forms it. Each sub-domain consists of an MC and zero or more access switches that have AP's associated to them.
- Mobility Agents (MA)— A mobility agent is either an access switch that has a wireless module running on it or an MC with an internal MA running on it. A mobility agent is the wireless component that maintains client mobility state machine for a mobile client that is connected via an AP to the device that the MA is running on.
- Mobility Sub Domain— It is an autonomous portion of the mobility domain network. A mobility sub-domain comprises of a single mobility controller and its associated mobility agents (MAs).

  Note Even when more than one mobility controller is present, only one MC can be active at any given time.

  A mobility sub-domain is the set of devices managed by the active mobility controller. A mobility sub-domain comprises of a set of mobility agents and associated access points.

- Mobility Group— A collection of mobility controllers (MCs) across which fast roaming is supported. The concept of mobility group is the same as a collection of buildings in a campus across which frequent roaming is expected.
- Mobility Domain— A collection of mobility sub-domains across which mobility is supported. The term mobility domain may be the same as a campus network.
- Mobility Oracle (MO)—The mobility oracle acts as the point of contact for mobility events that occur across mobility sub-domains. It also maintains a local database of each station in the entire mobility domain, their home and current sub-domain. A mobility domain includes one or more mobility oracle, though only one would be active at any given time.
- Mobility Tunnel Endpoint (MTE)— The mobility tunnel endpoint (MTE) provides data plane services for mobile devices through the use of tunneling. This minimizes the impact of roaming events on the network by keeping the user's point of presence on the network a constant.
- Point of Attachment— A station's point of attachment is where its data path is initially processed upon entry in the network. This could either be the access switch that is currently providing it service, or the wireless LAN controller.
- Point of Presence— A station's point of presence is the place in the network where the station is being advertised. For instance, if an access switch is advertising reachability to the station via a routing protocol, the interface on which the route is being advertised is considered the station's point of presence.
- Switch Peer Group (SPG)— A peer group is a statically created list of neighboring access switches between which fast mobility services is provided. A peer group limits the scope of interactions between switches during handoffs to only those that are geographically proximate.
- Station—A user's device that connects to and requests service from the network. The device may have a wired, wireless or both interfaces.
- Switch in the same SPG—A peer switch that is part of the peer group of the local switch.
- Switch outside the SPG—A peer access switch that is not part of the local switch's peer group.
- Foreign Mobility Controller— The mobility controller providing mobility management service for the station in a foreign mobility sub-domain. The foreign mobility controller acts as a liaison between access switches in the foreign sub-domain and the mobility controller in the home domain.
- Foreign Mobility Sub-Domain— The mobility sub-domain, controlled by a mobility controller, supporting a station which is anchored in another mobility sub-domain
- Foreign Switch— The access switch in the foreign mobility sub-domain currently providing service to the station.
- Anchor Mobility Controller— The mobility controller providing a single point of control and mobility management service for stations in their home mobility sub-domain.
- Anchor Mobility Sub-Domain— The mobility sub-domain, controlled by a mobility controller, for a station where its IP address was assigned.
- Anchor Switch— The switch in the home mobility sub-domain that last provided service to a station.

Sticky Anchoring for Low Latency Roaming

Sticky Anchoring ensures low roaming latency from the client's point of presence is maintained at the switch where the client initially joins the network. It is expensive to apply client policies at a switch for a roaming client. There can be considerable delay as it involves contacting the AAA server for downloadable ACLs which is not acceptable for restoring time sensitive client traffic.

To manage this delay, when the client roams between APs connected to different switches , irrespective of whether it is an intra sub-domain roam or inter sub-domain roam, the client traffic is always tunneled to the switch where the client first associates. The client is anchored at its first point of attachment for its lifetime in the network.

This behavior is enabled by default. You can also disable this behavior to allow the client anchoring only for inter-subnet roams. This configuration is per WLAN config and is available under the WLAN config mode. The customer can configure different SSIDs for time sensitive and non time sensitive applications.

Bridge Domain ID and L2/L3 Roaming

Bridge domain ID provides the mobility nodes with information to decide on specific roam type, either as L2 or L3 roam. It also allows the network administrators to reuse the VLAN IDs across network distribution. When the VLAN IDs do not have the associated subnet configurations, they may require additional parameter to use in conjunction with VLAN ID. The network administrator ensures that the given VLAN under the same bridge domain ID are associated with the unique subnet. The mobility nodes will first check for the bridge domain ID for the given node and the VLAN ID associated with the client to identify the roam type. The bridge domain ID and the VLAN ID must be same to treat a roam as L2 roam.

The bridge domain ID is configured for each SPG when creating a SPG and later on the MC. The bridge domain ID could be same for more than one SPG and all the MAs under the SPG will share the same bridge domain ID. This information is pushed to the MAs as part of the configuration download when MA comes up initially. If the bridge domain ID is modified when the system is up, it will be pushed to all the MAs in the modified SPG and will take immediate effect for the future roams.

Note The MC can also have a bridge domain ID for it self, as the MC can also be part of a SPG.

