WLAN Command Reference, Cisco IOS XE Release 3E (Catalyst 3850 Switches)

First Published: May 30, 2014

Last Modified: 0,

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

Text Part Number: OL-32349-01

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)

© 2014 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface vii

Document Conventions vii

Related Documentation ix

Obtaining Documentation and Submitting a Service Request ix

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 5

CLI Error Messages 5

Configuration Logging 5

How to Use the CLI to Configure Features 6

Configuring the Command History 6

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 9

Editing Command Lines That Wrap 10

Searching and Filtering Output of show and more Commands 11

Accessing the CLI on a Switch Stack 12

Accessing the CLI Through a Console Connection or Through Telnet 12

CHAPTER 2

WLAN Commands 13

aaa-override 15

accounting-list 16
assisted-roaming 17
band-select 19
broadcast-ssid 20
call-snoop 21
channel-scan defer-priority 23
channel-scan defer-time 24
chd 25
client association limit 26
client vlan 28
ccx aironet-iesupport 29
datalink flow monitor 30
device-classification 32
default 33
dtim dot11 36
exclusionlist 37
exit 38
exit (WLAN AP Group) 39
ip access-group 40
ip flow monitor 41
ip verify source mac-check 42
load-balance 43
mobility anchor 44
nac 46
passive-client 47
peer-blocking 48
radio 49
radio-policy 51
roamed-voice-client re-anchor 53
security ft 54
security pmf 56
security web-auth 58
security wpa akm 59
service-policy (WLAN) 61
session-timeout 63

show wlan 64
shutdown 67
sip-cac 68
static-ip tunneling 69
vlan 70
wgb non-cisco 71
wifidirect policy 72
wlan (AP Group Configuration) 73
wlan 74
wlan shutdown 75
wmm 76

Preface

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

Document Conventions

This document uses the following conventions:

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

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

Reader Alert Conventions

This document may use the following conventions for reader alerts:

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

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Documentation

Note Before installing or upgrading the 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/c/en/us/td/docs/general/whatsnew/whatsnew.html

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

Using the Command-Line Interface

- Information About Using the Command-Line Interface, page 1
- How to Use the CLI to Configure Features, page 6

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)#`		Use this mode to configure parameters for the Ethernet ports.

Mode	Access Method	Prompt	Exit Method	About This Mode
			To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	
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.

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.
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.
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`	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

	Command or Action	Purpose
	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)# $**15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45**	line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.
Step 2	**Ctrl-A** **Example:** Switch(config)# **access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2$**	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* **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	Searches and filters the output. Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain **output** are not displayed, but the lines that contain **output** appear.

Accessing the CLI 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.

WLAN Commands

- aaa-override, page 15
- accounting-list, page 16
- assisted-roaming, page 17
- band-select, page 19
- broadcast-ssid, page 20
- call-snoop, page 21
- channel-scan defer-priority, page 23
- channel-scan defer-time, page 24
- chd, page 25
- client association limit, page 26
- client vlan, page 28
- ccx aironet-iesupport, page 29
- datalink flow monitor, page 30
- device-classification, page 32
- default, page 33
- dtim dot11, page 36
- exclusionlist, page 37
- exit, page 38
- exit (WLAN AP Group), page 39
- ip access-group, page 40
- ip flow monitor, page 41
- ip verify source mac-check, page 42
- load-balance, page 43
- mobility anchor, page 44

- nac, page 46
- passive-client, page 47
- peer-blocking, page 48
- radio, page 49
- radio-policy, page 51
- roamed-voice-client re-anchor, page 53
- security ft, page 54
- security pmf, page 56
- security web-auth, page 58
- security wpa akm, page 59
- service-policy (WLAN), page 61
- session-timeout, page 63
- show wlan, page 64
- shutdown, page 67
- sip-cac, page 68
- static-ip tunneling, page 69
- vlan, page 70
- wgb non-cisco, page 71
- wifidirect policy, page 72
- wlan (AP Group Configuration), page 73
- wlan, page 74
- wlan shutdown, page 75
- wmm, page 76

aaa-override

To enable AAA override on the WLAN, use the **aaa-override** command. To disable AAA override, use the **no** form of this command.

aaa-override

no aaa-override

Syntax Description

This command has no keywords or arguments.

