WLAN Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

First Published: January 29, 2013

Last Modified: 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-27618-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2013 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface ix

Document Conventions ix

Related Documentation xi

Obtaining Documentation and Submitting a Service Request xi

CHAPTER 1

Using the Command-Line Interface 1

Information About Using the Command-Line Interface 1

Command Modes 1

Using the Help System 3

Understanding Abbreviated Commands 4

No and Default Forms of Commands 4

CLI Error Messages 4

Configuration Logging 5

How to Use the CLI to Configure Features 5

Configuring the Command History 5

Changing the Command History Buffer Size 6

Recalling Commands 6

Disabling the Command History Feature 7

Enabling and Disabling Editing Features 7

Editing Commands Through Keystrokes 8

Editing Command Lines That Wrap 9

Searching and Filtering Output of show and more Commands 10

Accessing the CLI on a Switch Stack 11

Accessing the CLI Through a Console Connection or Through Telnet 11

CHAPTER 2

Using the Web Graphical User Interface 13

Prerequisites for Using the Web GUI 13

Information About Using The Web GUI 13
Web GUI Features 13
Connecting the Console Port of the Switch 15
Logging On to the Web GUI 15
Enabling Web and Secure Web Modes 15
Configuring the Switch Web GUI 16

CHAPTER 3 Configuring WLANs 21
Finding Feature Information 21
Prerequisites for WLANs 21
Restrictions for WLANs 22
Information About WLANs 23
Band Selection 24
Off-Channel Scanning Defer 24
DTIM Period 25
Session Timeouts 25
Cisco Client Extensions 25
Peer-to-Peer Blocking 26
Diagnostic Channel 26
Per-WLAN Radius Source Support 26
How to Configure WLANs 27
Creating WLANs (CLI) 27
Creating WLANs (GUI) 28
Deleting WLANs (CLI) 29
Deleting WLANs (GUI) 29
Searching WLANs (CLI) 30
Searching WLANs (GUI) 30
Enabling WLANs (CLI) 31
Disabling WLANs (CLI) 32
Configuring General WLAN Properties (CLI) 32
Configuring General WLAN Properties (GUI) 35
Configuring Advanced WLAN Properties (CLI) 36
Configuring Advanced WLAN Properties (GUI) 39
Applying a QoS Policy on a WLAN (GUI) 43
Monitoring WLAN Properties (CLI) 44

Viewing WLAN Properties (GUI) 44
Where to Go Next 45
Additional References 45
Feature Information for WLANs 46

CHAPTER 4 Configuring DHCP for WLANs 47
Finding Feature Information 47
Prerequisites for Configuring DHCP for WLANs 47
Restrictions for Configuring DHCP for WLANs 48
Information About the Dynamic Host Configuration Protocol 48
Internal DHCP Servers 49
External DHCP Servers 49
DHCP Assignments 50
Information About DHCP Option 82 50
Configuring DHCP Scopes 51
Information About DHCP Scopes 51
How to Configure DHCP for WLANs 52
Configuring DHCP for WLANs (CLI) 52
Configuring DHCP Scopes (CLI) 54
Additional References 55
Feature Information for DHCP for WLANs 56

CHAPTER 5 Configuring WLAN Security 57
Finding Feature Information 57
Prerequisites for Layer 2 Security 57
Information About AAA Override 58
How to Configure WLAN Security 59
Configuring Static WEP + 802.1X Layer 2 Security Parameters (CLI) 59
Configuring Static WEP Layer 2 Security Parameters (CLI) 60
Configuring WPA + WPA2 Layer 2 Security Parameters (CLI) 61
Configuring 802.1X Layer 2 Security Parameters (CLI) 62
Configuring Layer 2 Parameters (GUI) 64
Additional References 68
Feature Information about WLAN Layer 2 Security 69

CHAPTER 6 Setting Client Count Per WLAN 71

Finding Feature Information 71

Restrictions for Setting Client Count for WLANs 71

Information About Setting the Client Count per WLAN 72

How to Configure Client Count Per WLAN 72

Configuring Client Count per WLAN (CLI) 72

Configuring Client Count Per AP Per WLAN (CLI) 73

Configuring Client Count per AP Radio per WLAN (CLI) 74

Monitoring Client Connections (CLI) 75

Additional References for Client Connections 76

Feature Information about Client Connections Per WLAN 77

CHAPTER 7 Configuring 802.11w 79

Finding Feature Information 79

Prerequisites for 802.11w 79

Restrictions for 802.11w 80

Information About 802.11w 80

How to Configure 802.11w 81

Configuring 802.11w (CLI) 81

Disabling 802.11w (CLI) 83

Monitoring 802.11w (CLI) 84

Additional References for 802.11w 85

Feature Information for 802.11w 86

CHAPTER 8 Configuring Wi-Fi Direct Client Policy 89

Finding Feature Information 89

Restrictions for the Wi-Fi Direct Client Policy 89

Information About the Wi-Fi Direct Client Policy 89

How to Configure Wi-Fi Direct Client Policy 90

Configuring the Wi-Fi Direct Client Policy (CLI) 90

Disabling Wi-Fi Direct Client Policy (CLI) 91

Monitoring Wi-Fi Direct Client Policy (CLI) 92

Additional References for Wi-Fi Direct Client Policy 92

Feature Information about Wi-Fi Direct Client Policy 93

CHAPTER 9 Configuring 802.11r BSS Fast Transition 95

Finding Feature Information 95
Restrictions for 802.11r Fast Transition 95
Information About 802.11r Fast Transition 96
How to Configure 802.11r Fast Transition 99
Configuring 802.11r Fast Transition in an Open WLAN (CLI) 99
Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI) 101
Configuring 802.11r Fast Transition on a PSK Security Enabled WLAN (CLI) 102
Configuring 802.11 Fast Transition (GUI) 104
Disabling 802.11r Fast Transition (CLI) 104
Monitoring 802.11r Fast Transition (CLI) 105
Additional References for 802.11r Fast Transition 106
Feature Information for 802.11r Fast Transition 107

CHAPTER 10 Configuring Assisted Roaming 109

Finding Feature Information 109
Restrictions for Assisted Roaming 109
Information About Assisted Roaming 110
How to Configure Assisted Roaming 111
Configuring Assisted Roaming (CLI) 111
Monitoring Assisted Roaming 113
Configuration Examples for Assisted Roaming 113
Additional References for Assisted Roaming 114
Feature History and Information For Performing Assisted Roaming Configuration 115

CHAPTER 11 Configuring Access Point Groups 117

Finding Feature Information 117
Prerequisites for Configuring AP Groups 117
Restrictions for Configuring Access Point Groups 118
Information About Access Point Groups 118
How to Configure Access Point Groups 120
Creating Access Point Groups 120
Assigning an Access Point to an AP Group 121
Viewing Access Point Group 121

Additional References 122

Feature History and Information for Access Point Groups 123

Preface

- Document Conventions, page ix
- Related Documentation, page xi
- Obtaining Documentation and Submitting a Service Request, page xi

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 3850 Switch documentation, located at:

  http://www.cisco.com/go/cat3850_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

- Cisco Validated Designs documents, located at:

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

- Error Message Decoder, located at:

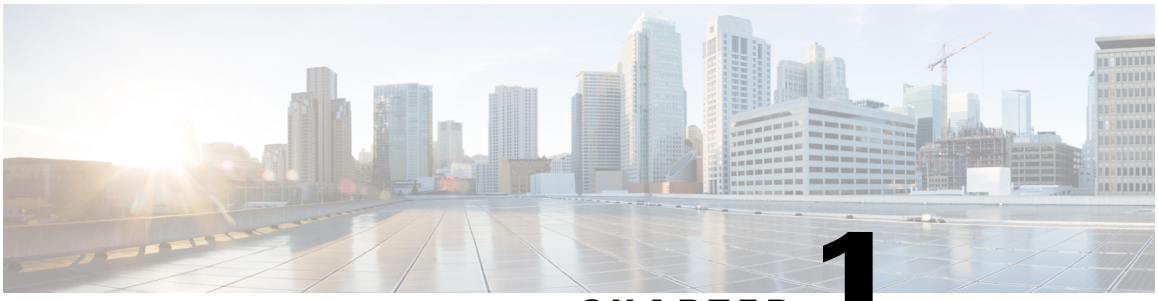
  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

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/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, page 1
- How to Use the CLI to Configure Features, page 5

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

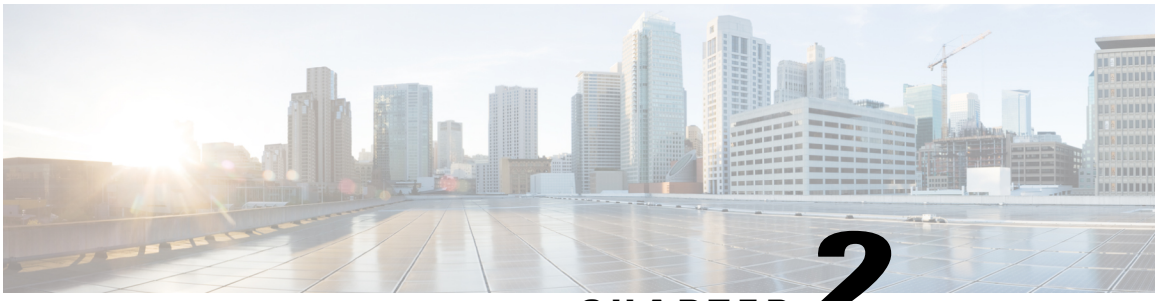
Before you can access the CLI, you must connect a terminal or a PC to the switch console or connect a PC to the Ethernet management port and then power on the switch, as described in the hardware installation guide that shipped with your switch.

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, page 13
- Information About Using The Web GUI, page 13
- Connecting the Console Port of the Switch , page 15
- Logging On to the Web GUI, page 15
- Enabling Web and Secure Web Modes , page 15
- Configuring the Switch Web GUI, page 16

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-CT3850 page appears.

Enabling Web and Secure Web Modes

Step 1 Choose **Configuration** > **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 **<Model Number> <Hostname>** page appears.

Step 3 On the 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**.

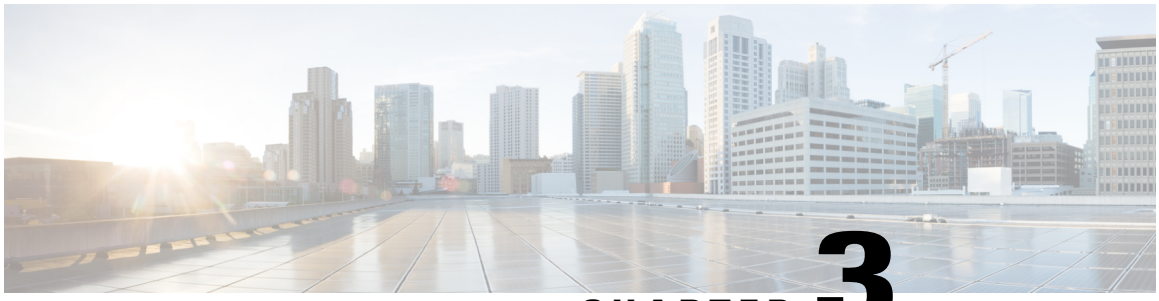
- Displays current timestamp on the switch in the Current Time text box.
- Choose either Manual or NTP from the Mode drop-down list.

  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

Configuring WLANs

- Finding Feature Information, page 21
- Prerequisites for WLANs, page 21
- Restrictions for WLANs, page 22
- Information About WLANs, page 23
- How to Configure WLANs, page 27
- Monitoring WLAN Properties (CLI), page 44
- Viewing WLAN Properties (GUI), page 44
- Where to Go Next, page 45
- Additional References, page 45
- Feature Information for WLANs, page 46

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. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Prerequisites for WLANs

- You can associate up to 16 WLANs with each access point group and assign specific access points to each group. Each access point advertises only the enabled WLANs that belong to its access point group. The access point (AP) does not advertise disabled WLANs in its access point group or WLANs that belong to another group.

- We recommend that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that controllers properly route VLAN traffic.
- The controller uses different attributes to differentiate between WLANs with the same Service Set Identifier (SSID).
  - WLANs with the same SSID and same Layer 2 policy cannot be created if the WLAN ID is lower than 17.
  - Two WLANs with IDs that are greater than 17 and that have the same SSID and same Layer 2 policy is allowed if WLANs are added in different AP groups.

Note This requirement ensures that clients never detect the SSID present on the same access point radio.

Related Topics

Creating WLANs (CLI), on page 27
Creating WLANs (GUI), on page 28
Configuring General WLAN Properties (CLI), on page 32
Configuring General WLAN Properties (GUI), on page 35
Deleting WLANs (CLI), on page 29
Configuring Advanced WLAN Properties (CLI), on page 36
Configuring Advanced WLAN Properties (GUI), on page 39
Band Selection, on page 24
Off-Channel Scanning Defer
DTIM Period
Session Timeout
Cisco Client Extensions, on page 25
Peer-to-Peer Blocking, on page 26
Diagnostic Channel
Client Count Per WLAN
Enabling WLANs (CLI), on page 31
Disabling WLANs (CLI), on page 32

Restrictions for WLANs

- Peer-to-peer blocking does not apply to multicast traffic.
- You can configure a maximum up to of 2000 clients.
- The WLAN name and SSID can have up to 32 characters. Spaces are not allowed in the WLAN profile name and SSID.
- You cannot map a WLAN to VLAN0, and you cannot map VLANs 1002 to 1006.

- Dual stack clients with a static-IPv4 address is not supported.
- When creating a WLAN with the same SSID, you must create a unique profile name for each WLAN.
- When multiple WLANs with the same SSID get assigned to the same AP radio, you must have a unique Layer 2 security policy so that clients can safely select between them.

Caution Some clients might not be able to connect to WLANs properly if they detect the same SSID with multiple security policies. Use this feature with care.

Related Topics

Creating WLANs (CLI), on page 27
Creating WLANs (GUI), on page 28
Configuring General WLAN Properties (CLI), on page 32
Configuring General WLAN Properties (GUI), on page 35
Deleting WLANs (CLI), on page 29
Configuring Advanced WLAN Properties (CLI), on page 36
Configuring Advanced WLAN Properties (GUI), on page 39
Band Selection, on page 24
Off-Channel Scanning Defer
DTIM Period
Session Timeout
Cisco Client Extensions, on page 25
Peer-to-Peer Blocking, on page 26
Diagnostic Channel
Client Count Per WLAN
Enabling WLANs (CLI), on page 31
Disabling WLANs (CLI), on page 32

Information About WLANs

This feature enables you to control up to 64 WLANs for lightweight access points. Each WLAN has a separate WLAN ID, a separate profile name, and a WLAN SSID. All switches publish up to 16 WLANs to each connected access point, but you can create up to the maximum number of WLANs supported and then selectively publish these WLANs (using access point groups) to different access points to better manage your wireless network.

You can configure WLANs with different SSIDs or with the same SSID. An SSID identifies the specific wireless network that you want the switch to access.

Band Selection

Band selection enables client radios that are capable of dual-band (2.4- and 5-GHz) operation to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of three nonoverlapping channels. To prevent these sources of interference and improve overall network performance, you can configure band selection on the controller.

Band selection works by regulating probe responses to clients. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels.

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 36
Configuring Advanced WLAN Properties (GUI), on page 39
Prerequisites for WLANs, on page 21
Restrictions for WLANs, on page 22

Off-Channel Scanning Defer

In deployments with certain power-save clients, you sometimes need to defer the Radio Resource Management's (RRM) normal off-channel scanning to avoid missing critical information from low-volume clients (for example, medical devices that use power-save mode and periodically send telemetry information). This feature improves the way that Quality of Service (QoS) interacts with the RRM scan defer feature.