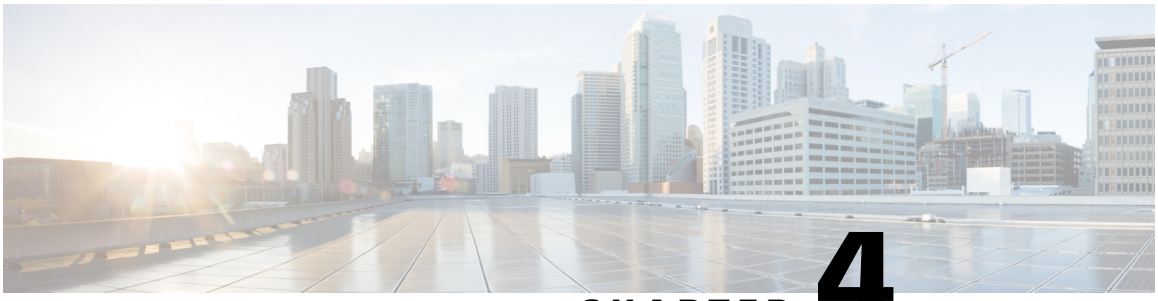
Link Down Behavior

This section provides information about data synchronization between MA-MC and MC-MO when MC or MO faces downtime in absence of redundancy manager. When Keepalive is configured between MA-MC or MC-MO the clients database is synchronized between the MO and the MCs and the MC and its MAs respectively.

Platform Specific Scale Requirement for the Mobility Controller

The Mobility Controller (MC) role is supported on a number of different platforms like, the Cisco WLC 5700 Series, CUWN and Catalyst 3850 Switches. The scale requirements on these three platforms are summarized in the table below:

Scalability	Catalyst 3850 as MC	Catalyst 3650 as MC	Cisco WLC 5700 as MC	CUWN 5508 as MC	WiSM2 as MC
Max number of MC in Mobility Domain	8	8	72	72	72
Max number of MC in Mobility Group	8	8	24	24	24
Max number of MAs in Sub-domain (per MC)	16	16	350	350	350
Max number of SPGs in Sub-domain (per MC)	8	8	24	24	24
Max number of MAs in a SPG	16	16	64	64	64



CHAPTER 4

Mobility Network Elements

Mobility Agent

- Handling the mobility events on the switch
- Configuring the datapath elements on the switch for mobility, and
- Communicating with the mobility controller

As MA, the switch performs the datapath functions by terminating the CAPWAP tunnels that encapsulate 802.11 traffic sourced by wireless stations.

This allows the switch to apply features to wired and wireless traffic in a uniform fashion. As far as switch is concerned, 802.11 is just another access medium.

The MA performs the following functions:

- Support the mobility protocol – The MA is responsible for responding in a timely manner, ensuring the switch is capable of achieving its roaming budget.
- Point of presence – If the wireless subnets are not available at the MC, the MA assumes the point of presence if the wireless client VLAN is not available at the new point of attachment and tunnel the client traffic accordingly.
- ARP Server – When the network is configured in a layer 2 mode, the MA is responsible for advertising reachability for the stations connected to it. If tunneling is employed, the ARP request is transmitted on behalf of the station through the tunnel, which the point of presence (anchor switch) would bridge onto its uplink interface.
- Proxy IGMP – The MA on the switch is responsible for subscribing to multicast groups on behalf of a station after a roaming event has occurred. This information is passed as part of the context to the new switch. This ensures the multicast flows follow the user as it roams.

- Routing – When the switch is connected to a layer 3 access network, the MA is responsible for injecting routes for the stations that are associated with it for which tunneling is not provided.
- 802.1X Authenticator – The authenticator function is included in the MA, and handles both wired and wireless stations.
- Secure PMK Sharing – When a station successfully authenticates to the network, the MA forwards the PMK to the MC. The MC is responsible for flooding the PMK to all the MAs under its sub-domain and to the peer MCs in the mobility group.

The MA also performs the following datapath functions:

- Mobility tunnel – If tunneling is used, the MA encapsulates and decapsulates packets from the mobility tunnel to the MC, and to other MA in the peer group, if the access switches are serving as points of presence. The MA supports the tunneling of client data traffic between the point of attachment and the point of attachment. The packet format used for other switches is CAPWAP with an 802.3 payload. The MA also supports reassembly and fragmentation for mobility tunnels.
- Encryption – The mobility control traffic between the mobility nodes is DTLS encrypted. The MA also encrypts the CAPWAP control and data (optional) at the point of attachment.
- CAPWAP – The switch supports the CAPWAP control and data planes. The switch forwarding logic is responsible for terminating the CAPWAP tunnels with 802.11 as well as 802.3 payloads. Since support for large frames (greater than 1500bytes) is not universally available, the switch supports CAPWAP fragmentation and reassembly.

Mobility Controller

The main function of mobility controller is to coordinate the client roaming beyond a switch peer group. The other features of the mobility controller are:

- Station Database—The Mobility Controller maintains a database of all the clients that are connected within the local mobility sub-domain.
- Mobility Protocol—The MC supports the mobility protocol which ensures the target roaming point responds in a timely manner and achieves the 150ms roaming budget
- Interface to Mobility Oracle—The Mobility Controller acts as a gateway between the switch and the Mobility Oracle. When the Mobility Controller does not find a match in its local database, it suggests a match for a wireless client entry (in its database) and forwards the request to the Mobility Oracle, which manages the Mobility Domain.

Note Mobility Oracle function can be enabled on an MC only if it is supported by the platform.

- ARP Server—When tunneling is employed for a station, its point of presence on the network is the Mobility Tunnel Endpoint (MTE). The Mobility Controller responds to any ARP requests received for the stations it is responsible for.
- Configures MTE—The Mobility Controller is the control point for the switch for all mobility management related requests. When a change in a station's point of attachment occurs, the Mobility Controller is responsible for configuring the forwarding policy on the MTE.

- NTP Server—The Mobility Controller acts as an NTP server to the switch and supports all the nodes to have their clocks synchronized with it.