Command Default

AAA is disabled by default.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to enable AAA on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
Switch(config-wlan)# aaa-override
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
```

This example shows how to disable AAA on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
Switch(config-wlan)# no aaa-override
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

accounting-list

To configure RADIUS accounting servers on a WLAN, use the **accounting-list** command. To disable RADIUS server accounting, use the **no** form of this command.

accounting-list *radius-server-acct*

no accounting-list

Syntax Description

radius-server-acct	Accounting RADIUS server name.

Command Default

RADIUS server accounting is disabled by default.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to configure RADIUS server accounting on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# accounting-list test
Switch(config-wlan)# end
```

This example shows how to disable RADIUS server accounting on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no accounting-list test
Switch(config-wlan)# end
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

assisted-roaming

To configure assisted roaming using 802.11k on a WLAN, use the **assisted-roaming** command. To disable assisted roaming, use the **no** form of this command.

assisted-roaming {**dual-list| neighbor-list| prediction**}

no assisted-roaming {**dual-list| neighbor-list| prediction**}

Syntax Description

dual-list	Configures a dual band 802.11k neighbor list for a WLAN. The default is the band that the client is currently associated with.
neighbor-list	Configures an 802.11k neighbor list for a WLAN.
prediction	Configures assisted roaming optimization prediction for a WLAN.

Command Default

Neighbor list and dual band support are enabled by default. The default is the band that the client is currently associated with.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

When you enable the assisted roaming prediction list, a warning appears and load balancing is disabled for the WLAN if load balancing is already enabled on the WLAN. To make changes to the WLAN, the WLAN must be in disabled state.

Examples

The following example shows how to configure a 802.11k neighbor list on a WLAN:

```
Switch(config-wlan)#assisted-roaming neighbor-list
```

The following example shows the warning message when load balancing is enabled on a WLAN. Load balancing must be disabled if it is already enabled when configuring assisted roaming:

```
Switch(config)#wlan test-prediction 2 test-prediction
Switch(config-wlan)#client vlan 43
Switch(config-wlan)#no security wpa
Switch(config-wlan)#load-balance
Switch(config-wlan)#assisted-roaming prediction
WARNING: Enabling neighbor list prediction optimization may slow association and impact
VOICE client perform.
Are you sure you want to continue? (y/n)[y]: y
```

```
% Request aborted - Must first disable Load Balancing before enabling Assisted Roaming
Prediction Optimization on this WLAN.
```

band-select

To configure band selection on a WLAN, use the **band-select** command. To disable band selection, use the **no** form of this command.

band-select

no band-select

Syntax Description

This command has no keywords or arguments.

Command Default

Band selection is disabled by default.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When you enable band select on a WLAN, the access point suppresses client probes on 2.4GHz and moves the dual band clients to the 5-GHz spectrum. The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to enable band select on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# band-select
Switch(config-wlan)# end
```

This example shows how to disable band selection on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no band-select
Switch(config-wlan)# end
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

broadcast-ssid

To enable a Service Set Identifier (SSID) on a WLAN, use the **broadcast-ssid** command. To disable broadcasting of SSID, use the **no** form of this command.

broadcast-ssid

no broadcast-ssid

Syntax Description

This command has no keywords or arguments.

Command Default

The SSIDs of WLANs are broadcasted by default.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to enable a broadcast SSID on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# broadcast-ssid
Switch(config-wlan)# end
```

This example shows how to disable a broadcast SSID on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no broadcast-ssid
Switch(config-wlan)# end
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

call-snoop

To enable Voice over IP (VoIP) snooping on a WLAN, use the **call-snoop** command. To disable Voice over IP (VoIP), use the **no** form of this command.

call-snoop

no call-snoop

Syntax Description

This command has no keywords or arguments.