You can use a client's Wi-Fi Multimedia (WMM) UP marking to configure the access point to defer off-channel scanning for a configurable period of time if it receives a packet marked UP.

Off-Channel Scanning Defer is essential to the operation of RRM, which gathers information about alternate channel choices such as noise and interference. Additionally, Off-Channel Scanning Defer is responsible for rogue detection. Devices that need to defer Off-Channel Scanning Defer should use the same WLAN as often as possible. If there are many of these devices (and the possibility exists that Off-Channel Defer scanning could be completely disabled by the use of this feature), you should implement an alternative to local AP Off-Channel Scanning Defer, such as monitoring access points, or other access points in the same location that do not have this WLAN assigned.

You can assign a QoS policy (bronze, silver, gold, and platinum) to a WLAN to affect how packets are marked on the downlink connection from the access point regardless of how they were received on the uplink from the client. UP=1,2 is the lowest priority, and UP=0,3 is the next higher priority. The marking results of each QoS policy are as follows:

- Bronze marks all downlink traffic to UP= 1.
- Silver marks all downlink traffic to UP= 0.
- Gold marks all downlink traffic to UP=4.
- Platinum marks all downlink traffic to UP=6.

DTIM Period

In the 802.11 networks, lightweight access points broadcast a beacon at regular intervals, which coincides with the Delivery Traffic Indication Map (DTIM). After the access point broadcasts the beacon, it transmits any buffered broadcast and multicast frames based on the value set for the DTIM period. This feature allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.

Typically, the DTIM value is set to 1 (to transmit broadcast and multicast frames after every beacon) or 2 (to transmit after every other beacon). For instance, if the beacon period of the 802.11 network is 100 ms and the DTIM value is set to 1, the access point transmits buffered broadcast and multicast frames 10 times per second. If the beacon period is 100 ms and the DTIM value is set to 2, the access point transmits buffered broadcast and multicast frames 5 times per second. Either of these settings are suitable for applications, including Voice Over IP (VoIP), that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (to transmit broadcast and multicast frames after every 255th beacon) if all 802.11 clients have power save enabled. Because the clients have to listen only when the DTIM period is reached, they can be set to listen for broadcasts and multicasts less frequently which results in a longer battery life. For example, if the beacon period is 100 ms and you set the DTIM value to 100, the access point transmits buffered broadcast and multicast frames once every 10 seconds. This rate allows the power-saving clients to sleep longer before they have to wake up and listen for broadcasts and multicasts, which results in a longer battery life.

Note A beacon period, which is specified in milliseconds on the controller, is converted internally by the software to 802.11 Time Units (TUs), where 1 TU = 1.024 milliseconds. On Cisco's 802.11n access points, this value is rounded to the nearest multiple of 17 TUs. For example, a configured beacon period of 100 ms results in an actual beacon period of 104 ms.

Many applications cannot tolerate a long time between broadcast and multicast messages, which results in poor protocol and application performance. We recommend that you set a low DTIM value for 802.11 networks that support such clients.

Session Timeouts

You can configure a WLAN with a session timeout. The session timeout is the maximum time for a client session to remain active before requiring reauthorization.

Cisco Client Extensions

The Cisco Client Extensions (CCX) software is licensed to manufacturers and vendors of third-party client devices. The CCX code resident on these clients enables them to communicate wirelessly with Cisco access points and to support Cisco features that other client devices do not, including those features that are related to increased security, enhanced performance, fast roaming, and power management.

- The software supports CCX versions 1 through 5, which enables controllers and their access points to communicate wirelessly with third-party client devices that support CCX. CCX support is enabled automatically for every WLAN on the controller and cannot be disabled. However, you can configure Aironet information elements (IEs).

- If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the controller sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the controller and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 36
Configuring Advanced WLAN Properties (GUI), on page 39
Prerequisites for WLANs, on page 21
Restrictions for WLANs, on page 22

Peer-to-Peer Blocking

Peer-to-peer blocking is applied to individual WLANs, and each client inherits the peer-to-peer blocking setting of the WLAN to which it is associated. Peer-to-Peer enables you to have more control over how traffic is directed. For example, you can choose to have traffic bridged locally within the switch, dropped by the switch, or forwarded to the upstream VLAN.

Peer-to-peer blocking is supported for clients that are associated with the local switching WLAN.

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 36
Configuring Advanced WLAN Properties (GUI), on page 39
Prerequisites for WLANs, on page 21
Restrictions for WLANs, on page 22

Diagnostic Channel

You can choose a diagnostic channel to troubleshoot why the client is having communication problems with a WLAN. You can test the client and access points to identify the difficulties that the client is experiencing and allow corrective measures to be taken to make the client operational on the network. You can use the controller GUI or CLI to enable the diagnostic channel, and you can use the controller CLI to run the diagnostic tests.

Note We recommend that you enable the diagnostic channel feature only for nonanchored SSIDs that use the management interface.

Per-WLAN Radius Source Support

By default, the switch sources all RADIUS traffic from the IP address on its management interface, which means that even if a WLAN has specific RADIUS servers configured instead of the global list, the identity used is the management interface IP address.

If you want to filter WLANs, you can use the callStationID that is set by RFC 3580 to be in the APMAC:SSID format. You can also extend the filtering on the authentication server to be on a per-WLAN source interface by using the NAS-IP-Address attribute.

When you enable the per-WLAN RADIUS source support, the switch sources all RADIUS traffic for a particular WLAN by using the dynamic interface that is configured. Also, RADIUS attributes are modified accordingly to match the identity. This feature virtualizes the switch on the per-WLAN RADIUS traffic, where each WLAN can have a separate layer 3 identity. This feature is useful in deployments that integrate with ACS Network Access Restrictions and Network Access Profiles.

You can combine per-WLAN RADIUS source support with the normal RADIUS traffic source and some WLANs that use the management interface and others using the per-WLAN dynamic interface as the address source.

How to Configure WLANs

Creating WLANs (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name wlan-id* [*ssid*]
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id* [*ssid*] **Example:** `Switch(config)# wlan mywlan 34 mywlan-ssid`	Specifies the WLAN name and ID: • For the *profile-name*, enter the profile name. The range is from 1 to 32 alphanumeric characters. • For the *wlan-id*, enter the WLAN ID. The range is from 1 to 512. • For the *ssid*, enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID. **Note** By default, the WLAN is disabled.

	Command or Action	Purpose
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for WLANs, on page 21
Restrictions for WLANs, on page 22

Creating WLANs (GUI)

Step 1 Click **Configuration** > **Wireless**.
The **WLANs** page is displayed.

Step 2 Click **New** to create a WLAN.
The **WLANs** > **Create New** page is displayed.

Step 3 Enter the following parameters:

Parameter	Description
WLAN ID	WLAN identifier. The value ranges from 1 to 512.
SSID	Broadcast name of the WLAN.
Profile	WLAN profile name.

Step 4 Click **Apply**.

Related Topics

Prerequisites for WLANs, on page 21
Restrictions for WLANs, on page 22

Deleting WLANs (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **no wlan** *wlan-name wlan-id ssid*
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**no wlan** *wlan-name wlan-id ssid* **Example:** `Switch(config)# no wlan test2`	Deletes the WLAN. The arguments are as follows: • The *wlan-name* is the WLAN profile name. • The *wlan-id* is the WLAN ID. • The *ssid* is the WLAN SSID name configured for the WLAN. **Note** If you delete a WLAN that is part of an AP group, the WLAN is removed from the AP group and from the AP's radio.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for WLANs, on page 21
Restrictions for WLANs, on page 22

Deleting WLANs (GUI)

Step 1 Click **Configuration** > **Wireless**.
The **WLANs** page is displayed.

Step 2 Select the checkbox corresponding to the WLAN you want to delete.
Note If you delete a WLAN that is part of an AP group, the WLAN is removed from the AP group and from the AP's radio.

Step 3 Click **Remove**.

Searching WLANs (CLI)

SUMMARY STEPS

1. **show wlan summary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show wlan summary** **Example:** `Switch# show wlan summary`	Displays the list of all WLANs configured on the device. You can search for the WLAN in the output.

```
Switch# show wlan summary
Number of WLANs: 4

WLAN Profile Name                     SSID                           VLAN Status
-------------------------------------------------------------------------------
1    test1                             test1-ssid                     137  UP
3    test2                             test2-ssid                     136  UP
2    test3                             test3-ssid                     1    UP
45   test4                             test4-ssid                     1    DOWN
```

You can also use wild cards to search WLANs. For example **show wlan summary include** | *variable*. Where variable is any search string in the output.

```
Switch# show wlan summary | include test-wlan-ssid
1    test-wlan                        test-wlan-ssid                   137   UP
```

Searching WLANs (GUI)

Step 1 Click **Configuration** > **Wireless**.
The **WLANs** page is displayed.

Step 2 Type the first few characters in the text box above the column you are searching. Fo For example, to search the WLAN based on the **Profile**, type the first few characters of the profile name.
You can search a WLAN based on the following criteria:

- **Profile**
- **ID**
- **SSID**

- **VLAN**
- **Status**

If a WLAN exists, it would appear based on the accuracy of the match.

Enabling WLANs (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **no shutdown**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Enables the WLAN.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for WLANs, on page 21
Restrictions for WLANs, on page 22

Disabling WLANs (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **shutdown**
4. **end**
5. **show wlan summary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**shutdown** **Example:** `Switch(config-wlan)# shutdown`	Disables the WLAN.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 5	**show wlan summary** **Example:** `Switch# show wlan summary`	Displays the list of all WLANs configured on the device. You can search for the WLAN in the output.

Related Topics

Prerequisites for WLANs, on page 21
Restrictions for WLANs, on page 22

Configuring General WLAN Properties (CLI)

You can configure the following properties:

- Media stream
- Broadcast SSID
- Call Snooping
- Radio
- Interface
- Status

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **shutdown**
4. **broadcast-ssid**
5. **radio** {**all** | **dot11a** | **dot11ag** | **dot11bg** | **dot11g**}
6. **client vlan** *vlan-identifier*
7. **ip multicast vlan** *vlan-name*
8. **media-stream multicast-direct**
9. **call-snoop**
10. **no shutdown**
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**shutdown** **Example:** `Switch# shutdown`	Disables the WLAN before configuring the parameters.
Step 4	**broadcast-ssid** **Example:** `Switch(config-wlan)# broadcast-ssid`	Broadcasts the SSID for this WLAN. This field is enabled by default.

	Command or Action	Purpose
Step 5	**radio** {**all** | **dot11a** | **dot11ag** | **dot11bg** | **dot11g**} **Example:** `Switch# radio all`	Enables radios on the WLAN. The keywords are as follows: • **all**—Configures the WLAN on all radio bands. • **dot1a**—Configures the WLAN on only 802.11a radio bands. • **dot11g**—Configures the WLAN on 802.11ag radio bands. • **dot11bg**—Configures the WLAN on only 802.11b/g radio bands (only 802.11b if 802.11g is disabled). • **dot11ag**— Configures the wireless LAN on 802.11g radio bands only.
Step 6	**client vlan** *vlan-identifier* **Example:** `Switch# client vlan test-vlan`	Enables an interface group on the WLAN. *vlan-identifier*—Specifies the VLAN identifier. This can be the VLAN name, VLAN ID, or VLAN group name.
Step 7	**ip multicast vlan** *vlan-name* **Example:** `Switch(config-wlan)# ip multicast vlan test`	Enables IP multicast on a WLAN. The keywords are as follows: • **vlan**—Specifies the VLAN ID. • *vlan-name*—Specifies the VLAN name.
Step 8	**media-stream multicast-direct** **Example:** `Switch(config-wlan)# media-stream multicast-direct`	Enables multicast VLANs on this WLAN.
Step 9	**call-snoop** **Example:** `Switch(config-wlan)# call-snoop`	Enables call-snooping support.
Step 10	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Enables the WLAN.
Step 11	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for WLANs, on page 21
Restrictions for WLANs, on page 22

Configuring General WLAN Properties (GUI)

Use this procedure to perform the following actions on a WLAN:

- Set WLAN Status
- Configure Radio Policies
- Assign Interface/Interface Groups
- Enable or Disable Multicast VLAN Feature
- Enable or Disable Broadcast SSID Feature

Before You Begin

Step 1 Click **Configuration** > **Wireless**.
The **WLANs** page is displayed.

Step 2 Locate the WLAN you want to configure by using the search mechanisms on the page.

Step 3 Click on the **WLAN Profile** of the WLAN.
The **WLAN** > **Edit** page is displayed.

Step 4 Click the **General** tab. This tab is displayed by default.

Step 5 Configure the **General** parameters.

Parameter	Description
Profile Name	Displays the configured profile name of the WLAN.
Type	Displays the configured LAN type.
SSID	Displays the configured SSID of the WLAN.
Status	Check box to enable the WLAN. The default value is enabled.
Security Policies	WLAN security policies set using the Security tab.
Radio Policy	WLAN radio policy to enable radios on the WLAN. Values are the following: • All • 802.11a only • 802.11g only • 802.11a/g only • 802.11b/g only

Parameter	Description
Interface/Interface Group	Interface or interface group that you want this WLAN to be mapped. Displays the non-service port and non-virtual interface names configured on the **Interfaces** page. **Note** This field displays a drop down box only when the VLAN for a WLAN is mapped using a existing VLAN name on the controller.
Broadcast SSID	Check box to broadcast this SSID. The default is enabled.
Multicast VLAN Feature	Check box to enable the multicast VLAN. The default is disabled. **Note** The Multicast Interface field appears only after you enable the Multicast VLAN feature text box. **Note** You have to configure the multicast VLAN feature only once if you want to use the multicast feature.

Step 6 Click **Apply**.

What to Do Next

Proceed to configure the Security, QoS, and Advanced Properties.

Related Topics

Prerequisites for WLANs, on page 21
Restrictions for WLANs, on page 22

Configuring Advanced WLAN Properties (CLI)

You can configure the following advanced properties:

- AAA Override
- Coverage Hole Detection
- Session Timeout
- Cisco Client Extensions
- Diagnostic Channels
- Interface Override ACLs
- P2P Blocking
- Client Exclusion
- Maximum Clients Per WLAN
- Off Channel Scan Defer

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **aaa-override**
4. **chd**
5. **session-timeout** *time-in-seconds*
6. **ccx aironet-iesupport**
7. **diag-channel**
8. **ip access-group** [web] *acl-name*
9. **peer-blocking** [**drop** | **forward-upstream**]
10. **exclusionlist** *time-in-seconds*
11. **client association limit** *max-number-of-clients*
12. **channel-scan defer-priority** {**defer-priority** {**0-7**} | **defer-time** {**0 - 6000**}}
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**aaa-override** **Example:** `Switch(config-wlan)# aaa-override`	Enables AAA override.
Step 4	**chd** **Example:** `Switch(config-wlan)# chd`	Enables coverage hole detection for this WLAN. This field is enabled by default.
Step 5	**session-timeout** *time-in-seconds* **Example:** `Switch(config-wlan)# session-timeout 450`	Sets the session timeout in seconds. The range and default values vary according to the security configuration. If the WLAN security is configured to dot1x, the range is 300 to 86400 seconds and the default value is 1800 seconds. For all other WLAN security configurations, the range is 1 to 65535 seconds and the default value is 0 seconds. A value of 0 indicates no session timeout.