Mobility Oracle

The Mobility Oracle coordinates the client roams beyond the subdomain on a need basis and consists of the following features:

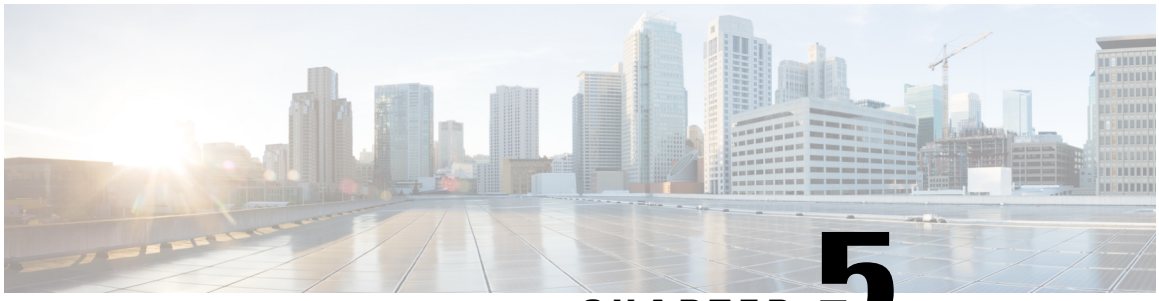
- Station Database—The Mobility Oracle maintains a database of all stations that are serviced within the mobility domain. This database is populated during the Mobility Oracle's interactions with all the Mobility Controllers, in all of the mobility sub-domains it supports.
- Interface to Mobility Controller—When the Mobility Oracle receives a request from a Mobility Controller, it performs a station lookup, and forwards, whenever needed, the request to the proper Mobility Controller.
- NTP Server—The Mobility Oracle acts as an NTP server to the Mobility Controllers and synchronizes all the **switch** clocks within the mobility domain.

Guest Controller

The guest access feature provides guest access to wireless clients. The guest tunnels use the same format as the mobility tunnels. Using the guest access feature, there is no need to configure guest VLANs on the access switch. Traffic from the wired and wireless clients terminates on Guest Controller. Since the guest VLAN is not present on the access switch, the traffic is tunneled to the MTE over the existing mobility tunnel, and then via a guest tunnel to the Guest Controller.

The advantage of this approach is that all guest traffic passes through the MTE before it is tunneled to the Guest Controller. The Guest Controller only needs to support tunnels between itself and all the MTEs.

The disadvantage is that the traffic from the guest client is tunneled twice - once to the MTE and then again to the Guest Controller.



CHAPTER 5

Mobility Control Protocols

About Mobility Control Protocols

The mobility control protocol is used regardless of whether tunneled or routed. The mobility control protocol is used for mobility events between the MO, MC and MA.

The mobility architecture uses both,

- Distributed approach, using the direct communication with the switches in their respective SPG, as well as
- Centralized approach, using the MC and MO.

The goal is to reduce the overhead on the centralized MC, while limiting the interactions between switches to help scale the overall system.

Initial Association and Roaming

The following scenarios are applicable to the mobility management protocol:

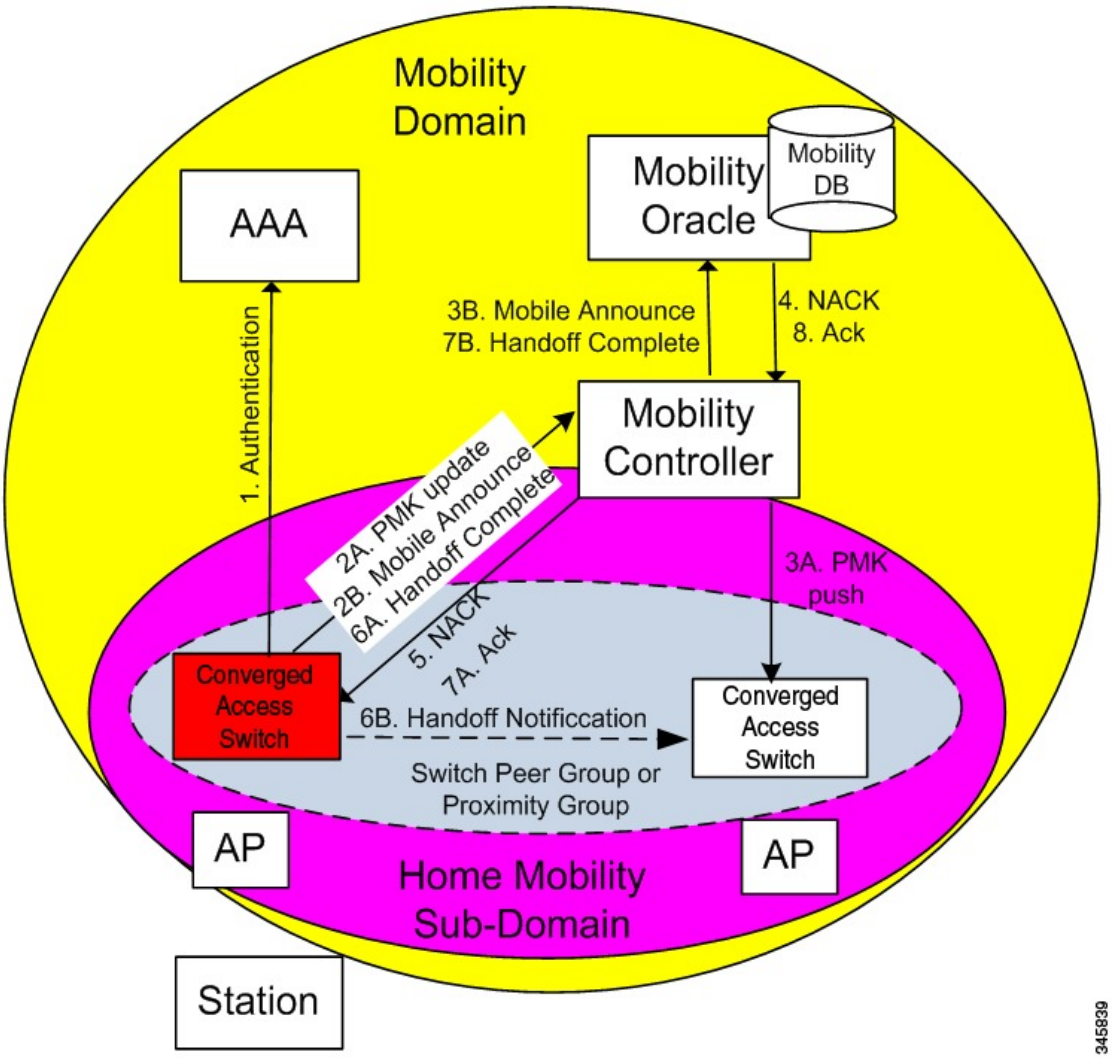
- Initial Association
- Intra Switch Roam