Command Default

VoIP snooping is disabled by default.

Command Modes

WLN configuration

Usage Guidelines

You must disable the WLAN before using this command. See the Related Commands section for more information on how to disable a WLAN.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The WLAN on which call snooping is configured must be configured with Platinum QoS. You must disable quality of service before using this command. See Related Commands section for more information on configuring QoS service-policy.

Examples

This example shows how to enable VoIP on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# call-snoop
Switch(config-wlan)# end
```

This example shows how to disable VoIP on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no call-snoop
Switch(config-wlan)# end
```

Related Commands

Command	Description
service-policy (WLAN)	Configures the QoS Policy on a WLAN.

Command	Description
wlan	Creates or disables a WLAN.

channel-scan defer-priority

To configure the device to defer priority markings for packets that can defer off-channel scanning, use the **channel-scan defer-priority** command. To disable the device to defer priority markings for packets that can defer off-channel scanning, use the **no** form of this command.

channel-scan defer-priority *priority*

no channel-scan defer-priority *priority*

Syntax Description

priority	Channel priority value. The range is 0 to 7. The default is 3.

Command Default

Channel scan defer is enabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable channel scan defer priority on a WLAN and set it to a priority value 4:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# channel-scan defer-priority 4
Switch(config-wlan)# end
```

This example shows how to disable channel scan defer priority on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no channel-scan defer-priority 4
Switch(config-wlan)# end
```

channel-scan defer-time

To assign a channel scan defer time, use the **channel-scan defer-time** command. To disable the channel scan defer time, use the **no** form of this command.

channel-scan defer-time *msecs*

no channel-scan defer-time

Syntax Description

msecs	Deferral time in milliseconds. The range is from 0 to 60000. The default is 100.

Command Default

Channel-scan defer time is enabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The time value in milliseconds should match the requirements of the equipment on the WLAN.

Examples

This example shows how to enable a channel scan on the WLAN and set the scan deferral time to 300 milliseconds:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# channel-scan defer-time 300
Switch(config-wlan)# end
```

This example shows how to disable channel scan defer time on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no channel-scan defer-time
Switch(config-wlan)# end
```

chd

To enable coverage hole detection on a WLAN, use the **chd** command. To disable coverage hole detection, use the **no** form of this command.

chd

no chd

Syntax Description

This command has no keywords or arguments.

Command Default

Coverage hole detection is enabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable coverage hole detection on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# chd
Switch(config-wlan)# end
```

This example shows how to disable coverage hole detection on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no chd
Switch(config-wlan)# end
```

client association limit

To configure the maximum number of client connections, clients per access points, or clients per access point radio on a WLAN, use the **client association limit** command. To disable clients association limit on the WLAN, use the **no** form of this command.

client association limit {*association-limit*| **ap** *ap-limit*| **radio** *max-ap-radio-limit*}

no client association limit {*association-limit*| **ap** *ap-limit*| **radio** *max-ap-radio-limit*}

Syntax Description

association-limit	Number of client connections to be accepted. The range is from 0 to 2000. A value of zero (0) indicates no set limit.
ap	Maximum number of clients per access point.
ap-limit	Configures the maximum number of client connections to be accepted per access point radio. The valid range is from 0 to 400.
radio	Configures the maximum number of clients per AP radio.
max-ap-radio-limit	Maximum number of client connections to be accepted per access point radio. The valid range is from 0 - 200.

Command Default

The maximum number of client connections is set to 0 (no limit).