	Command or Action	Purpose
Step 6	**ccx aironet-iesupport** **Example:** `Switch(config-wlan)# ccx aironet-iesupport`	Enables support for Aironet IEs for this WLAN. This field is enabled by default.
Step 7	**diag-channel** **Example:** `Switch(config-wlan)# diag-channel`	Enables diagnostic channel support to troubleshoot client communication issues on a WLAN.
Step 8	**ip access-group** [web] *acl-name* **Example:** `Switch(config)# ip access-group test-acl-name`	Configures the WLAN ACL group. The variable *acl-name* specifies the user-defined IPv4 ACL name. The keyword **web** specifies the IPv4 web ACL.
Step 9	**peer-blocking** [**drop** | **forward-upstream**] **Example:** `Switch(config)# peer-blocking drop`	Configures peer to peer blocking parameters. The keywords are as follows: • **drop—**Enables peer-to-peer blocking on the drop action. • **forward-upstream—**Enables peer-to-peer blocking on the forward upstream action.
Step 10	**exclusionlist** *time-in-seconds* **Example:** `Switch(config)# exclusionlist 10`	Specifies the timeout in seconds. The valid range is from 0 to 2147483647. Enter 0 for no timeout. A zero (0) timeout indicates that the client is permanently added to the exclusion list.
Step 11	**client association limit** *max-number-of-clients* **Example:** `Switch(config)# client association limit 200`	Sets the maximum number of clients that can be configured on a WLAN.
Step 12	**channel-scan defer-priority** {**defer-priority** {**0-7**} | **defer-time** {**0 - 6000**}} **Example:** `Switch(config)# channel-scan defer-priority 6`	Sets the channel scan defer priority and defer time. The arguments are as follows: • **defer-priority—**Specifies the priority markings for packets that can defer off-channel scanning. The range is from 0 to 7. The default is 3. • **defer-time—**Deferral time in milliseconds. The range is from 0 to 6000. The default is 100.
Step 13	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Band Selection, on page 24
Off-Channel Scanning Defer
DTIM Period
Session Timeout
Cisco Client Extensions, on page 25
Peer-to-Peer Blocking, on page 26
Diagnostic Channel
Client Count Per WLAN
Prerequisites for WLANs, on page 21
Restrictions for WLANs, on page 22
Information About AAA Override, on page 58
Prerequisites for Layer 2 Security, on page 57

Configuring Advanced WLAN Properties (GUI)

Before You Begin

Step 1 Click **Configuration** > **Wireless**.
The **WLANs** page is displayed.

Step 2 Locate the WLAN you want to configure by using the search mechanisms on the page.

Step 3 Click on the **WLAN Profile** of the WLAN.
The **WLAN** > **Edit** page is displayed.

Step 4 Click on the **Advanced Properties** tab.

Step 5 Configure the **Advanced** properties.

Parameter	Description
Allow AAA Override	AAA override for global WLAN parameters that you can enable or disable. When AAA Override is enabled, and a client has conflicting AAA and switches WLAN authentication parameters, client authentication is performed by the AAA server. As part of this authentication, the operating system moves clients from the default Cisco WLAN Solution WLAN VLAN to a VLAN returned by the AAA server and predefined in the switches interface configuration. In all cases, the operating system also uses QoS, DSCP, 802.1p priority tag values, and ACLs provided by the AAA server, if they are predefined in the switches interface configuration. (This VLAN switching by AAA Override is also referred to as Identity Networking.) If the Corporate WLAN primarily uses a Management Interface assigned to VLAN 2, and if AAA Override returns a redirect to VLAN 100, the operating system redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned. When AAA Override is disabled, all client authentication defaults to the switches authentication parameter settings, and authentication is performed only by the AAA server if the switches WLAN does not contain any client-specific authentication parameters. The AAA override values might come from a RADIUS server, for example.
Coverage Hole Detection	Coverage hole detection (CHD) on this WLAN that you can enable or disable. By default, CHD is enabled on all WLANs on the switches. You can disable CHD on a WLAN. When you disable CHD on a WLAN, a coverage hole alert is still sent to the Switch, but no other processing is done to mitigate the coverage hole. This feature is useful for guest WLANs where guests are connected to your network for short periods of time and are likely to be highly mobile.
Session Timeout	Configure a WLAN with a session timeout in seconds. The session timeout is the maximum time for a client session to remain active before requiring reauthorization. Entering zero denotes the session will never expire.
Aironet IE	Support of Aironet IEs per WLAN that you can enable or disable. The default is disabled.
Diagnostic Channel	Diagnostic channel support on the WLAN that you can enable or disable. The default is disabled.
P2P Blocking Action	Peer-to-peer blocking settings that you can choose from the following: • Disabled—(Default) Disables peer-to-peer blocking and bridges traffic locally within the controller whenever possible. • Drop—Causes the switches to discard the packets. • Forward-UpStream—Causes the packets to be forwarded on the upstream VLAN. The device above the switches decides what action to take regarding the packets.

Parameter	Description
Client Exclusion	Timeout in seconds for disabled client machines that you can enable or disable. Client machines are disabled by their MAC address and their status can be observed on the Clients > Details page. A timeout setting of 0 indicates that the client is disabled permanently. Administrative control is required to reenable the client. The default is enabled and the timeout setting is configured as 60 seconds.
Timeout Value (secs)	
Max Allowed Client	Maximum clients allowed per Switch. You can set a limit to the number of clients that can connect to a WLAN. This feature is useful in scenarios where you have a limited number of clients that can connect to a Switch. You can set a limit on the number of guest clients that can access a given WLAN. The number of clients that you can configure per WLAN depends on the platform that you are using. A maximum of up to 12000 clients are supported. **Note** The maximum number of clients per WLAN feature is supported only for access points that are in connected mode.
DHCP	
DHCP Server IP Address	Enter the DHCP server on the WLAN that overrides the DHCP server address on the interface assigned to the WLAN.
DHCP Address Assignment Required	Enables the DHCP address assignment and makes it mandatory for clients to get their IP address from the DHCP server.
DHCP Option 82	Enables the DHCP82 payload on the WLAN.
DHCP option 82 Format	Specifies the DHCP option 82 format. Valus are as follows: • add-ssid— Set RemoteID format that is the AP radio MAC address and SSID. • ap-ethmac—Set RemoteID format that is the AP Ethernet MAC address. **Note** If the format option is not configured, only the AP radio MAC address is used.
DHCP Option ASCII Mode	Configures ASCII for DHCP Option 82. If this is not configured, the option 82 format is set to ASCII format.
DHCP Option 82 RID Mode	Adds the Cisco 2 byte RID for DHCP option 82.
NAC	
NAC State	Enables the NAC on the WLAN.
Off Channel Scanning Defer	

Parameter	Description
Scan Differ Priority	Defer priority for the channel scan that you can assign by clicking on the priority argument. The valid range for the priority is 0 to 7. The priority is 0 to 7 (this value should be set to 6 on the client and on the WLAN). Multiple values can be set. The default values are 4, 5 and 6.
Scan Differ Time	Channel scan defer time in milliseconds that you can assign. The valid range is 100 (default) to 60000 (60 seconds). This setting should match the requirements of the equipment on your wireless LAN.
Override Interface ACL	
IPv4 ACL	The WLANs IPv4 ACL group. Values are as follow: • Un-configured • Pre-auth_ipv4_acl
IPv6 ACL	The WLANs IPv6 ACL group. Values are as follow: • Un-configured • Pre-auth_ipv6_acl

Step 6 Click **Apply**.

Related Topics

Band Selection, on page 24
Off-Channel Scanning Defer
DTIM Period
Session Timeout
Cisco Client Extensions, on page 25
Peer-to-Peer Blocking, on page 26
Diagnostic Channel
Client Count Per WLAN
Prerequisites for WLANs, on page 21
Restrictions for WLANs, on page 22
Information About the Dynamic Host Configuration Protocol, on page 48
Internal DHCP Servers, on page 49
External DHCP Servers, on page 49
DHCP Assignments, on page 50
Information About DHCP Option 82, on page 50

Configuring DHCP Scopes, on page 51
Information About DHCP Scopes, on page 51
Prerequisites for Configuring DHCP for WLANs, on page 47
Restrictions for Configuring DHCP for WLANs, on page 48

Applying a QoS Policy on a WLAN (GUI)

Step 1 Choose **Configuration** > **Wireless**.

Step 2 Expand the **WLAN** node by clicking on the left pane and choose **WLANs**.
The **WLANs** page is displayed.

Step 3 Select the WLAN for which you want to configure the QoS policies by clicking on the WLAN **Profile**.

Step 4 Click the QoS tab to configure the QoS policies on the WLAN.
The following options are available:

Parameter	Description
QoS SSID Policy	
Downstream QoS Policy	QoS downstream policy configuration. The **Existing Policy** column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the **Assign Policy** column.
Upstream QoS Policy	QoS upstream policy configuration. The **Existing Policy** column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the **Assign Policy** column.
QoS Client Policy	
Downstream QoS Policy	QoS downstream policy configuration. The **Existing Policy** column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the **Assign Policy** column.
Upstream QoS Policy	QoS upstream policy configuration. The **Existing Policy** column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the **Assign Policy** column.
WMM	
WMM Policy	WMM Policy. Values are the following: • Disabled—Disables this WMM policy. • Allowed—Allows the clients to communicate with the WLAN. • Required—Ensures that it is mandatory for the clients to have WMM features enabled on them to communicate with the WLAN.

Step 5 Click **Apply**.

Monitoring WLAN Properties (CLI)

Command	Description
show wlan id *wlan-id*	Displays WLAN properties based on the WLAN ID.
show wlan name *wlan-name*	Displays WLAN properties based on the WLAN name.
show wlan all	Displays WLAN properties of all configured WLANs.
show wlan summary	Displays a summary of all WLANs. The summary details includes the following information: • WLAN ID • Profile name • SSID • VLAN • Status
show running-config wlan *wlan-name*	Displays the running configuration of a WLAN based on the WLAN name.
show running-config *wlan*	Displays the running configuration of all WLANs.

Viewing WLAN Properties (GUI)

Before You Begin

- You must have administrator privileges.

Step 1 Select **Configuration** > **WLAN**
The WLANs page is displayed.

Step 2 Click the **WLAN Profile** link.

The **WLANs** > **Edit** page is displayed. The WLANs page contains the following tabs:

- General : Displays the WLAN general properties.
- Security: Displays the security properties. The properties include Layer 2, Layer 3, and AAA properties.
- QoS: Displays the QoS configuration properties.
- Advanced: Displays the advanced properties.

Where to Go Next

Proceed to configure DHCP for WLANs.

Additional References

Related Documents

Related Topic	Document Title
WLAN command reference	*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
Mobility Anchor configuration	*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
WebAuth Configuration	*Security Configuration Guide (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

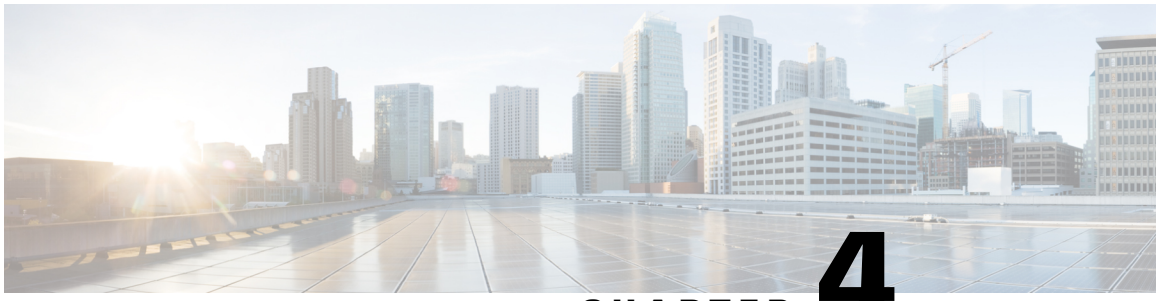
Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for WLANs

This table lists the features in this module and provides links to specific configuration information:

Feature	Release	Modification
WLAN Functionality	Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 4

Configuring DHCP for WLANs

- Finding Feature Information, page 47
- Prerequisites for Configuring DHCP for WLANs, page 47
- Restrictions for Configuring DHCP for WLANs, page 48
- Information About the Dynamic Host Configuration Protocol, page 48
- How to Configure DHCP for WLANs, page 52
- Additional References, page 55
- Feature Information for DHCP for WLANs, page 56

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. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Prerequisites for Configuring DHCP for WLANs

- To be able to use the DHCP option 82, you must configure DHCP on Cisco IOS software. By default, DHCP option 82 is enabled for all clients. You can control the wireless client behavior using the WLAN suboptions.

Related Topics

Configuring DHCP for WLANs (CLI), on page 52

Configuring Advanced WLAN Properties (GUI), on page 39

Information About the Dynamic Host Configuration Protocol, on page 48

Internal DHCP Servers, on page 49
External DHCP Servers, on page 49
DHCP Assignments, on page 50
Information About DHCP Option 82, on page 50
Configuring DHCP Scopes, on page 51
Information About DHCP Scopes, on page 51

Restrictions for Configuring DHCP for WLANs

- If you override the DHCP server in a WLAN, you must ensure that you configure the underlying Cisco IOS configuration to make sure that the DHCP server is reachable.
- WLAN DHCP override works only if DHCP service is enabled on the controller.

  You can configure DHCP service in the following ways:

  - Configuring the DHCP pool on the controller.
  - Configuring a DHCP relay agent on the SVI. Note: the VLAN of the SVI must be mapped to the WLAN where DHCP override is configured.

Related Topics

Configuring DHCP for WLANs (CLI), on page 52
Configuring Advanced WLAN Properties (GUI), on page 39
Information About the Dynamic Host Configuration Protocol, on page 48
Internal DHCP Servers, on page 49
External DHCP Servers, on page 49
DHCP Assignments, on page 50
Information About DHCP Option 82, on page 50
Configuring DHCP Scopes, on page 51
Information About DHCP Scopes, on page 51

Information About the Dynamic Host Configuration Protocol

You can configure WLANs to use the same or different Dynamic Host Configuration Protocol (DHCP) servers or no DHCP server. Two types of DHCP servers are available: internal and external.

Related Topics

Configuring DHCP for WLANs (CLI), on page 52
Configuring Advanced WLAN Properties (GUI), on page 39
Prerequisites for Configuring DHCP for WLANs, on page 47
Restrictions for Configuring DHCP for WLANs, on page 48

Internal DHCP Servers

The switches contain an internal DHCP server. This server is typically used in branch offices that do not already have a DHCP server. The wireless network generally contains a maximum of 10 access points or fewer, with the access points on the same IP subnet as the switch. The internal server provides DHCP addresses to wireless clients, direct-connect access points, and DHCP requests that are relayed from access points. Only lightweight access points are supported. When you want to use the internal DHCP server, you must set the management interface IP address of the switch as the DHCP server IP address.

DHCP option 43 is not supported on the internal server. Therefore, the access point must use an alternative method to locate the management interface IP address of the switch, such as local subnet broadcast, Domain Name System (DNS), or priming.

An internal DHCP server pool only serves the wireless clients of that switch, not clients of other switches. Also, an internal DHCP server can serve only wireless clients, not wired clients.

When clients use the internal DHCP server of the switch, IP addresses are not preserved across reboots. As a result, multiple clients can be assigned with the same IP address. To resolve any IP address conflicts, clients must release their existing IP address and request a new one. Wired guest clients are always on a Layer 2 network connected to a local or foreign controller.

Note DHCPv6 is not supported in the internal DHCP servers.

Related Topics

Configuring DHCP for WLANs (CLI), on page 52
Configuring Advanced WLAN Properties (GUI), on page 39
Prerequisites for Configuring DHCP for WLANs, on page 47
Restrictions for Configuring DHCP for WLANs, on page 48

External DHCP Servers

The operating system is designed to appear as a DHCP Relay to the network and as a DHCP server to clients with industry-standard external DHCP servers that support DHCP Relay, which means that each controller appears as a DHCP Relay agent to the DHCP server and as a DHCP server at the virtual IP address to wireless clients.