- Intra Switch Peer Group Roam
- Inter Switch Peer Group Roam
- Inter Sub-Domain Roam
- Inter Group Roam

Initial Association

The illustration below explains the initial association process followed by theswitch:

Figure 1: Initial Association



1 When a station initially associates with a mobility agent, the MA performs a lookup to determine whether keying information for key caching is locally available in the MA. If no keying information is available,

which is the case when the station first appears in the network, the switch prompts the device to authenticate itself to generate the Pairwise Master Key (PMK). The PMK is generated on the client and the RADIUS server side, and the RADIUS sever forwards the PMK to the authenticator, the MA.

2 The MA sends the PMK to the MC.

3 After receiving the PMK from the MA, the MC transmits the PMK to all the MAs in its sub-domain, and to all the other MCs in its mobility group.

4 The mobility group is a single key domain. This ensures that 802.11r compliant stations recognize the key domain, and attempts to utilize the fast transition procedures defined in 802.11r.

Note The 802.11r protocol defines a key domain, which is a collection of access points that share keying information.

5 (Refer to step 2B in the illustration). Since the station is new to the mobility sub-domain, as indicated by the fact that the PMK is not in the MA local key cache, the MA transmits a mobile announce message to the MC.

6 The MC checks if the client exists in its database. As the client cannot be found, the MC in turn forwards it to the MO, if available.

7 (Refer to step 5 in the illustration). As the station is new to the network, the MO returns a negative response (NACK), which is forwarded by the MC to the switch. If the Mobility Oracle is not available then the MC is responsible for not responding to the Mobile Announce.

8 The MA on the switch informs the MC about the station's new point of attachment via the Handoff Complete message.

9 The MA then informs the other MAs in its switch peer group (SPG) about the station's new point of attachment via the Handoff Notification message. It is necessary to transmit this notification to the MAs in its SPG to allow local handoff without interacting with the MC. The Handoff Notification message sent to MAs in SPG need not carry all the information in Handoff Complete message sent to the MC.

10 (Refer to step 7B in the illustration). The MC updates its database and forwards the Handoff Complete message to the Mobility Oracle. This ensures that the Mobility Oracle's database is updated to record the station's current home mobility sub-domain.

To eliminate race conditions that could occur with devices moving quickly across switch, regardless of whether they are within a mobility sub-domain or not, the messages between MA and MC/MO are time synchronized. This would allow the MC and MO to properly process requests, if they are received out of order.

The Handoff Notification sent to MAs in the SPG are not acknowledged.

Intra Switch Handoff

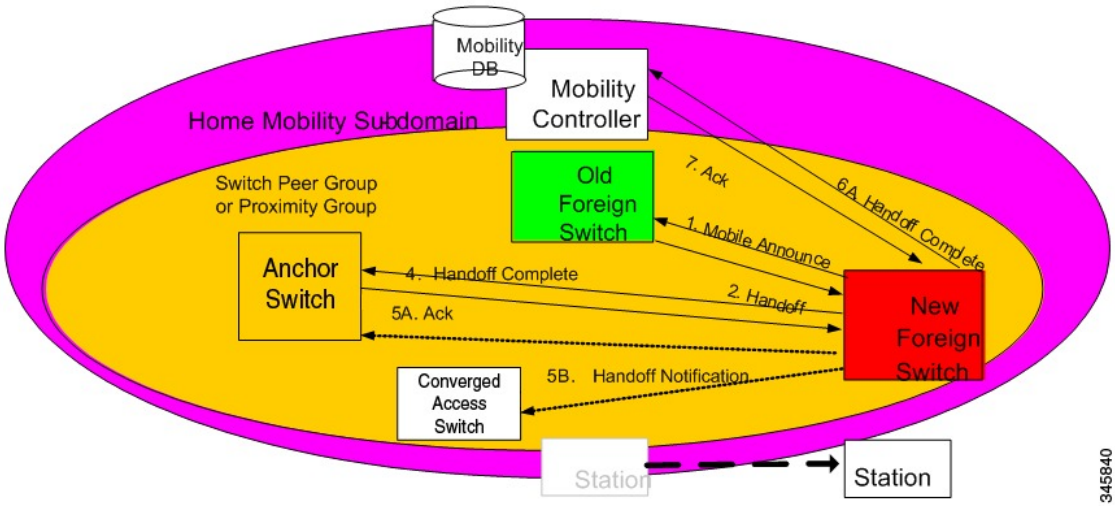
Mobility events within an MA are completely transparent to the SPG and the MC. When a station moves across APs on the same MA and attempts to perform a fast handoff, the PMK is present on the MA. The MA will complete the fast handoff without invoking any additional signal.