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The command was modified. The **ap** and **radio** keywords were added.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to configure a client association limit on a WLAN and configure the client limit to 200:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
Switch(config-wlan)# client association limit 200
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
```

This example shows how to disable a client association limit on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
Switch(config-wlan)# no client association limit
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
```

This example shows how to configure a client association limit per radio on a WLAN and configure the client limit to 200:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# client association limit radio 200
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
```

This example shows how to configure a client association limit per AP on a WLAN and configure the client limit to 300::

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# client association limit ap 300
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

client vlan

To configure a WLAN interface or an interface group, use the **client vlan** command. To disable the WLAN interface, use the **no** form of this command.

client vlan *interface-id-name-or-group-name*

no client vlan

Syntax Description

interface--id-name-or-group-name	Interface ID, name, or VLAN group name.

Command Default

The default interface is configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to enable a client VLAN on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# client vlan client-vlan1
Switch(config-wlan)# end
```

This example shows how to disable a client VLAN on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no client vlan
Switch(config-wlan)# end
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

ccx aironet-iesupport

To enable Aironet Information Elements (IEs) for a WLAN, use the **ccx aironet-iesupport** command. To disable Aironet Information Elements (IEs), use the **no** form of this command.

ccx aironet-iesupport

no ccx aironet-iesupport

Syntax Description

This command has no keywords or arguments.

Command Default

Aironet IE support is enabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to enable an Aironet IE for a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# ccx aironet-iesupport
Switch(config-wlan)# end
```

This example shows how to disable an Aironet IE on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no ccx aironet-iesupport
Switch(config-wlan)# end
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

datalink flow monitor

To enable NetFlow monitoring in a WLAN, use the **datalink flow monitor** command. To disable NetFlow monitoring, use the **no** form of this command.

datalink flow monitor *datalink-monitor-name* {**input**| **output**}

no datalink flow monitor *datalink-monitor-name* {**input**| **output**}

Syntax Description

datalink-monitor-name	Flow monitor name. The datalink monitor name can have up to 31 characters.
input	Specifies the NetFlow monitor for ingress traffic.
output	Specifies the NetFlow monitor for egress traffic.

Command Default

None.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to enable NetFlow monitoring on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# datalink flow monitor test output
Switch(config-wlan)# end
```

This example shows how to disable NetFlow monitoring on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no datalink flow monitor test output
Switch(config-wlan)# end
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

device-classification

To enable client device classification in a WLAN, use the **device-classification** command. To disable device classification, use the **no** form of this command.

device-classification

no device-classification

Syntax Description

device-classification	Enables/Disables Client Device Classification.

Command Default

None.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# device-classification
Switch(config-wlan)# end
```

default

To set the parameters to their default values, use the **default** command.

default {**aaa-override**| **accounting-list**| **band-select**| **broadcast-ssid**| **call-snoop**| **ccx**| **channel-scan**| **parameters**| **chd**| **client**| **datalink**| **diag-channel**| **dtim**| **exclusionlist**| **ip**| **ipv6**| **load-balance**| **local-auth**| **mac-filtering**| **media-stream**| **mfp**| **mobility**| **nac**| **passive-client**| **peer-blocking**| **radio**| **roamed-voice-client**| **security**| **service-policy**| **session-timeout**| **shutdown**| **sip-cac**| **static-ip**| **uapsd**| **wgb**| **wmm**}

Syntax Description

aaa-override	Sets the AAA override parameter to its default value.
accounting-list	Sets the accounting parameter and its attributes to their default values.
band-select	Sets the band selection parameter to its default values.
broadcast-ssid	Sets the broadcast Service Set Identifier (SSID) parameter to its default value.
call-snoop	Sets the call snoop parameter to its default value.
ccx	Sets the Cisco client extension (Cisco Aironet IE) parameters and attributes to their default values.
channel-scan	Sets the channel scan parameters and attributes to their default values.
chd	Sets the coverage hold detection parameter to its default value.
client	Sets the client parameters and attributes to their default values.
datalink	Sets the datalink parameters and attributes to their default values.
diag-channel	Sets the diagnostic channel parameters and attributes to their default values.
dtim	Sets the Delivery Traffic Indicator Message (DTIM) parameter to its default value.
exclusionlist	Sets the client exclusion timeout parameter to its default value.
ip	Sets the IP parameters to their default values.
ipv6	Sets the IPv6 parameters and attributes to their default values.
load-balance	Sets the load-balancing parameter to its default value.
local-auth	Sets the Extensible Authentication Protocol (EAP) profile parameters and attributes to their default values.
mac-filtering	Sets the MAC filtering parameters and attributes to their default values.

media-stream	Sets the media stream parameters and attributes to their default values.
mfp	Sets the Management Frame Protection (MPF) parameters and attributes to their default values.
mobility	Sets the mobility parameters and attributes to their default values.
nac	Sets the RADIUS Network Admission Control (NAC) parameter to its default value.
passive-client	Sets the passive client parameter to its default value.
peer-blocking	Sets the peer to peer blocking parameters and attributes to their default values.
radio	Sets the radio policy parameters and attributes to their default values.
roamed-voice-client	Sets the roamed voice client parameters and attributes to their default values.
security	Sets the security policy parameters and attributes to their default values.
service-policy	Sets the WLAN quality of service (QoS) policy parameters and attributes to their default values.
session-timeout	Sets the client session timeout parameter to its default value.
shutdown	Sets the shutdown parameter to its default value.
sip-cac	Sets the Session Initiation Protocol (SIP) Call Admission Control (CAC) parameters and attributes to their default values.
static-ip	Sets the static IP client tunneling parameters and their attributes to their default values.
uapsd	Sets the Wi-Fi Multimedia (WMM) Unscheduled Automatic Power Save Delivery (UAPSD) parameters and attributes to their default values.
wgb	Sets the Workgroup Bridges (WGB) parameter to its default value.
wmm	Sets the WMM parameters and attributes to their default values.

Command Default None.

Command Modes WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to set the Cisco Client Extension parameter to its default value:

```
Switch(config-wlan)# default ccx aironet-iesupport
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

dtim dot11

To configure the Delivery Traffic Indicator Message (DTIM) period for a WLAN, use the **dtim dot11** command. To disable DTIM, use the **no** form of this command.

dtim dot11 {**5ghz**| **24ghz**} *dtim-period*

no dtim dot11 {**5ghz**| **24ghz**} *dtim-period*

Syntax Description

5ghz	Configures the DTIM period on the 5-GHz band.
24ghz	Configures the DTIM period on the 2.4-GHz band.
dtim-period	Value for the DTIM period. The range is from 1 to 255.

Command Default

The DTIM period is set to 1.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to enable the DTIM period on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# dtim dot11 24ghz 3
```

This example shows how to disable the DTIM period on a WLAN on the 2.4-GHz band:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no dtim dot11 24ghz 3
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

exclusionlist

To configure an exclusion list on a wireless LAN, use the **exclusionlist** command. To disable an exclusion list, use the **no** form of this command.

exclusionlist [**timeout** *seconds*]

no exclusionlist [timeout]

Syntax Description

timeout *seconds*	(Optional) Specifies an exclusion list timeout in seconds. The range is from 0 to 2147483647. A value of zero (0) specifies no timeout.

Command Default

The exclusion list is set to 60 seconds.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to configure a client exclusion list for a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# exclusionlist timeout 345
```

This example shows how to disable a client exclusion list on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no exclusionlist timeout 345
```

exit

To exit the WLAN configuration submode, use the **exit** command.

exit

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to exit the WLAN configuration submode:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# exit
Switch(config)#
```

exit (WLAN AP Group)

To exit the WLAN access point group submode, use the **exit** command.

exit

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

WLAN AP Group configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to exit the WLAN AP group submode:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ap group test
Switch(config-apgroup)# exit
```

ip access-group

To configure WLAN access control group (ACL), use the **ip access-group** command. To remove a WLAN ACL group, use the **no** form of the command.

ip access-group [web] *acl-name*

no ip access-group [web]

Syntax Description

web	(Optional) Configures the IPv4 web ACL.
acl-name	Specify the preauth ACL used for the WLAN with the security type value as webauth.

Command Default

None

Command Modes

WLAN configuration

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure a WLAN ACL:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wlan wlan1
Switch(config-wlan)#ip access-group test-acl
```

This example shows how to configure an IPv4 WLAN web ACL:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# ip access-group web test
Switch(config-wlan)#
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

ip flow monitor

To configure IP NetFlow monitoring, use the **ip flow monitor** command. To remove IP NetFlow monitoring, use the **no** form of this command.

ip flow monitor *ip-monitor-name* {**input**| **output**}

no ip flow monitor *ip-monitor-name* {**input**| **output**}

Syntax Description

ip-monitor-name	Flow monitor name.
input	Enables a flow monitor for ingress traffic.
output	Enables a flow monitor for egress traffic.