Because the controller captures the client IP address that is obtained from a DHCP server, it maintains the same IP address for that client during intra switch, inter switch, and inter-subnet client roaming.

Note External DHCP servers can support DHCPv6.

Related Topics

Configuring DHCP for WLANs (CLI), on page 52
Configuring Advanced WLAN Properties (GUI), on page 39

Prerequisites for Configuring DHCP for WLANs, on page 47
Restrictions for Configuring DHCP for WLANs, on page 48

DHCP Assignments

You can configure DHCP on a per-interface or per-WLAN basis. We recommend that you use the primary DHCP server address that is assigned to a particular interface.

You can assign DHCP servers for individual interfaces. You can configure the management interface, AP-manager interface, and dynamic interface for a primary and secondary DHCP server, and you can configure the service-port interface to enable or disable DHCP servers. You can also define a DHCP server on a WLAN. In this case, the server overrides the DHCP server address on the interface assigned to the WLAN.

Security Considerations

For enhanced security, we recommend that you require all clients to obtain their IP addresses from a DHCP server. To enforce this requirement, you can configure all WLANs with a DHCP Addr. Assignment Required setting, which disallows client static IP addresses. If DHCP Addr. Assignment Required is selected, clients must obtain an IP address via DHCP. Any client with a static IP address is not allowed on the network. The switch monitors DHCP traffic because it acts as a DHCP proxy for the clients.

Note WLANs that support management over wireless must allow management (device-servicing) clients to obtain an IP address from a DHCP server.

If slightly less security is tolerable, you can create WLANs with DHCP Addr. Assignment Required disabled. Clients then have the option of using a static IP address or obtaining an IP address from a designated DHCP server.

Note DHCP Addr. Assignment Required is not supported for wired guest LANs.

You can create separate WLANs with DHCP Addr. Assignment Required configured as disabled. This is applicable only if DHCP proxy is enabled for the switch. You must not define the primary/secondary configuration DHCP server you should disable the DHCP proxy. These WLANs drop all DHCP requests and force clients to use a static IP address. These WLANs do not support management over wireless connections.

Related Topics

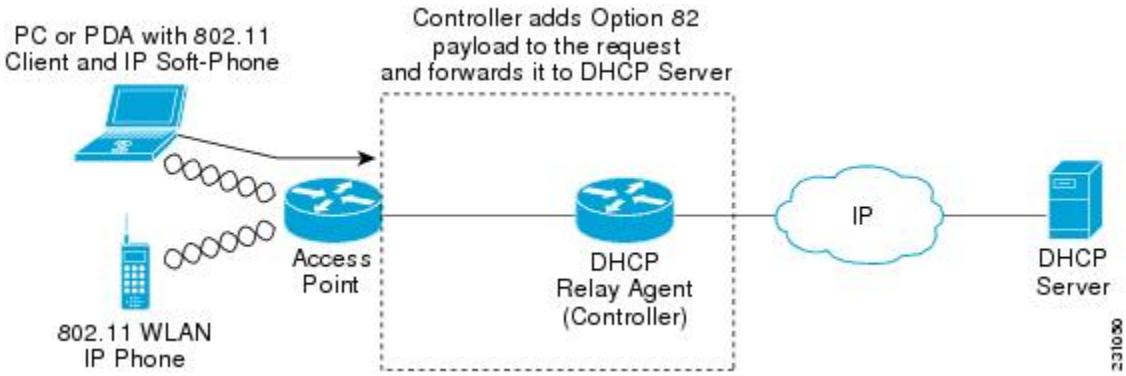
Configuring DHCP for WLANs (CLI), on page 52
Configuring Advanced WLAN Properties (GUI), on page 39
Prerequisites for Configuring DHCP for WLANs, on page 47
Restrictions for Configuring DHCP for WLANs, on page 48

Information About DHCP Option 82

DHCP option 82 provides additional security when DHCP is used to allocate network addresses. It enables the switch to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources. You can

configure the switch to add option 82 information to DHCP requests from clients before forwarding the requests to the DHCP server.

Figure 1: DHCP Option 82



The access point forwards all DHCP requests from a client to the switch. The switch adds the DHCP option 82 payload and forwards the request to the DHCP server. The payload can contain the MAC address or the MAC address and SSID of the access point, depending on how you configure this option.

Note Any DHCP packets that already include a relay agent option are dropped at the switch.

For DHCP option 82 to operate correctly, DHCP proxy must be enabled.

Related Topics

Configuring DHCP for WLANs (CLI), on page 52
Configuring Advanced WLAN Properties (GUI), on page 39
Prerequisites for Configuring DHCP for WLANs, on page 47
Restrictions for Configuring DHCP for WLANs, on page 48

Configuring DHCP Scopes

Related Topics

Configuring DHCP for WLANs (CLI), on page 52
Configuring Advanced WLAN Properties (GUI), on page 39
Prerequisites for Configuring DHCP for WLANs, on page 47
Restrictions for Configuring DHCP for WLANs, on page 48

Information About DHCP Scopes

Controllers have built-in DHCP relay agents. However, when you desire network segments that do not have a separate DHCP server, the controllers can have built-in DHCP scopes that assign IP addresses and subnet

masks to wireless clients. Typically, one controller can have one or more DHCP scopes that each provide a range of IP addresses.

DHCP scopes are needed for internal DHCP to work. Once DHCP is defined on the controller, you can then point the primary DHCP server IP address on the management, AP-manager, and dynamic interfaces to the controller's management interface.

Related Topics

Configuring DHCP for WLANs (CLI), on page 52
Configuring Advanced WLAN Properties (GUI), on page 39
Prerequisites for Configuring DHCP for WLANs, on page 47
Restrictions for Configuring DHCP for WLANs, on page 48
Configuring DHCP Scopes (CLI), on page 54

How to Configure DHCP for WLANs

Configuring DHCP for WLANs (CLI)

Use this procedure to configure the following DHCP parameters on a WLAN:

- DHCP Option 82 Payload
- DHCP Required
- DHCP Override

Before You Begin

- You must have admin privileges for configuring the WLAN.
- To configure the DHCP override, you must have the IP address of the DHCP server.

SUMMARY STEPS

1. **configure terminal**
2. **shutdown**
3. **wlan** *profile-name*
4. **ip dhcp opt82** {**ascii** | **format** {*add-ssid* | *ap-ethmac*} | **rid**}
5. **ip dhcp required**
6. **ip dhcp server** *ip-address*
7. **no shutdown**
8. **end**
9. **show wlan** *wlan-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**shutdown** **Example:** `Switch(config)# shutdown`	Shut down the WLAN.
Step 3	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.

Step 4	**ip dhcp opt82** {**ascii** | **format** {*add-ssid* | *ap-ethmac*} | **rid**}
	
	Example:
	`Switch(config)# ip dhcp opt82 format add-ssid`
		Specifies the DHCP82 payload on the WLAN. The keyword and arguments are as follows:
		• **ascii—**Configures ASCII for DHCP Option 82. If this is not configured, the option 82 format is set to ASCII format.
		• **format—**Specifies the DHCP option 82 format. The following options are available:
		  • *add-ssid***—**Set RemoteID format that is the AP radio MAC address and SSID.
		  • *ap-ethmac***—**Set RemoteID format that is the AP Ethernet MAC address.
		Note If the format option is not configured, only the AP radio MAC address is used.
		• **rid—**Adds the Cisco 2 byte RID for DHCP option 82.

Step 5	**ip dhcp required** **Example:** `Switch(config-wlan)# ip dhcp required`	Makes it mandatory for clients to get their IP address from the DHCP server. Static clients are not allowed.
Step 6	**ip dhcp server** *ip-address* **Example:** `Switch(config-wlan)# ip dhcp server 200.1.1.2`	Defines a DHCP server on the WLAN that overrides the DHCP server address on the interface assigned to the WLAN.
Step 7	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Restarts the WLAN.

	Command or Action	Purpose
Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 9	**show wlan** *wlan-name* **Example:** `Switch(config-wlan)# show wlan test-wlan`	Verifies the DHCP configuration.

Related Topics

Information About the Dynamic Host Configuration Protocol, on page 48
Internal DHCP Servers, on page 49
External DHCP Servers, on page 49
DHCP Assignments, on page 50
Information About DHCP Option 82, on page 50
Configuring DHCP Scopes, on page 51
Information About DHCP Scopes, on page 51
Prerequisites for Configuring DHCP for WLANs, on page 47
Restrictions for Configuring DHCP for WLANs, on page 48

Configuring DHCP Scopes (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ip dhcp pool** *pool-name*
3. **network** *network-name mask-address*
4. **dns-server** *hostname*
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**ip dhcp pool** *pool-name* **Example:** `Switch(config)#ip dhcp pool test-pool`	Configures the DHCP pool address.
Step 3	**network** *network-name mask-address* **Example:** `Switch(dhcp-config)#network 209.165.200.224 255.255.255.0`	Specifies the network number in dotted-decimal notation and the mask address.
Step 4	**dns-server** *hostname* **Example:** `Switch(dhcp-config)#dns-server example.com`	Specifies the DNS name server. You can specify an IP address or a hostname.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Information About DHCP Scopes, on page 51

Additional References

Related Documents

Related Topic	Document Title
System Management	*System Management Configuration Guide (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

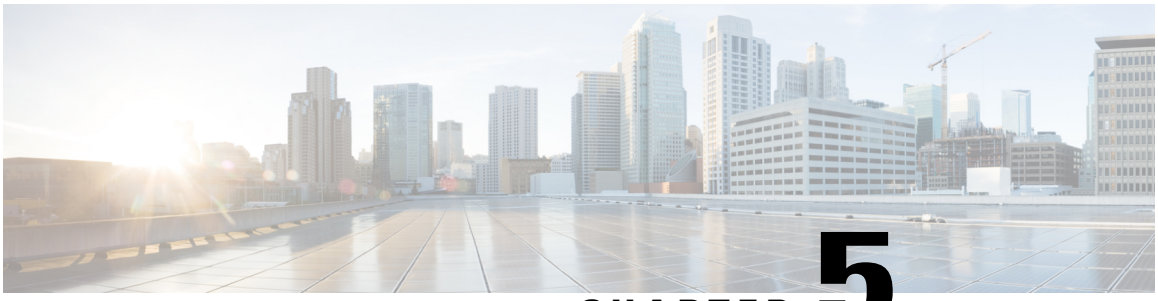
MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for DHCP for WLANs

Feature Name	Release	Feature Information
DHCP functionality for WLAN	Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 5

Configuring WLAN Security

- Finding Feature Information, page 57
- Prerequisites for Layer 2 Security, page 57
- Information About AAA Override, page 58
- How to Configure WLAN Security, page 59
- Additional References, page 68
- Feature Information about WLAN Layer 2 Security, page 69

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. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Prerequisites for Layer 2 Security

WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on information advertised in beacon and probe responses. The available Layer 2 security policies are as follows:

- None (open WLAN)
- Static WEP or 802.1X

Note Because static WEP and 802.1X are both advertised by the same bit in beacon and probe responses, they cannot be differentiated by clients. Therefore, they cannot both be used by multiple WLANs with the same SSID.

- WPA/WPA2

Note Although WPA and WPA2 cannot be used by multiple WLANs with the same SSID, you can configure two WLANs with the same SSID with WPA/TKIP with PSK and Wi-Fi Protected Access (WPA)/Temporal Key Integrity Protocol (TKIP) with 802.1X, or with WPA/TKIP with 802.1X or WPA/AES with 802.1X.

Related Topics

Configuring Static WEP + 802.1X Layer 2 Security Parameters (CLI), on page 59
Configuring Layer 2 Parameters (GUI), on page 64
Configuring Static WEP Layer 2 Security Parameters (CLI), on page 60
Configuring Layer 2 Parameters (GUI), on page 64
Configuring WPA + WPA2 Layer 2 Security Parameters (CLI), on page 61
Configuring Layer 2 Parameters (GUI), on page 64
Configuring 802.1X Layer 2 Security Parameters (CLI), on page 62
Configuring Layer 2 Parameters (GUI), on page 64
Configuring Advanced WLAN Properties (CLI), on page 36
Information About AAA Override, on page 58

Information About AAA Override

The AAA Override option of a WLAN enables you to configure the WLAN for identity networking. It enables you to apply VLAN tagging, Quality of Service (QoS), and Access Control Lists (ACLs) to individual clients based on the returned RADIUS attributes from the AAA server.

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 36
Prerequisites for Layer 2 Security, on page 57

How to Configure WLAN Security

Configuring Static WEP + 802.1X Layer 2 Security Parameters (CLI)

Before You Begin

You must have administrator privileges.

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **security static-wep-key** {**authentication** {**open** | **sharedkey**} | **encryption** {**104** | **40**} [**ascii** | **hex**] {**0**|**8**}} *wep-key wep-key-index1-4*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**security static-wep-key** {**authentication** {**open**	**sharedkey**}	**encryption** {**104**	**40**} [**ascii**	**hex**] {**0**|**8**}} *wep-key wep-key-index1-4* **Example:** `Switch(config-wlan)# security static-wep-key encryption 40 hex 0 test 2`	Configures static WEP security on a WLAN. The keywords and arguments are as follows: • **authentication—**Configures 802.11 authentication. • **encryption—**Sets the static WEP keys and indices. • **open—**Configures open system authentication. • **sharedkey—**Configures shared key authentication. • **104, 40—**Specifies the WEP key size. • **hex, ascii—**Specifies the input format of the key. • *wep-key-index* , *wep-key-index1-4***—**Type of password that follows. A value of 0 indicates that an unencrypted password follows. A value of 8 indicates that an AES encrypted follows.

	Command or Action	Purpose
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for Layer 2 Security, on page 57

Configuring Static WEP Layer 2 Security Parameters (CLI)

Before You Begin

You must have administrator privileges.

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **security static-wep-key** [**authentication** {**open** | **shared**} | **encryption** {**104** | **40**} {**ascii** | **hex**} [**0** | **8**]]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**security static-wep-key** [**authentication** {**open**	**shared**}	**encryption** {**104**	**40**} {**ascii**	**hex**} [**0**	**8**]] **Example:** `Switch(config-wlan)# security static-wep-key authentication open`	The keywords are as follows: • **static-wep-key—**Configures Static WEP Key authentication. • **authentication—**Specifies the authentication type you can set. The values are open and shared. • **encryption—**Specifies the encryption type that you can set. The valid values are 104 and 40. 40-bit keys must contain 5 ASCII text characters or 10 hexadecimal characters. 104-bit keys must contain 13 ASCII text characters or 26 hexadecimal characters

	Command or Action	Purpose
		• **ascii**—Specifies the key format as ASCII. • **hex**—Specifies the key format as HEX.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for Layer 2 Security, on page 57

Configuring WPA + WPA2 Layer 2 Security Parameters (CLI)

Note The default security policy is WPA2.

Before You Begin

You must have administrator privileges.

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **security wpa**
4. **security wpa wpa1**
5. **security wpa wpa1 ciphers** [**aes** | **tkip**]
6. **security wpa wpa2**
7. **security wpa wpa2 ciphers** [**aes** | **tkip**]
8. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**security wpa** **Example:** `Switch(config-wlan)# security wpa`	Enables WPA.
Step 4	**security wpa wpa1** **Example:** `Switch(config-wlan)# security wpa wpa1`	Enables WPA1.
Step 5	**security wpa wpa1 ciphers** [**aes** | **tkip**] **Example:** `Switch(config-wlan)# security wpa wpa1 ciphers aes`	Specifies the WPA1 cipher. Choose one of the following encryption types: • **aes—**Specifies WPA/AES support. • **tkip—**Specifies WPA/TKIP support.
Step 6	**security wpa wpa2** **Example:** `Switch(config-wlan)# security wpa`	Enables WPA 2.
Step 7	**security wpa wpa2 ciphers** [**aes** | **tkip**] **Example:** `Switch(config-wlan)# security wpa wpa2 ciphers tkip`	Configure WPA2 cipher. Choose one of the following encryption types: • **aes—**Specifies WPA/AES support. • **tkip—**Specifies WPA/TKIP support.
Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for Layer 2 Security, on page 57

Configuring 802.1X Layer 2 Security Parameters (CLI)

Before You Begin

You must have administrator privileges.