Intra Switch Peer Group Handoff

The switch peer group (SPG) is a group of MAs between which users may roam, and expect fast roaming services. Allowing the MA to handoff directly within a SPG reduces the overhead on the MC as it requires fewer messages to be exchanged.

After the initial association is complete the station moves to another MA belonging to its SPG. In an intra switch peer group roam, the initial association, the stations PMK was forwarded to all MAs in the mobility sub-domain.

Figure 2: Intra Switch Peer Group Handoff



The following process explains the intra switch peer group handoff:

1. In the initial association example, the Handoff Notification message is sent to all MAs in its SPG to know the station's current point of attachment.
2. The new MA sends a unicast Mobile Announce message to the previous MA to which the client is associated.
3. After the handoff completion, the new MA transmits a Handoff Complete message to the MC.
4. The new switch sends a Handoff Notification to all MA in its own SPG to inform them about the clients new point of presence.

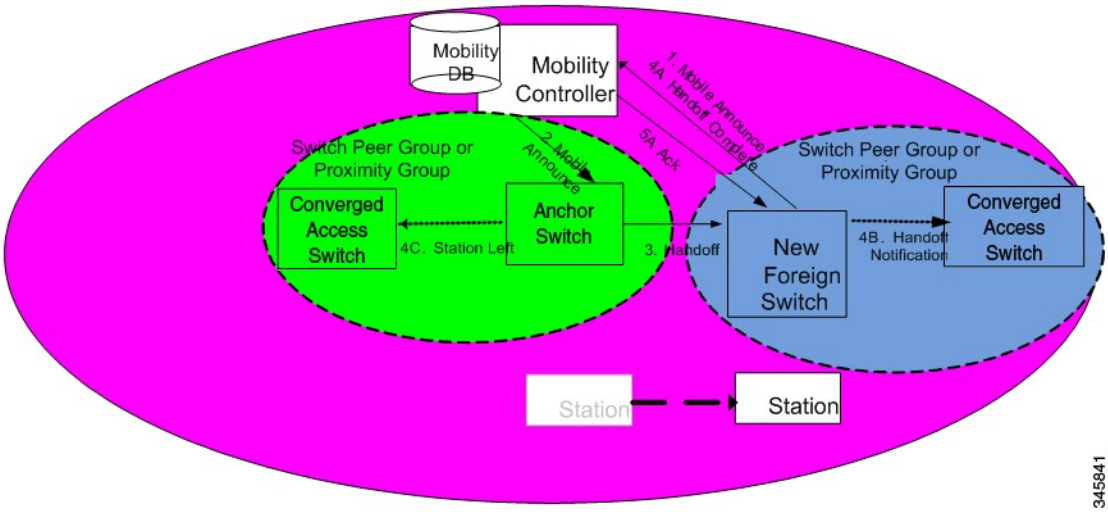
Inter Switch Peer Group Handoff

The Intra SPG roams do not cover all possible scenarios and there can be cases where it is possible for mobility events to occur between two MAs that are not in the same SPG.

When a MA does not have any information about a station's current point of attachment, because of the Handoff Notification message getting lost in the network, or because of the the station roaming to an MA that is not in the new SPG, the MA consults the MC. The MC provides information about the clients point of

presence within the mobility sub-domain. This eliminates the need to consult all other MCs within the mobility sub-domain.

Figure 3: Inter Switch Peer Group Handoff



The image above illustrates an example of a mobility event that occurs across MAs that are not in the same SPG, but within the same mobility sub-domain.

Note The MA color matches the circle representing its SPG.

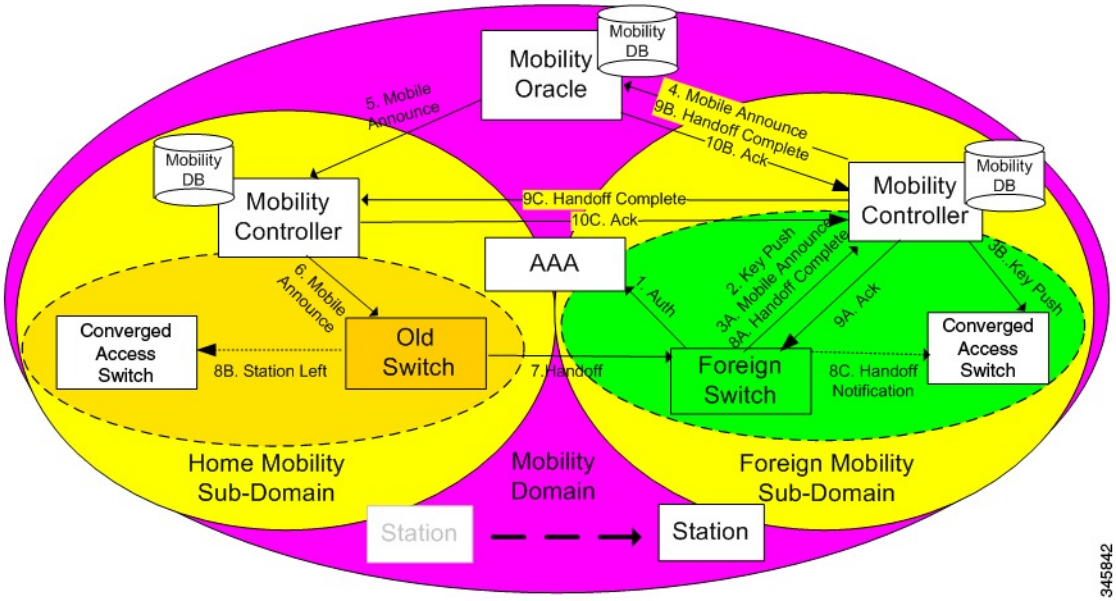
1. The new MA will have the PMK for the station, which was forwarded to each MA in the mobility sub-domain upon client initial authentication.
2. Since the MA had not been previously notified of the station's presence on a neighboring MA inside a different SPG transmits the mobile announce to the sub-domain's MC.
3. (Refer to step 2 in the illustration) On receiving the mobile announce message, the MC performs a lookup in its database, and forwards the request to the MA that was previously providing service to the station. This information is known to the MC through a previously received Handoff Complete message sent in a reliable fashion from the old MA.
4. (Refer to step 3 in the illustration) The old MA, shown in green above, transmits a Handoff message directly to the new MA.
5. The old MA needs to notify other MAs within its SPG of the fact that the station has left the group using a Station Left message. This ensures that if the station were to come back to one of the MA , they would be aware of the fact that the station is no longer being serviced by the old MA.
6. Once the handoff is complete, the new MA transmits the Handoff Complete message in a reliable fashion to the MC.
7. The new MA then transmits the Handoff Notification to the other MAs within its SPG.

Inter Sub Domain Handoff

A sub-domain is an ensemble formed by a mobility controller and the mobility agents it directly manages. An inter sub-domain mobility event implies communication between two mobility controllers. These 2 mobility controllers can be configured with the same mobility group value and recognize each other. They will appear in each other's mobility list, or they can be configured with different mobility group values, and still recognize each other.

When the roaming event occurs across sub-domains between MCs in the same mobility group, the 802.11r key domain advertised by the new APs are the same. Additionally, the client PMK is also transmitted to all MCs upon the client's initial authentication. The new MC does not need to force the client to reauthenticate, and the new MC also knows which previous MC was managing the wireless client mobility.

Figure 4: Inter Sub Domain Handoff



The following steps are involved in the inter sub domain handoff, when mobility controllers belong to the same mobility group:

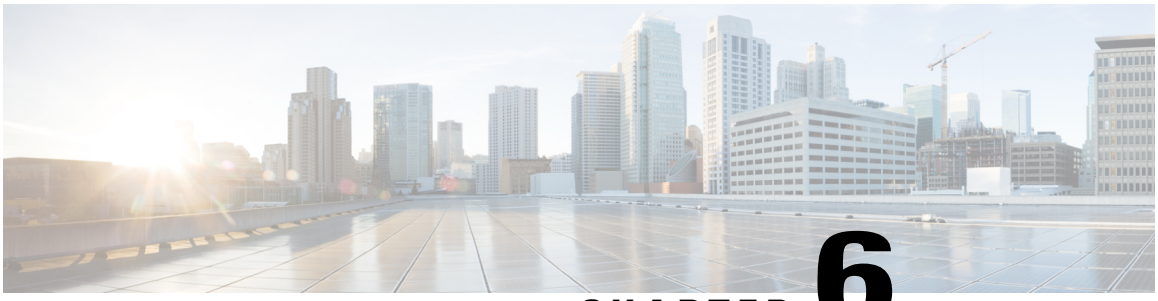
1. When a clients PMK was sent by the initial MA to all the MCs in the mobility group, the new MA already had already received the client PMK from its MC, and re-authentication is not required.
2. The new MA was not notified previously of the station's presence on a neighboring MA inside a different SPG it transmits the mobile announce to the sub-domain's MC.
3. On receiving the mobile announce message, the MC forwards the mobile announce to the MO, which performs a lookup in its database, and forwards the request to the MC that was previously providing service to the station.
4. The previous MC, in turn, forwards the request to the MA that was previously providing service to the station.
5. The old MA, shown in yellow color above, transmits a Handoff message directly to the new MA.

6 The old MA must notify the other MAs within its SPG of the fact that the station has left the SPG using a Station Left message. This ensures that if the station comes back to one of the MA , the MA is aware of the fact that the station is no longer serviced by the old MA.
7 Once the handoff is complete, the new MA transmits the Handoff Complete message in a reliable fashion to the new Mobility Controller.
8 The new MA then transmits the Handoff Notification to all other MAs.
9 The new MC then transmits the Handoff Complete to the old MC.

Inter Mobility Group Handoff

A mobility group is formed by MCs sharing the same mobility group name, and knowing each other.

Since the roaming event occurs across mobility groups, the 802.11r key domain advertised by the new APs differ. This forces the client to re-authenticate. They are propagated only within a mobility group, and roaming across mobility groups requires the stations to re-authenticate when they cross mobility group boundaries. When the authentication is complete, the PMK that is generated is pushed to the MAs and MCs within the same mobility group. The stations cache the PMK from the previous sub-domain because each PMK is associated to a given sub-domain (802.11y key domain). This ensures that you do not have to re-authenticate when the PMK roams back to the previous sub-domain within the pmk cache timeout interval. The remaining procedure follows the inter-sub-domain handoff steps, except that these steps relate to inter mobility group roaming.



CHAPTER 6

Configuring Mobility

Configuring Mobility Controller

Configuring Converged Access Controllers

Creating Peer Groups, Peer Group Member, and Bridge Domain ID (CLI)

Before You Begin

- On the mobility agent, you can only configure the IP address of the mobility controller.
- On the mobility controller, you can define the peer group and the IP address of each peer group member.