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **security dot1x**
4. **security** [**authentication-list** *auth-list-name* | **encryption** {**0** | **104** | **40**}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**security dot1x** **Example:** `Switch(config-wlan)# security dot1x`	Specifies 802.1X security.
Step 4	**security** [**authentication-list** *auth-list-name*	**encryption** {**0**	**104**	**40**} **Example:** `Switch(config-wlan)# security encryption 104`	The keywords and arguments are as follows: • **authentication-list—**Specifies the authentication list for IEEE 802.1X. • **encryption—**Specifies the length of the CKIP encryption key. The valid values are 0, 40, and 104. Zero (0) signifies no encryption. This is the default. **Note** All keys within a WLAN must be of the same size.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for Layer 2 Security, on page 57

Configuring Layer 2 Parameters (GUI)

Before You Begin

- You must have administrator privileges.

Step 1 Click **Configuration** > **WLAN** > .
The **WLANs** page appears.

Step 2 Click the WLANs profile of the WLAN you want to configure.
The **WLANs** > **Edit** > page appears.

Step 3 Click the **Security** > **Layer 2** > tab.

Parameter	Description
Layer2 Security	Layer2 security for the selected WLAN. Values are the following: • None—No Layer 2 security selected. • WPA+WPA2—Wi-Fi Protected Access. • 802.1X—WEP 802.1X data encryption type. For information on these settings, see the Layer 2 802.1X Parameters topic. • Static WEP—Static WEP encryption parameters. • Static WEP + 802.1x—Both Static WEP and 802.1X parameters.
MAC Filtering	MAC address filtering. You can locally configure clients by their MAC addresses in the **MAC Filters** > **New page** . Otherwise, configure the clients on a RADIUS server. **Note** MAC Filtering is also known as MAC Authentication By Pass (MAB).
Fast Transition	Check box to enable or disable a fast transition between access points.
Over the DS	Check box to enable or disable a fast transition over a distributed system.
Reassociation Timeout	Time in seconds after which a fast transition reassociation times out.

To configure the **WPA + WPA2** parameters, provide the following details:

Parameter	Description
WPA Policy	Check box to enable or disable WPA policy.
WPA Encryption	WPA2 encryption type: TKIP or AES. Available only if the WPA policy is enabled.
WPA2 Policy.	Check box to enable or disable WPA2 policy.
WPA2 Encryption	WPA2 encryption type: TKIP or AES. Available only if the WPA2 policy is enabled.

Parameter	Description
Authentication Key Management	The rekeying mechanism parameter.. Values are the following: • 802.1X • CCKM • PSK • 802.1x + CCKM
PSK Format	Enabled when you select the PSK value for Authentication Key Management. Choose ASCII or the HEX format and enter the preshared key.

To configure **802.1x** parameters, provide the following details:

Parameter	Description
802.11 data encryption	WEP 802.11 data encryption type.
Type	Security type.
Key size	Key size. Values are the following: • None • 40 bits • 104 bits The third-party AP WLAN (17) can only be configured with 802.1X encryption. Drop-down configurable 802.1X parameters are not available for this WLAN.

To specify **Static WEP**, configure the following parameters:

Parameter	Description
802.11 Data Encryption	Static WEP encryption type.
Current Key	Displays the current selected key details.
Type	Security type.
Key size	Key size. Values are the following: • Not set • 40 bits • 104 bits

Parameter	Description
Key Index	Key index from 1 to 4. One unique WEP key index can be applied to each WLAN. Because there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer 2 encryption. Because there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer 2 encryption.
Encryption Key	Encryption key.
Key Format	Encryption key format in ASCII or HEX.
Allow Shared Key Authentication	Key authentication that you can enable or disable.

To configure Static WEP + 802.1X Parameters

Parameter	Description
Static WEP Parameters	
802.11 Data Encryption	Static WEP encryption type.
Current Key	Displays the current selected key details.
Type	Security type.
Key size	Key size. Values are the following: • Not set • 40 bits • 104 bits
Key Index	Key index from 1 to 4. One unique WEP key index can be applied to each WLAN. Because there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer 2 encryption. Because there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer 2 encryption.
Encryption Key	Encryption key.
Key Format	Encryption key format in ASCII or HEX.
Allow Shared Key Authentication	Key authentication that you can enable or disable.
802.1x Parameters	

Parameter	Description
802.11 Data Encryption	Static WEP encryption type.
Current Key	Display Only. The current selected key details.
Type	Security type.
Key size	Key size. Values are the following: • Not set • 40 bits • 104 bits
Key Index	Key index from 1 to 4. Note One unique WEP key index can be applied to each WLAN. Because there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer 2 encryption.
Encryption Key	Encryption key.
Key Format	Encryption key format in ASCII or HEX.
Allow Shared Key Authentication	Key authentication that you can enable or disable.

Step 4 Click **Apply**.

Related Topics

Prerequisites for Layer 2 Security, on page 57
Prerequisites for Layer 2 Security, on page 57
Prerequisites for Layer 2 Security, on page 57
Prerequisites for Layer 2 Security, on page 57

Additional References

Related Documents

Related Topic	Document Title
WLAN command reference	*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
Security configuration guide	*Security Configuration Guide (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

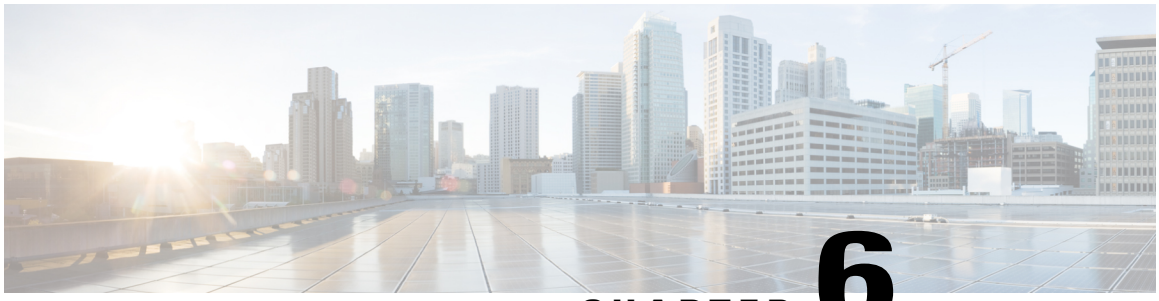
Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information about WLAN Layer 2 Security

This table lists the features in this module and provides links to specific configuration information.

Feature Name	Release	Feature Information
WLAN Security functionality	Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 6

Setting Client Count Per WLAN

- Finding Feature Information, page 71
- Restrictions for Setting Client Count for WLANs, page 71
- Information About Setting the Client Count per WLAN, page 72
- How to Configure Client Count Per WLAN, page 72
- Monitoring Client Connections (CLI), page 75
- Additional References for Client Connections, page 76
- Feature Information about Client Connections Per WLAN, page 77

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. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Restrictions for Setting Client Count for WLANs

- When a WLAN has reached the limit on the maximum number of clients connected to it or an AP radio and a new client tries to join the WLAN, the client cannot connect to the WLAN until an existing client gets disconnected.
- Roaming clients are considered as new clients. The new client can connect to a WLAN, which has reached the maximum limit on the number of connected clients, only when an existing client gets disconnected.

Note For more information about the number of clients that are supported, see the product data sheet of your switch.

Related Topics

Configuring Client Count per WLAN (CLI), on page 72
Configuring Client Count Per AP Per WLAN (CLI), on page 73
Configuring Client Count per AP Radio per WLAN (CLI), on page 74
Information About Setting the Client Count per WLAN, on page 72

Information About Setting the Client Count per WLAN

You can set a limit to the number of clients that can connect to a WLAN, which is useful in scenarios where you have a limited number of clients that can connect to a switch. For example, consider a scenario where the switch can serve up to 256 clients on a WLAN and these clients can be shared between enterprise users (employees) and guest users. You can set a limit on the number of guest clients that can access a given WLAN. The number of clients that you can configure for each WLAN depends on the platform that you are using.

Related Topics

Configuring Client Count per WLAN (CLI), on page 72
Configuring Client Count Per AP Per WLAN (CLI), on page 73
Configuring Client Count per AP Radio per WLAN (CLI), on page 74
Restrictions for Setting Client Count for WLANs, on page 71
Monitoring Client Connections (CLI), on page 75

How to Configure Client Count Per WLAN

Configuring Client Count per WLAN (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **client association limit** *limit*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**client association limit** *limit* **Example:** `Switch(config-wlan)# client association limit 2000`	Configures the maximum number of client associations per WLAN. The range is 0 to 2000. A default value is 0 (no limit).
Step 4	**end** **Example:** `Switch(wlan-config)# end`	Returns to priviled EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Related Topics

Information About Setting the Client Count per WLAN, on page 72
Restrictions for Setting Client Count for WLANs, on page 71
Monitoring Client Connections (CLI), on page 75

Configuring Client Count Per AP Per WLAN (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **client association limit ap** *ap-limit*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**client association limit ap** *ap-limit* **Example:** `Switch(config-wlan)# client association limit ap 250`	Configures the maximum number of clients per AP per WLAN. The range is 1 - 400.
Step 4	**end** **Example:** `Switch(wlan-config)# end`	Returns to privileded EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Related Topics

Information About Setting the Client Count per WLAN, on page 72
Restrictions for Setting Client Count for WLANs, on page 71
Monitoring Client Connections (CLI), on page 75

Configuring Client Count per AP Radio per WLAN (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **client association limit radio** *max-client-connections*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**client association limit radio** *max-client-connections* **Example:** `Switch(config-wlan)# client association limit radio 180`	Configures the maximum number of client connections per AP radio per WLAN. The range is 0 - 200 for the a, b, and g radios.
Step 4	**end** **Example:** `Switch(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Related Topics

Information About Setting the Client Count per WLAN, on page 72
Restrictions for Setting Client Count for WLANs, on page 71
Monitoring Client Connections (CLI), on page 75

Monitoring Client Connections (CLI)

The following commands can be used to monitor client connections on the switch:

Command	Description

show wlan name *wlan-name*	Displays the WLAN properties. Here is an example:
	
	`. . . .`
	`Max Associated Clients per WLAN :0`
	`Max Associated Clients per AP per WLAN :0`
	`Max Associated Clients per AP Radio per WLAN :0`
	`. . .`
	`. . .`

Command	Description
show wlan id *wlan-id*	Displays the WLAN properties. here is an example: . . . . Max Associated Clients per WLAN :0 Max Associated Clients per AP per WLAN :0 Max Associated Clients per AP Radio per WLAN :0 . . . . . .

Related Topics

Configuring Client Count per WLAN (CLI), on page 72
Configuring Client Count Per AP Per WLAN (CLI), on page 73
Configuring Client Count per AP Radio per WLAN (CLI), on page 74
Information About Setting the Client Count per WLAN, on page 72

Additional References for Client Connections

Related Documents

Related Topic	Document Title
WLAN Command References	*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

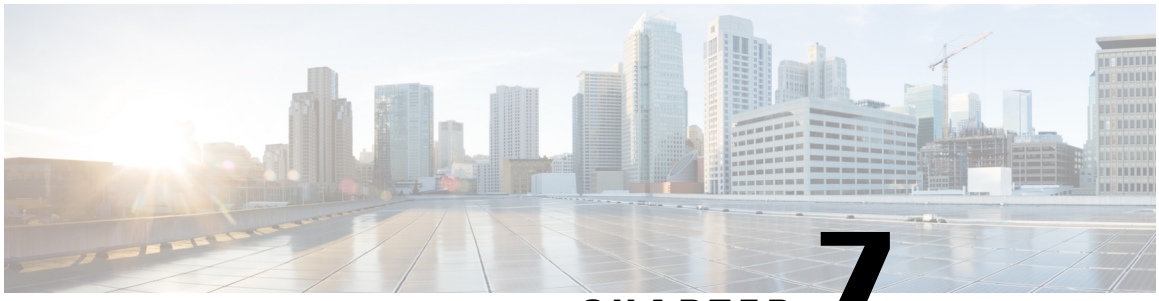
Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information about Client Connections Per WLAN

This table lists the features in this module and provides links to specific configuration information:

Feature Name	Release	Feature Information
Client Connections Per WLAN, Per AP, and per AP Radio	Cisco IOS XE 3.3SE	This feature was introduced.



CHAPTER 7

Configuring 802.11w

- Finding Feature Information, page 79
- Prerequisites for 802.11w, page 79
- Restrictions for 802.11w, page 80
- Information About 802.11w, page 80
- How to Configure 802.11w, page 81
- Disabling 802.11w (CLI), page 83
- Monitoring 802.11w (CLI), page 84
- Additional References for 802.11w, page 85
- Feature Information for 802.11w, page 86

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. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Prerequisites for 802.11w

- To configure 802.11w feature for optional and mandatory, you must have WPA and AKM configured.

Note The RNS (Robust Secure Network) IE must be enabled with an AES Cipher.

- To configure 802.11w as mandatory, you must enable PMF AKM in addition to WPA AKM.

Related Topics

Configuring 802.11w (CLI), on page 81
Disabling 802.11w (CLI), on page 83
Information About 802.11w, on page 80

Restrictions for 802.11w

- 802.11w cannot be applied on an open WLAN, WEP-encrypted WLAN, or a TKIP-encrypted WLAN.
- The WLAN on which 802.11w is configured must have either WPA2-PSK or WPA2-802.1x security configured.

Related Topics

Configuring 802.11w (CLI), on page 81
Disabling 802.11w (CLI), on page 83
Information About 802.11w, on page 80

Information About 802.11w

Wi-Fi is a broadcast medium that enables any device to eavesdrop and participate either as a legitimate or rogue device. Control and management frames such as authentication/deauthentication, association/disassociation, beacons, and probes are used by wireless clients to select an AP and to initiate a session for network services.

Unlike data traffic which can be encrypted to provide a level of confidentiality, these frames must be heard and understood by all clients and therefore must be transmitted as open or unencrypted. While these frames cannot be encrypted, they must be protected from forgery to protect the wireless medium from attacks. For example, an attacker could spoof management frames from an AP to tear down a session between a client and AP.

The 802.11w protocol applies only to a set of robust management frames that are protected by the Management Frame Protection (PMF) service. These include Disassociation, Deauthentication, and Robust Action frames.

Management frames that are considered as robust action and therefore protected are the following:

- Spectrum Management
- QoS
- Block Ack
- SA Query
- Vendor-specific Protected

When 802.11w is implemented in the wireless medium, the following occur:

- Client protection is added by the AP adding cryptographic protection (by including the MIC information element) to deauthentication and disassociation frames preventing them from being spoofed in a DOS attack.

- Infrastructure protection is added by adding a Security Association (SA) teardown protection mechanism consisting of an Association Comeback Time and an SA-Query procedure preventing spoofed association request from disconnecting an already connected client.

Related Topics

Configuring 802.11w (CLI), on page 81
Disabling 802.11w (CLI), on page 83
Prerequisites for 802.11w, on page 79
Restrictions for 802.11w, on page 80
Monitoring 802.11w (CLI), on page 84

How to Configure 802.11w

Configuring 802.11w (CLI)

Before You Begin

WPA and AKM must be configured.