SUMMARY STEPS

1. **wireless mobility controller**
2. **wireless mobility controller peer-group** *SPG1*
3. **wireless mobility controller peer-group** *SPG1* **member ip** *member-ip-addr* **public-ip** *public-ip-addr*
4. **wireless mobility controller peer-group** *SPG1* **member ip** *member-ip-addr* **public-ip** *public-ip-addr*
5. **wireless mobility controller peer-group** *SPG2*
6. **wireless mobility controller peer-group** *SPG2* **member ip** *member-ip-addr* **public-ip** *public-ip-addr*
7. **wireless mobility controller peer-group** *SPG1* **bridge-domain-id** *id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wireless mobility controller** **Example:** `Switch(config)# wireless mobility controller`	Enables the mobility controller functionality on the device. This command is applicable only to the switch. The controller is by default a mobility controller.
Step 2	**wireless mobility controller peer-group** *SPG1* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1`	Creates a peer group named SPG1.
Step 3	**wireless mobility controller peer-group** *SPG1* **member ip** *member-ip-addr* **public-ip** *public-ip-addr* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.2 public-ip 10.10.20.2`	Adds a mobility agent to the peer group. **Note** The 10.10.20.2 is the mobility agent's direct IP address. When NAT is used, use the optional public IP address to enter the mobility agent's NATed address. When NAT is not used, the public IP address is not used and the device displays the mobility agent's direct IP address.
Step 4	**wireless mobility controller peer-group** *SPG1* **member ip** *member-ip-addr* **public-ip** *public-ip-addr* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6 public-ip 10.10.20.6`	Adds another member to the peer group SPG1.
Step 5	**wireless mobility controller peer-group** *SPG2* **Example:** `Switch(config)# wireless mobility controller peer-group SPG2`	Creates another peer group SPG2.
Step 6	**wireless mobility controller peer-group** *SPG2* **member ip** *member-ip-addr* **public-ip** *public-ip-addr* **Example:** `Switch(config)# wireless mobility controller peer-group SPG2 member ip 10.10.10.20 public-ip 10.10.10.20`	Adds a member to peer group SPG2.
Step 7	**wireless mobility controller peer-group** *SPG1* **bridge-domain-id** *id* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1 bridge-domain-id 54`	(Optional) Adds a bridge domain to SPG1 used for defining the subnet-VLAN mapping with other SPGs.

This example shows how to create peer group and add members to it:

```
Switch(config)# wireless mobility controller
Switch(config)# wireless mobility controller peer-group SPG1
Switch(config)# wireless mobility controller peer-group SPG1
Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.2 public-ip
 10.10.20.2
Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6 public-ip
 10.10.20.6
Switch(config)# wireless mobility controller peer-group SPG2
Switch(config)# wireless mobility controller peer-group SPG2 member ip 10.10.10.20 public-ip
 10.10.10.20
Switch(config)# wireless mobility controller peer-group SPG1 bridge-domain-id 54
```

Creating Peer Groups, Peer Group Member, and Bridge Domain ID (GUI)

Before You Begin

- Ensure that the device is in mobility controller state.
- On the mobility agent, you can only configure the IP address of the mobility controller.
- On the mobility controller, you can define the peer group and the IP address of each peer group member.

Step 1 Choose **Controller** > **Mobility Management** > **Switch Peer Group**.
The **Mobility Switch Peer Groups** page is displayed.

Step 2 Click **New**.

Step 3 Enter the following details:

a) **Switch Peer Group Name**
b) **Bridge Domain ID**
c) **Multicast IP Address**

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Configuring Local Mobility Group (CLI)

Configuration for wireless mobility groups and mobility group members where the mobility group is a group of MCs.

Before You Begin

MCs can belong only to one mobility group, and can know MCs in several mobility groups.

SUMMARY STEPS

1. **wireless mobility group name** *group-name*
2. **wireless mobility group member ip** *member-ip-addr* **public-ip** *public-ip-addr*
3. **wireless mobility group keepalive interval** *time-in-seconds*
4. **wireless mobility group keepalive count** *count*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wireless mobility group name** *group-name* **Example:** `Switch(config)# wireless mobility group name Mygroup`	Creates a mobility group named Mygroup.
Step 2	**wireless mobility group member ip** *member-ip-addr* **public-ip** *public-ip-addr* **Example:** `Switch(config)# wireless mobility group member ip 10.10.34.10 public-ip 10.10.34.28`	Adds a mobility controller to the Mygroup mobility group. **Note** When NAT is used, use the optional public IP address to enter the NATed IP address of the mobility controller.
Step 3	**wireless mobility group keepalive interval** *time-in-seconds* **Example:** `Switch(config)# wireless mobility group keepalive interval 5`	Configures the interval between two keepalives sent to a mobility member.
Step 4	**wireless mobility group keepalive count** *count* **Example:** `Switch(config)# wireless mobility group keepalive count 3`	Configures the keep alive retries before a member status is termed DOWN.

```
Switch(config)# wireless mobility group name Mygroup
Switch(config)# wireless mobility group member ip 10.10.34.10 public-ip 10.10.34.28
Switch(config)# wireless mobility group keepalive interval 5
Switch(config)# wireless mobility group keepalive count 3
```

Configuring Local Mobility Group (GUI)

Before You Begin

Mobility controllers can belong to only one mobility group and can know mobility controllers in several mobility groups.

Step 1 Choose **Controller** > **Mobility Management** > **Mobility Global Config**.

The **Mobility Controller Configuration** page is displayed.

Step 2 Enter the following details:

a) **Mobility Group Name**
b) **Mobility Keepalive Interval**
c) **Mobility Keepalive Count**
d) **Multicast IP Address** if you want to enable multicast mode to send mobile announce messages to the mobility members.

Note If you do not enable multicast IP address, the device uses unicast mode to send mobile announce messages.

Step 3 Click **Apply**.

Step 4 Click **Save Configuration**.

Adding a Peer Mobility Group (CLI)

Before You Begin

MCs belong to only one group, and can know MCs in several groups.