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **shutdown**
4. **security pmf** {**association-check** *association-comeback-time-in-seconds* | **mandatory** | **optional** | **saquery** *saquery-time-in-milliseconds*}
5. **no shutdown**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.

	Command or Action	Purpose
Step 3	**shutdown** **Example:** `Switch shutdown`	Shutdown the WLAN before configuring the PMF.
Step 4	**security pmf** {**association-check** *association-comeback-time-in-seconds* | **mandatory** | **optional** | **saquery** *saquery-time-in-milliseconds*} **Example:** `Switch(config-wlan)# security pmf saquery-retry-time 200`	Configures the PMF parameters with the following options: • **association-comeback—**Configures the 802.11w association comeback time. The range is from 1 to 20 seconds. • **mandatory—**Requires clients to negotiate 802.11w PMF protection on a WLAN. • **optional—**Enables 802.11w PMF protection on a WLAN. • **saquery—**Time interval identified in milliseconds before which the SA query response is expected. If the switch does not get a response, another SQ query is tried. The range is from 100 to 500 ms. The value must be specified in multiples of 100 milliseconds.
Step 5	**no shutdown** **Example:** `Switch no shutdown`	Restart the WLAN for the changes to take effect.
Step 6	**end** **Example:** `Switch(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Related Topics

Information About 802.11w, on page 80
Prerequisites for 802.11w, on page 79
Restrictions for 802.11w, on page 80
Monitoring 802.11w (CLI), on page 84

Disabling 802.11w (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **shutdown**
4. **no security pmf [association-comeback** *association-check-comback-interval-seconds* | **mandatory** | **optional** | **saquery** *saquery-time-interval-milliseconds*]
5. **no shutdown**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**shutdown** **Example:** `Switch shutdown`	Shutdown the WLAN before configuring the PMF.
Step 4	**no security pmf [association-comeback** *association-check-comback-interval-seconds*	**mandatory**	**optional**	**saquery** *saquery-time-interval-milliseconds*] **Example:** `Switch(config-wlan)# no security pmf`	Disables PMF on the WLAN. The following attributes are available: • **association-comeback—**Disables the 802.11w association comeback time. • **mandatory—**Disables clients to negotiate 802.11w PMF protection on a WLAN. • **optional—**Disables 802.11w PMF protection on a WLAN. • **saquery—**Time interval identified in the association response to an already associated client before the association can be tried again. This time interval checks if the client is a real client and not a rogue client during the association comeback time. If the client does not respond within this time, the client association is deleted from the switch The range is from 100 to 500 ms. The value must be specified in multiples of 100 milliseconds.

	Command or Action	Purpose
Step 5	**no shutdown** **Example:** `Switch no shutdown`	Restart the WLAN for the changes to take effect.
Step 6	**end** **Example:** `Switch(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Related Topics

Information About 802.11w, on page 80
Prerequisites for 802.11w, on page 79
Restrictions for 802.11w, on page 80
Monitoring 802.11w (CLI), on page 84

Monitoring 802.11w (CLI)

The following command can be used to monitor 802.11w:

Command	Description

show wlan name *wlan-profile-name*	Displays the WLAN parameters on the WLAN. The PMF parameters are displayed. Here is an example:
	
	`. . . .`
	`. . . .`
	`Auth Key Management`
	`  802.1x                                        :`
	` Disabled`
	`  PSK                                          :`
	` Enabled`
	`  CCKM                                         :`
	` Disabled`
	`  FT dot1x                                     :`
	` Disabled`
	`  FT PSK                                       :`
	` Disabled`
	`  PMF dot1x                                    :`
	` Disabled`
	`  PMF PSK                                      :`
	` Enabled`
	`    FT Support                                 :`
	` Disabled`
	`        FT Reassociation Timeout               :`
	` 20`
	`        FT Over-The-DS mode                    :`
	` Disabled`
	`    PMF Support                                :`
	` Required`
	`        PMF Association Comeback Timeout       :`
	` 9`
	`        PMF SA Query Time                      :`
	` 200`
	`. . . .`
	`. . . .`

Related Topics

Configuring 802.11w (CLI), on page 81

Disabling 802.11w (CLI), on page 83

Information About 802.11w, on page 80

Additional References for 802.11w

Related Documents

Related Topic	Document Title
WLAN Command Reference	*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
WLAN Security	*Configuring WLAN Security* chapter in this book.

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
802.11w	IEEE 802.11w Protected Management Frames

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

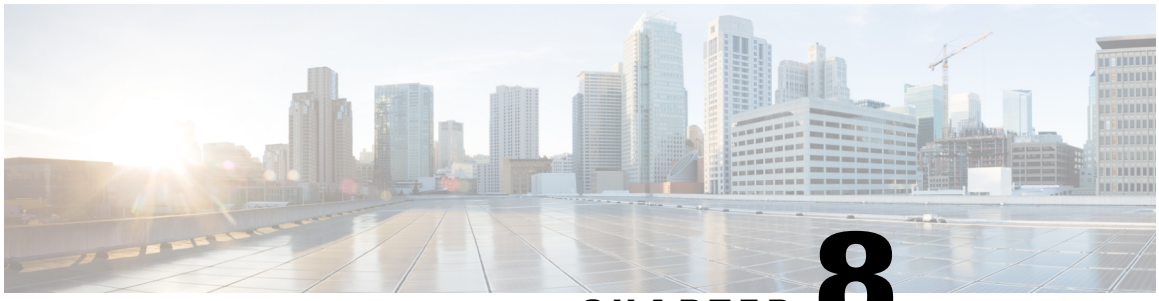
Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for 802.11w

This table lists the features in this module and provides links to specific configuration information:

Feature Name	Release	Feature Information
802.11w	Cisco IOS XE 3.3SE	This feature was introduced.



CHAPTER 8

Configuring Wi-Fi Direct Client Policy

- Finding Feature Information, page 89
- Restrictions for the Wi-Fi Direct Client Policy, page 89
- Information About the Wi-Fi Direct Client Policy, page 89
- How to Configure Wi-Fi Direct Client Policy, page 90
- Additional References for Wi-Fi Direct Client Policy, page 92
- Feature Information about Wi-Fi Direct Client Policy, page 93

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. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Restrictions for the Wi-Fi Direct Client Policy

Wi-Fi Direct Client Policy is applicable to WLANs that have APs in local mode only.

Information About the Wi-Fi Direct Client Policy

Devices that are Wi-Fi Direct capable can connect directly to each other quickly and conveniently to do tasks such as printing, synchronization, and sharing of data. Wi-Fi Direct devices may associate with multiple peer-to-peer (P2P) devices and with infrastructure wireless LANs (WLANs) concurrently. You can use the controller to configure the Wi-Fi Direct Client Policy, on a per WLAN basis, where you can allow or disallow association of Wi-Fi devices with infrastructure WLANs, or disable Wi-Fi Direct Client Policy altogether for WLANs.

Related Topics

Configuring the Wi-Fi Direct Client Policy (CLI), on page 90
Disabling Wi-Fi Direct Client Policy (CLI), on page 91
Monitoring Wi-Fi Direct Client Policy (CLI), on page 92

How to Configure Wi-Fi Direct Client Policy

Configuring the Wi-Fi Direct Client Policy (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **wifidirect policy** {**permit** | **deny** }
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.

Step 3	**wifidirect policy** {**permit**	**deny** }
		
		Example:
		`Switch(config-wlan)# wifidirect policy permit`
			Configures the Wi-Fi Direct client policy on the WLAN using one of the following:
			• **permit—**Enables Wi-Fi Direct clients to associate with the WLAN.
			• **deny—**When the Wi-Fi Direct policy is configured as "deny," the switch permits or denies Wi-Fi Direct devices based on the device capabilities. A Wi-Fi Direct device reports these capabilities in its association request to the switch and these are based on the Wi-Fi capabilities of the device. These include:
			  • Concurrent operation
			  • Cross connection
			
			Note The command **no wifidirect policy** ignores the client's Wi-Fi direct status. Additionally, the access point also does not advertise any beacons and probes. Effectively, the **no** form of the command disables the Wi-Fi direct feature on the WLAN.

	Command or Action	Purpose
		If the Wi-Fi device supports either concurrent operations or cross connections or both, the client association is denied. The client can associate if the device does not support concurrent operations and cross connections.
Step 4	**end** **Example:** `Switch(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Related Topics

Information About the Wi-Fi Direct Client Policy, on page 89
Monitoring Wi-Fi Direct Client Policy (CLI), on page 92

Disabling Wi-Fi Direct Client Policy (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **no wifidirect policy**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**no wifidirect policy** **Example:** `Switch(config)# no wifidirect policy`	Ignores the Wi-Fi Direct status of clients thereby allowing Wi-Fi Direct clients to associate.

	Command or Action	Purpose
Step 4	**end** **Example:** `Switch(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Related Topics

Information About the Wi-Fi Direct Client Policy, on page 89
Monitoring Wi-Fi Direct Client Policy (CLI), on page 92

Monitoring Wi-Fi Direct Client Policy (CLI)

The following commands can be used to monitor Wi-Fi Direct Client Policy:

Command	Description
show wireless client wifidirect stats	Displays the total number of clients associated and the number of association requests rejected if the Wi-Fi Direct Client Policy is enabled.
show wlan summary	Displays status of the Wi-Fi Direct on the WLAN.
show wireless cli mac-address *mac-address*	Displays the detail information of a client.

Related Topics

Configuring the Wi-Fi Direct Client Policy (CLI), on page 90
Disabling Wi-Fi Direct Client Policy (CLI), on page 91
Information About the Wi-Fi Direct Client Policy, on page 89

Additional References for Wi-Fi Direct Client Policy

Related Documents

Related Topic	Document Title
WLAN Command reference	*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

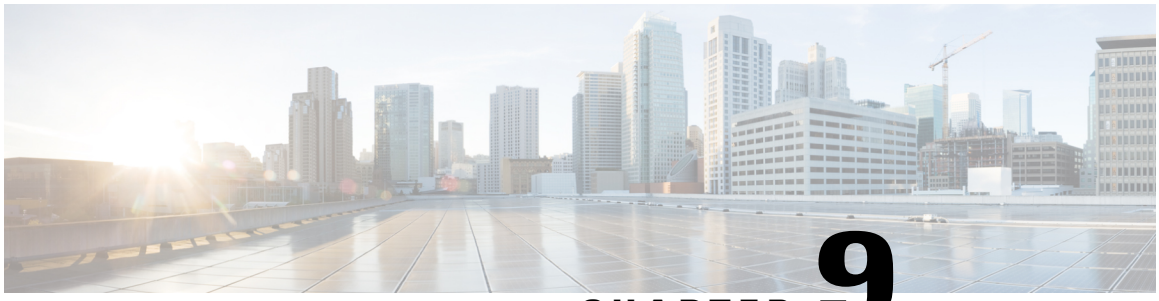
MIB	MIBs Link
All Supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information about Wi-Fi Direct Client Policy

Feature Name	Release	Feature Information
Wi-Fi Direct Feature	Cisco IOS XE 3.3SE	This feature was introduced.



CHAPTER 9

Configuring 802.11r BSS Fast Transition

- Finding Feature Information, page 95
- Restrictions for 802.11r Fast Transition, page 95
- Information About 802.11r Fast Transition, page 96
- How to Configure 802.11r Fast Transition, page 99
- Additional References for 802.11r Fast Transition, page 106
- Feature Information for 802.11r Fast Transition, page 107

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. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Restrictions for 802.11r Fast Transition

- 802.11r client association is not supported on access points in standalone mode.
- 802.11r fast roaming is not supported on access points in standalone mode.
- 802.11r fast roaming between local authentication and central authentication WLAN is not supported.
- EAP LEAP method is not supported.
- TSpec is not supported for 802.11r fast roaming. Therefore, RIC IE handling is not supported.
- If WAN link latency exists, fast roaming is also delayed. Voice or data maximum latency should be verified. The controller handles 802.11r Fast Transition authentication request during roaming for both Over-the-Air and Over-the-DS methods.

- This feature is supported only on open and WPA2 configured WLANs.
- Legacy clients cannot associate with a WLAN that has 802.11r enabled if the driver of the supplicant that is responsible for parsing the Robust Security Network Information Exchange (RSN IE) is old and not aware of the additional AKM suites in the IE. Due to this limitation, clients cannot send association requests to WLANs. These clients, however, can still associate with non-802.11r WLANs. Clients that are 802.11r capable can associate as 802.11i clients on WLANs that have both 802.11i and 802.11r Authentication Key Management Suites enabled.

  The workaround is to enable or upgrade the driver of the legacy clients to work with the new 802.11r AKMs, after which the legacy clients can successfully associate with 802.11r enabled WLANs.

  Another workaround is to have two SSIDs with the same name but with different security settings (FT and non-FT).
- Fast Transition resource request protocol is not supported because clients do not support this protocol. Also, the resource request protocol is an optional protocol.
- To avoid any Denial of Service (DoS) attack, each controller allows a maximum of three Fast Transition handshakes with different APs.

Related Topics

Configuring 802.11r Fast Transition in an Open WLAN (CLI), on page 99
Disabling 802.11r Fast Transition (CLI), on page 104
Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI), on page 101
Configuring 802.11r Fast Transition on a PSK Security Enabled WLAN (CLI), on page 102
Configuring 802.11 Fast Transition (GUI), on page 104
Information About 802.11r Fast Transition, on page 96

Information About 802.11r Fast Transition

802.11r, which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP, which is called Fast Transition (FT). The initial handshake allows the client and APs to do the Pairwise Transient Key (PTK) calculation in advance. These PTK keys are applied to the client and AP after the client does the reassociation request or response exchange with new target AP.

802.11r provides two methods of roaming:

- Over-the-Air
- Over-the-DS (Distribution System)

The FT key hierarchy is designed to allow clients to make fast BSS transitions between APs without requiring reauthentication at every AP. WLAN configuration contains a new Authenticated Key Management (AKM) type called FT (Fast Transition).

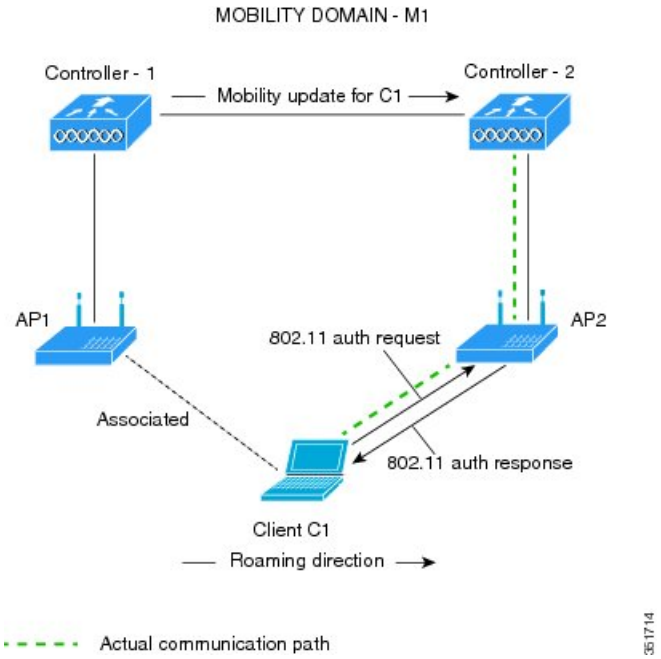
How a Client Roams

For a client to move from its current AP to a target AP using the FT protocols, the message exchanges are performed using one of the following two methods:

- Over-the-Air—The client communicates directly with the target AP using IEEE 802.11 authentication with the FT authentication algorithm.
- Over-the-DS—The client communicates with the target AP through the current AP. The communication between the client and the target AP is carried in FT action frames between the client and the current AP and is then sent through the controller.

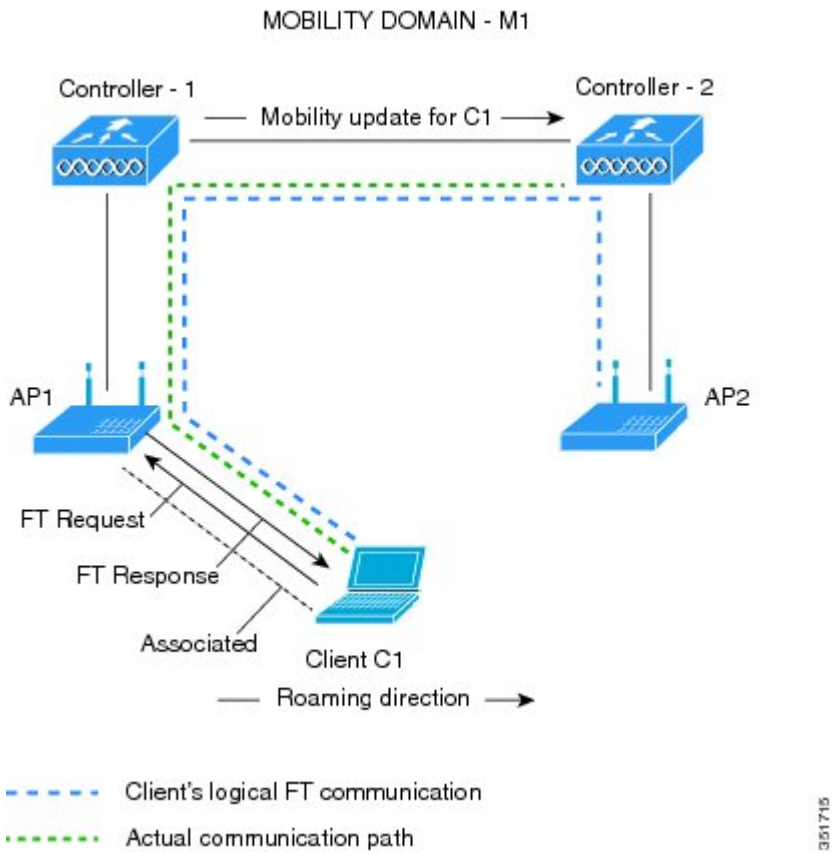
This figure shows the sequence of message exchanges that occur when Over the Air client roaming is configured.

Figure 2: Message Exchanges when Over the Air client roaming is configured



This figure shows the sequence of message exchanges that occur when Over the DS client roaming is configured.

Figure 3: Message Exchanges when Over the DS client roaming is configured



Related Topics

Configuring 802.11r Fast Transition in an Open WLAN (CLI), on page 99
Disabling 802.11r Fast Transition (CLI), on page 104
Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI), on page 101
Configuring 802.11r Fast Transition on a PSK Security Enabled WLAN (CLI), on page 102
Configuring 802.11 Fast Transition (GUI), on page 104
Monitoring 802.11r Fast Transition (CLI), on page 105
Restrictions for 802.11r Fast Transition, on page 95

How to Configure 802.11r Fast Transition

Configuring 802.11r Fast Transition in an Open WLAN (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **client vlan** *vlan-id*
4. **no security wpa**
5. **no security wpa akm dot1x**
6. **no security wpa wpa2**
7. **no wpa wpa2 ciphers aes**
8. **security ft**
9. **no shutdown**
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**client vlan** *vlan-id* **Example:** `Switch(config-wlan)# client vlan 0120`	Associate the client VLAN to the WLAN.
Step 4	**no security wpa** **Example:** `Switch(config-wlan)# no security wpa`	Disable WPA secuirty.
Step 5	**no security wpa akm dot1x** **Example:** `Switch(config-wlan)# no security wpa akm dot1x`	Disable security AKM for dot1x.

	Command or Action	Purpose
Step 6	**no security wpa wpa2** **Example:** `Switch(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 7	**no wpa wpa2 ciphers aes** **Example:** `Switch(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.
Step 8	**security ft** **Example:** `Switch(config-wlan)# security ft`	Specifies the 802.11r fast transition parameters.
Step 9	**no shutdown** **Example:** `Switch(config-wlan)# shutdown`	Shutdown the WLAN.
Step 10	**end** **Example:** `Switch(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode

Related Topics

Information About 802.11r Fast Transition, on page 96
Monitoring 802.11r Fast Transition (CLI), on page 105
Restrictions for 802.11r Fast Transition, on page 95

Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **client vlan** *vlan-name*
4. **local-auth** *local-auth-profile-eap*
5. **security dot1x authentication-list default**
6. **security ft**
7. **security wpa akm ft dot1x**
8. **no shutdown**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**client vlan** *vlan-name* **Example:** `Switch(config-wlan)# client vlan 0120`	Associate the client VLAN to this WLAN.
Step 4	**local-auth** *local-auth-profile-eap* **Example:** `Switch(config-wlan)# local-auth`	Enable the local auth EAP profile.
Step 5	**security dot1x authentication-list default** **Example:** `Switch(config-wlan)# security dot1x authentication-list default`	Enable security authentication list for dot1x security. The configuration is similar for any dot1x security WLAN.
Step 6	**security ft** **Example:** `Switch(config-wlan)# security ft`	Enables 802.11r Fast Transition on this WLAN.

	Command or Action	Purpose
Step 7	**security wpa akm ft dot1x** **Example:** `Switch(config-wlan)# security wpa akm ft dot1x`	Enables 802.1x security on the WLAN.
Step 8	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Enable the WLAN.
Step 9	**end** **Example:** `Switch(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode

Related Topics

Information About 802.11r Fast Transition, on page 96
Monitoring 802.11r Fast Transition (CLI), on page 105
Restrictions for 802.11r Fast Transition, on page 95

Configuring 802.11r Fast Transition on a PSK Security Enabled WLAN (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **client vlan** *vlan-name*
4. **no security wpa akm dot1x**
5. **security wpa akm ft psk**
6. **security wpa akm psk set-key {ascii {0 | 8} | hex {0 | 8}}**
7. **security ft**
8. **no shutdown**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**client vlan** *vlan-name* **Example:** `Switch(config-wlan)# client vlan 0120`	Associates the client VLAN to this WLAN.
Step 4	**no security wpa akm dot1x** **Example:** `Switch(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**security wpa akm ft psk** **Example:** `Switch(config-wlan)# security wpa akm ft psk`	Configures FT PSK support.
Step 6	**security wpa akm psk set-key** {**ascii** {**0** | **8**} | **hex** {**0** | **8**}} **Example:** `Switch(config-wlan)# security wpa akm psk set-key ascii 0 test`	Configures PSK AKM shared key.
Step 7	**security ft** **Example:** `Switch(config-wlan)# security ft`	Configures 802.11r Fast Transition.
Step 8	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Enables the WLAN.
Step 9	**end** **Example:** `Switch(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode

Related Topics

Information About 802.11r Fast Transition, on page 96
Monitoring 802.11r Fast Transition (CLI), on page 105

Restrictions for 802.11r Fast Transition, on page 95

Configuring 802.11 Fast Transition (GUI)

Step 1 Click **Configuration** > **Wireless** > **WLANs**
The **WLANs** page is displayed.

Step 2 Locate the WLAN you want to configure by using the search mechanism on the page.

Step 3 Click on the **WLAN Profile** of the WLAN.
The **WLAN > Edit** page is displayed.

Step 4 Click the **Security** and **Layer 2** tab.

Step 5 Enable the **Fast Transition** checkbox to enable BSS Fast Transition.
Uncheck the **Fast Transition** checkbox to disable BSS Fast Transition.

Step 6 To enable BSS Fast Transition over the distributed system, enable the **Over the DS** checkbox. This is enabled by default.

Note Disabling over the DS enables over the air fast transition.

Step 7 (Optional) Specify a reassociation timeout value in seconds in the **Reassociation Timeout** text box. The range is 1 to 100 seconds. The default value is 20 seconds.

Step 8 Click **Apply**.

Related Topics

Information About 802.11r Fast Transition, on page 96
Monitoring 802.11r Fast Transition (CLI), on page 105
Restrictions for 802.11r Fast Transition, on page 95

Disabling 802.11r Fast Transition (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **no security ft** [**over-the-ds** | **reassociation-timeout** *timeout-in-seconds*]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**no security ft** [**over-the-ds** | **reassociation-timeout** *timeout-in-seconds*] **Example:** `Switch(config-wlan)# no security ft over-the-ds`	Disables 802.11r Fast Transition on the WLAN. **Note** Disabling 802.11r Fast Transition for over the data source enables over the air fast transition.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Information About 802.11r Fast Transition, on page 96
Monitoring 802.11r Fast Transition (CLI), on page 105
Restrictions for 802.11r Fast Transition, on page 95

Monitoring 802.11r Fast Transition (CLI)

The following command can be used to monitor 802.11r Fast Transition:

Command	Description
show wlan name *wlan-name*	Displays a summary of the configured parameters on the WLAN.

Command	Description
show wireless cli mac-address *mac-address*	Displays the summary of the 802.11r authentication key management configuration on a client. . . . . . . Client Capabilities CF Pollable : Not implemented CF Poll Request : Not implemented Short Preamble : Not implemented PBCC : Not implemented Channel Agility : Not implemented Listen Interval : 15 Fast BSS Transition : Implemented Fast BSS Transition Details : Client Statistics: Number of Bytes Received : 9019 Number of Bytes Sent : 3765 Number of Packets Received : 130 Number of Packets Sent : 36 Number of EAP Id Request Msg Timeouts : 0 Number of EAP Request Msg Timeouts : 0 Number of EAP Key Msg Timeouts : 0 Number of Data Retries : 1 Number of RTS Retries : 0 Number of Duplicate Received Packets : 1 Number of Decrypt Failed Packets : 0 Number of Mic Failured Packets : 0 Number of Mic Missing Packets : 0 Number of Policy Errors : 0 Radio Signal Strength Indicator : -48 dBm Signal to Noise Ratio : 40 dB . . . . . .

Related Topics

Configuring 802.11r Fast Transition in an Open WLAN (CLI), on page 99
Disabling 802.11r Fast Transition (CLI), on page 104
Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI), on page 101
Configuring 802.11r Fast Transition on a PSK Security Enabled WLAN (CLI), on page 102
Configuring 802.11 Fast Transition (GUI), on page 104
Information About 802.11r Fast Transition, on page 96

Additional References for 802.11r Fast Transition

Related Documents

Related Topic	Document Title
WLAN Command Reference.	*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
802.11r from IEEE.	IEEE Standard for 802.11r

MIBs

MIB	MIBs Link
All MIBs supported for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

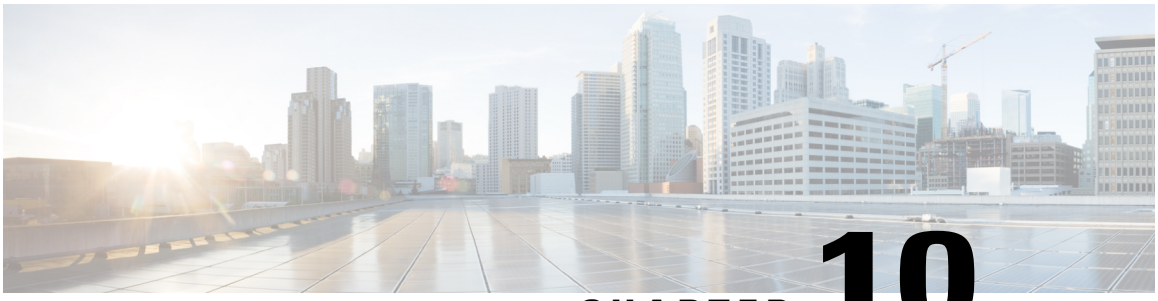
Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for 802.11r Fast Transition

This table lists the features in this module and provides links to specific configuration information:

Feature Name	Release	Feature Information
802.11r Fast Transition	Cisco IOS XE 3.3SE	This feature was introduced.



CHAPTER 10

Configuring Assisted Roaming

- Finding Feature Information, page 109
- Restrictions for Assisted Roaming, page 109
- Information About Assisted Roaming, page 110
- How to Configure Assisted Roaming, page 111
- Monitoring Assisted Roaming, page 113
- Configuration Examples for Assisted Roaming, page 113
- Additional References for Assisted Roaming, page 114
- Feature History and Information For Performing Assisted Roaming Configuration, page 115

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. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Restrictions for Assisted Roaming

- The assisted roaming feature is supported across multiple controllers.
- This feature is supported only on 802.11n capable indoor access points. For a single band configuration, a maximum of 6 neighbors are visible in a neighbor list. For dual band configuration, a maximum of 12 neighbors are visible.
- You can configure assisted roaming only using the switch CLI.

Related Topics

Information About Assisted Roaming, on page 110
Configuring Assisted Roaming (CLI), on page 111
Monitoring Assisted Roaming, on page 113
Configuration Examples for Assisted Roaming, on page 113

Information About Assisted Roaming

The 802.11k standard allows clients to request neighbor reports containing information about known neighbor access points that are candidates for a service set transition. The use of the 802.11k neighbor list can limit the need for active and passive scanning.

The assisted roaming feature is based on an intelligent and client optimized neighbor list.

Unlike the Cisco Client Extension (CCX) neighbor list, the 802.11k neighbor list is generated dynamically on-demand and is not maintained on the switch. The 802.11k neighbor list is based on the location of the clients without requiring the mobility services engine (MSE). Two clients on the same switch but different APs can have different neighbor lists delivered depending on their individual relationship with the surrounding APs.

By default, the neighbor list contains only neighbors in the same band with which the client is associated. However, a switch exists that allows 802.11k to return neighbors in both bands.

Clients send requests for neighbor lists only after associating with the APs that advertize the RRM (Radio Resource Management) capability information element (IE) in the beacon. The neighbor list includes information about BSSID, channel, and operation details of the neighboring radios.

Assembling and Optimizing the Neighbor List

When the switch receives a request for an 802.11k neighbor list, the following occurs:

1. The switch searches the RRM neighbor table for a list of neighbors on the same band as the AP with which the client is currently associated with.
2. The switch checks the neighbors according to the RSSI (Received Signal Strength Indication) between the APs, the current location of the present AP, the floor information of the neighboring AP from Cisco Prime Infrastructure, and roaming history information on the switch to reduce the list of neighbors to six per band. The list is optimized for APs on the same floor.

Assisted Roaming for Non-802.11k Clients

It is also possible to optimize roaming for non-802.11k clients. You can generate a prediction neighbor list for each client without the client requiring to send an 802.11k neighbor list request. When this is enabled on a WLAN, after each successful client association/reassociation, the same neighbor list optimization is applied on the non-802.11k client to generate the neighbor list and store the list in the mobile station software data structure. Clients at different locations have different lists because the client probes are seen with different RSSI values by different neighbors. Because clients usually probe before any association or reassociation, this list is constructed with the most updated probe data and predicts the next AP that the client is likely to roam to.

We discourage clients from roaming to those less desirable neighbors by denying association if the association request to an AP does not match the entries on the stored prediction neighbor list.

Similar to aggressive load balancing, there is a switch to turn on the assisted roaming feature both on a per-WLAN basis and globally. The following options are available:

- Denial count—Maximum number of times a client is refused association.
- Prediction threshold—Minimum number of entries required in the prediction list for the assisted roaming feature to be activated.

Because both load balancing and assisted roaming are designed to influence the AP that a client associates with, it is not possible to enable both the options at the same time on a WLAN.