SUMMARY STEPS

1. **wireless mobility group member ip** *member-ip-addr* **public-ip** *public-ip-addr* **group** *group-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wireless mobility group member ip** *member-ip-addr* **public-ip** *public-ip-addr* **group** *group-name* **Example:** `Switch(config)# wireless mobility group member ip 10.10.10.24 public-ip 10.10.10.25 group Group2`	Adds the member as a peer MC in a different group than the Mygroup.

Adding a Peer Mobility Group (GUI)

Before You Begin

Mobility controllers belong to only one group, and can know several mobility groups.

Step 1 Choose **Controller** > **Mobility Management** > **Mobility Peer**.

The **Mobility Peer** page is displayed.

Step 2 Click **New**.

Step 3 Enter the following details:

a) **Mobility Member IP**
b) **Mobility Member Public IP**
c) **Mobility Member Group Name**
d) **Multicast IP Address**

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Configuring Optional Parameters for Roaming Behavior

Use this configuration to disable the sticky anchor. This command can also be used, if required, between all MA's and MC's where roaming is expected for the target SSID.

SUMMARY STEPS

1. **wlan** open21
2. **no mobility anchor sticky**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wlan** open21 **Example:** `Switch(config)# wlan open20`	Configures a WLAN.
Step 2	**no mobility anchor sticky** **Example:** `Switch(config-wlan)# no mobility anchor sticky`	Disables the default sticky mobility anchor.

```
Switch(config)# wlan open20
Switch(config-wlan)# no mobility anchor sticky
```

Pointing the Mobility Controller to a Mobility Oracle (CLI)

Before You Begin

You can configure a mobility oracle on a known mobility controller.

SUMMARY STEPS

1. **wireless mobility group member ip** *member-ip-addr* **group** *group-name*
2. **wireless mobility oracle ip** *oracle-ip-addr*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wireless mobility group member ip** *member-ip-addr* **group** *group-name* **Example:** `Switch(config)# wireless mobility group member ip 10.10.10.10 group Group3`	Creates and adds a MC to a mobility group.
Step 2	**wireless mobility oracle ip** *oracle-ip-addr* **Example:** `Switch(config)# wireless mobility oracle ip 10.10.10.10`	Configures the mobility controller as mobility oracle.

```
Switch(config)# wireless mobility group member ip 10.10.10.10 group Group3
Switch(config)# wireless mobility oracle ip 10.10.10.10
```

Pointing the Mobility Controller to a Mobility Oracle (GUI)

Before You Begin

You can configure a mobility oracle on a known mobility controller.

Step 1 Choose **Controller** > **Mobility Management** > **Mobility Global Config**.
The **Mobility Controller Configuration** page is displayed.

Step 2 Enter the **Mobility Oracle IP Address**.

Note To make the mobility controller itself a mobility oracle, select the **Mobility Oracle Enabled** check box.

Step 3 Click **Apply**.

Step 4 Click **Save Configuration**.

Configuring Guest Controller

A guest controller is used when the client traffic is tunneled to a guest anchor controller in the demilitarized zone (DMZ). The guest client goes through a web authentication process. The web authentication process is optional, and the guest is allowed to pass traffic without authentication too.

Enable the WLAN on the mobility agent on which the guest client connects with the mobility anchor address of the guest controller.

On the guest controller WLAN, which can be Cisco 5500 Series WLC, Cisco WiSM2, or Cisco 5700 Series WLC, configure the IP address of the mobility anchor as its own IP address. This allows the traffic to be tunneled to the guest controller from the mobility agent.

SUMMARY STEPS

1. **wlan** *wlan-id*
2. **mobility anchor** *guest-anchor-ip-addr*
3. **client vlan** *vlan-name*
4. **security open**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wlan** *wlan-id* **Example:** `Switch(config)# wlan Mywlan1`	Creates a WLAN for the client.
Step 2	**mobility anchor** *guest-anchor-ip-addr* **Example:** `Switch(config-wlan)# mobility anchor 10.10.10.2`	Enables the guest anchors (GA) IP address on the MA. **Note** To enable guest anchor on the mobility controller, you need not enter the IP address. Enter the **mobility anchor** command in the WLAN configuration mode to enable GA on the mobility controller.
Step 3	**client vlan** *vlan-name* **Example:** `Switch(config-wlan)# client vlan gc_ga_vlan1`	Assigns a VLAN to the client's WLAN.
Step 4	**security open** **Example:** `Switch(config-wlan)# security open`	Assigns a security type to the WLAN.

```
Switch(config)# wlan Mywlan1
Switch(config-wlan)# mobility anchor 10.10.10.2
Switch(config-wlan)# client vlan gc_ga_vlan1
Switch(config-wlan)# security open
```

Configuring Guest Anchor

SUMMARY STEPS

1. **wlan** Mywlan1
2. **mobility anchor** <guest-anchors-own-ip-address>
3. **client vlan**<vlan-name>
4. **security open**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wlan** Mywlan1 **Example:** `Switch(config)# wlan Mywlan1`	Creates a wlan for the client.
Step 2	**mobility anchor** <guest-anchors-own-ip-address> **Example:** `Switch(config-wlan)# mobility anchor 10.10.10.2`	Enables the guest anchors IP address on the guest anchor (GA). The GA assigns its own address on itself.
Step 3	**client vlan**<vlan-name> **Example:** `Switch(config-wlan)# client vlan gc_ga_vlan1`	Assigns a vlan to the clients wlan.
Step 4	**security open** **Example:** `Switch(config-wlan)# security open`	Assigns a security type to the wlan.

```
Switch(config)# wlan Mywlan1
Switch(config-wlan)# mobility anchor 10.10.10.2
Switch(config-wlan)# client vlan gc_ga_vlan1
Switch(config-wlan)# security open
```