Related Topics

Configuring Assisted Roaming (CLI), on page 111
Monitoring Assisted Roaming, on page 113
Configuration Examples for Assisted Roaming, on page 113
Restrictions for Assisted Roaming, on page 109

How to Configure Assisted Roaming

Configuring Assisted Roaming (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wireless assisted-roaming floor-bias** *dBm*
3. **wlan** *wlan-id*
4. **assisted-roaming neighbor-list**
5. **assisted-roaming dual-list**
6. **assisted-roaming prediction**
7. **wireless assisted-roaming prediction-minimum** *count*
8. **wireless assisted-roaming denial-maximum** *count*
9. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**wireless assisted-roaming floor-bias** *dBm* **Example:** `Switch(config)# wireless assisted-roaming floor-bias 20`	Configures neighbor floor label bias. The valid range is from 5 to 25 dBm, and the default value is 15 dBm.
Step 3	**wlan** *wlan-id* **Example:** `Switch(config)# wlan wlan1`	Enters the WLAN configuration submode. The *wlan-name* is the profile name of the configured WLAN.
Step 4	**assisted-roaming neighbor-list** **Example:** `Switch(wlan)# assisted-roaming neighbor-list`	Configures an 802.11k neighbor list for a WLAN. By default, assisted roaming is enabled on the neighbor list when you create a WLAN. The **no** form of the command disables assisted roaming neighbor list.
Step 5	**assisted-roaming dual-list** **Example:** `Switch(wlan)# assisted-roaming dual-list`	Configures a dual-band 802.11k dual list for a WLAN. By default, assisted roaming is enabled on the dual list when you create a WLAN. The **no** form of the command disables assisted roaming dual list.
Step 6	**assisted-roaming prediction** **Example:** `Switch(wlan)# assisted-roaming prediction`	Configures assisted roaming prediction list feature for a WLAN. By default, the assisted roaming prediction list is disabled. **Note** A warning message is displayed and load balancing is disabled for the WLAN if load balancing is already enabled for the WLAN.
Step 7	**wireless assisted-roaming prediction-minimum** *count* **Example:** `Switch# wireless assisted-roaming prediction-minimum`	Configures the minimum number of predicted APs required for the prediction list feature to be activated. The default value is 3. **Note** If the number of the AP in the prediction assigned to the client is less than the number that you specify, the assisted roaming feature will not apply on this roam.
Step 8	**wireless assisted-roaming denial-maximum** *count* **Example:** `Switch# wireless assisted-roaming denial-maximum 8`	Configures the maximum number of times a client can be denied association if the association request is sent to an AP does not match any AP on the prediction. The valid range is from 1 to 10, and the default value is 5.
Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Information About Assisted Roaming, on page 110
Restrictions for Assisted Roaming, on page 109

Monitoring Assisted Roaming

The following command can be used to monitor assisted roaming configured on a WLAN. .

Command	Description
show wlan id *wlan-id*	Displays the WLAN parameters on the WLAN.

Related Topics

Information About Assisted Roaming, on page 110
Restrictions for Assisted Roaming, on page 109

Configuration Examples for Assisted Roaming

This example shows how to configure the neighbor floor label bias:

```
Switch# configure terminal
Switch(config)# wireless assisted-roaming floor-bias 10
Switch(config)# end
Switch# show wlan id 23
```

This example shows how to disable neighbor list on a specific WLAN:

```
Switch# configure terminal
Switch(config)# wlan test1
Switch(config (wlan)# no assisted-roaming neighbor-list
Switch(config)(wlan)# end
Switch# show wlan id 23
```

This example shows how to configure the prediction list on a specific WLAN:

```
Switch# configure terminal
Switch(config)# wlan test1
Switch(config)(wlan)# assisted-roaming prediction
Switch(config)(wlan)# end
Switch# show wlan id 23
```

This example shows how to configure the prediction list based on assisted roaming prediction threshold and maximum denial count on a specific WLAN:

```
Switch# configure terminal
Switch(config)# wireless assisted-roaming prediction-minimum 4
Switch(config)# wireless assisted-roaming denial-maximum 4
Switch(config)(wlan)# end
Switch# show wlan id 23
```

Related Topics

Information About Assisted Roaming, on page 110
Restrictions for Assisted Roaming, on page 109

Additional References for Assisted Roaming

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
802.11k	—

MIBs

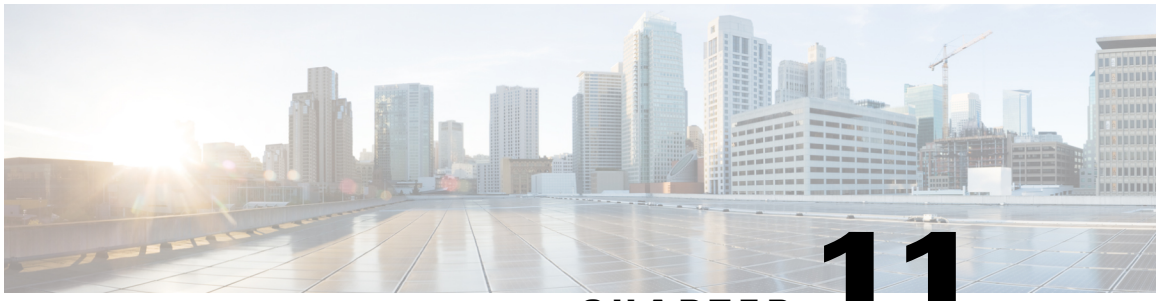
MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Performing Assisted Roaming Configuration

Feature Name	Release	Feature Information
Assisted Roaming	Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 11

Configuring Access Point Groups

- Finding Feature Information, page 117
- Prerequisites for Configuring AP Groups, page 117
- Restrictions for Configuring Access Point Groups, page 118
- Information About Access Point Groups, page 118
- How to Configure Access Point Groups, page 120
- Additional References, page 122
- Feature History and Information for Access Point Groups, page 123

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. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Prerequisites for Configuring AP Groups

The following are the prerequisites for creating access point groups on a switch:

- The required access control list (ACL) must be defined on the router that serves the VLAN or subnet.
- Multicast traffic is supported with access point group VLANs. However, if the client roams from one access point to another, the client might stop receiving multicast traffic, unless IGMP snooping is enabled.

Related Topics

Information About Access Point Groups, on page 118

Restrictions for Configuring Access Point Groups, on page 118

Restrictions for Configuring Access Point Groups

- Suppose that the interface mapping for a WLAN in the AP group table is the same as the WLAN interface. If the WLAN interface is changed, the interface mapping for the WLAN in the AP group table also changes to the new WLAN interface.

  Suppose that the interface mapping for a WLAN in the AP group table is different from the one defined for the WLAN. If the WLAN interface is changed, then the interface mapping for the WLAN in the AP group table does not change to the new WLAN interface.

- If you clear the configuration on the switch, all of the access point groups disappear except for the default access point group "default-group," which is created automatically.

- The default access point group can have up to 16 WLANs associated with it. The WLAN IDs for the default access point group must be less than or equal to 16. If a WLAN with an ID greater than 16 is created in the default access point group, the WLAN SSID will not be broadcasted. All WLAN IDs in the default access point group must have an ID that is less than or equal to 16. WLANs with IDs greater than 16 can be assigned to custom access point groups.

Related Topics

Information About Access Point Groups, on page 118
Prerequisites for Configuring AP Groups, on page 117

Information About Access Point Groups

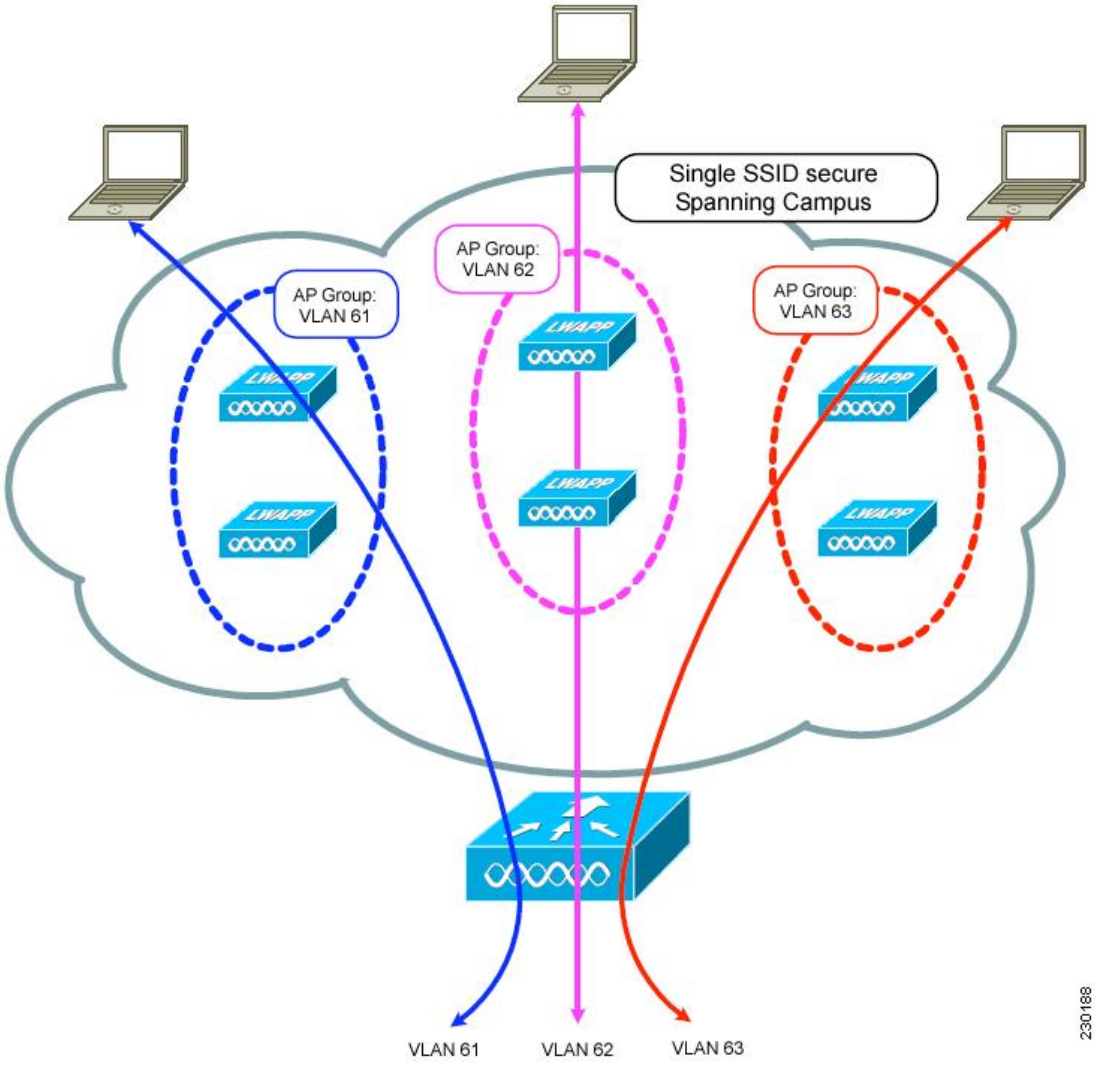
After you create up to 512 WLANs on the switch, you can selectively publish them (using access point groups) to different access points to better manage your wireless network. In a typical deployment, all users on a WLAN are mapped to a single interface on the switch. Therefore, all users that are associated with that WLAN are on the same subnet or VLAN. However, you can choose to distribute the load among several interfaces or to a group of users based on specific criteria such as individual departments (such as Marketing) by creating access point groups. Additionally, these access point groups can be configured in separate VLANs to simplify network administration.

In the figure, three configured dynamic interfaces are mapped to three different VLANs (VLAN 61, VLAN 62, and VLAN 63). Three access point groups are defined, and each is a member of a different VLAN, but all are members of the same SSID. A client within the wireless SSID is assigned an IP address from the VLAN subnet on which its access point is a member. For example, any user that associates with an access point that is a member of access point group VLAN 61 is assigned an IP address from that subnet.

In the figure, the switch internally treats roaming between access points as a Layer 3 roaming event. In this way, WLAN clients maintain their original IP addresses.

After all access points have joined the switch, you can create access point groups and assign up to 16 WLANs to each group. Each access point advertises only the enabled WLANs that belong to its access point group. The access point does not advertise disabled WLANs in its access point group or WLANs that belong to another group.

Figure 4: Access Point Groups



Related Topics

Creating Access Point Groups, on page 120
Viewing Access Point Group, on page 121
Assigning an Access Point to an AP Group, on page 121
Prerequisites for Configuring AP Groups, on page 117
Restrictions for Configuring Access Point Groups, on page 118

How to Configure Access Point Groups

Creating Access Point Groups

Before You Begin

You must have administrator privileges to perform this operation.

SUMMARY STEPS

1. **configure terminal**
2. **ap group** *ap-group-name*
3. **wlan** *wlan-name*
4. (Optional) **vlan** *vlan-name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap group** *ap-group-name* **Example:** `Switch(config)# ap group my-ap-group`	Creates an access point group.
Step 3	**wlan** *wlan-name* **Example:** `Switch(config-apgroup)# wlan wlan-name`	Associates the AP group to a WLAN.
Step 4	**vlan** *vlan-name* **Example:** `Switch(config-apgroup)# vlan test-vlan`	(Optional) Assigns the access point group to a VLAN.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

This example shows how to create an AP group:

```
Switch# configure terminal
```

```
Switch(config-apgroup)# ap group test-ap-group-16
Switch(config-wlan-apgroup)# wlan test-ap-group-16
Switch(config-wlan-apgroup)# vlan VLAN1300
```

Related Topics

Information About Access Point Groups, on page 118

Assigning an Access Point to an AP Group

Before You Begin

You must have administrator privileges to perform this operation.

SUMMARY STEPS

1. **ap name** *ap-name* **ap-group-name** *ap-group*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ap name** *ap-name* **ap-group-name** *ap-group* **Example:** `Switch# ap name 1240-101 ap-groupname apgroup_16`	Assigns the access point to the access point group. The keywords and arguments are as follows: • **name**—Specifies that the argument following this keyword is the name of an AP that is associated to the switch. • *ap-name*—AP that you want to associate to the AP group. • **ap-group-name**—Specifies that the argument following this keyword is the name of the AP group that is configured on the switch. • *ap-group*—Name of the access point group that is configured on the switch.

Related Topics

Information About Access Point Groups, on page 118

Viewing Access Point Group

Before You Begin

You must have administrator privileges to perform this operation.

SUMMARY STEPS

1. **show ap groups** [**extended**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show ap groups** [**extended**] **Example:** `Switch# show ap groups`	Displays the AP groups configured on the switch. The **extended** keyword displays all AP Groups information defined in the system in detail.

Related Topics

Information About Access Point Groups, on page 118

Additional References

Related Documents

Related Topic	Document Title
WLAN commands	*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
Lightweight Access Point configuration	*Lightweight Access Point Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
Lightweight Access Point commands	*Lightweight Access Point Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for Access Point Groups

This table lists the features in this modules and provides links to specific configuration information.

Feature Name	Release	Feature Information
AP Groups	Cisco IOS XE 3.2SE	This feature was introduced.

INDEX

C

CCX 25
  described 25

D

default-group access point group 118
DHCP option 82 50, 51
  described 50
  example 51
DHCP servers 49
  internal 49
diagnostic channel 26
  described 26
DTIM 25

P

peer-to-peer blocking 26
  described 26

Q

QoS Policy, WLAN 43

S

SSID 23
  described 23

W

WLAN broadcast ssid, Configure 33
WLAN call snoop, Configure 33
WLAN interface VLAN, Configure 33
WLAN media stream multicast, Configure 33
WLAN radio, Configure 33
WLAN, enable, disable 33
WLANs 25
  session timeout 25
    described 25