Command Default

None

Command Modes

WLAN configuration

Usage Guidelines

You must disable the WLAN before using this command.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure an IP flow monitor for the ingress traffic:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# ip flow monitor test input
```

This example shows how to disable an IP flow monitor:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no ip flow monitor test input
```

ip verify source mac-check

To enable IPv4 Source Guard (IPSG) on a WLAN, use the **ip verify source mac-check** command. To disable IPSG, use the **no** form of this command.

ip verify source mac-check

no ip verify source mac-check

Syntax Description

This command has no keywords or arguments.

Command Default

IPSG is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this feature to restrict traffic from a host to a specific interface that is based on the host's IP address. The feature can also be configured to bind the source MAC and IP of a host so that IP spoofing is prevented.

Use this feature to bind the IP and MAC address of a wireless host that is based on information received from DHCP snooping, ARP, and Dataglean. Dataglean is the process of extracting location information such as host hardware address, ports that lead to the host, and so on from DHCP messages as they are forwarded by the DHCP relay agent. If a wireless host tries to send traffic with IP address and MAC address combination that has not been learned by the switch, this traffic is dropped in the hardware. IPSG is not supported on DHCP packets. IPSG is not supported for foreign clients in a foreign switch.

You must disable the WLAN before using this command.

Examples

This example shows how to enable IPSG:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# ip verify source mac-check
```

This example shows how to disable IPSG:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no ip verify source mac-check
```

load-balance

To enable load balancing on a WLAN, use the **load-balance** command. To disable load balancing, use the **no** form of this command.

load-balance

no load-balance

Syntax Description

This command has no keywords or arguments.

Command Default

Load balancing is disabled by default.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	The command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to enable load balancing on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# shutdown
Switch(config)# wlan wlan1
Switch(config-wlan)# load-balance
Switch(config)# no shutdown
Switch(config-wlan)# end
```

This example shows how to disable load balancing on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# shutdown
Switch(config)# wlan wlan1
Switch(config-wlan)# no load-balance
Switch(config)# no shutdown
Switch(config-wlan)# end
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

mobility anchor

To configure mobility sticky anchoring, use the **mobility anchor sticky** command. To disable the sticky anchoring, use the **no** form of the command.

To configure guest anchoring, use the **mobility anchor** *ip-address* command.

To delete the guest anchor, use the **no** form of the command.

To configure the device as an auto-anchor, use the **mobility anchor** command.

mobility anchor {*ip-address*| **sticky**}

no mobility anchor {*ip-address*| **sticky** }

Syntax Description

sticky	The client is anchored to the first switch that it associates. **Note** This command is by default enabled and ensures low roaming latency. This ensures that the point of presence for the client does not change when the client joins the mobility domain and roams within the domain.
ip-address	Configures the IP address for the guest anchor switch to this WLAN.

Command Default

Sticky configuration is enabled by default.

Command Modes

WLAN Configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The auto-anchor configuration required the device IP address to be entered prior to the Cisco IOS XE 3.3SE release; with this release, if no IP address is given, the device itself becomes an anchor; you do not have to explicitly specify the IP address.

Usage Guidelines

- The wlan_id or guest_lan_id must exist and be disabled.
- Auto-anchor mobility is enabled for the WLAN or wired guest LAN when you configure the first mobility anchor.
- Deleting the last anchor disables the auto-anchor mobility feature and resumes normal mobility for new associations.
- Mobility uses the following ports, that are allowed through the firewall:

- 16666
- 16667
- 16668

Examples

This example shows how to enable the sticky mobility anchor:

```
Switch(config-wlan)# mobility anchor sticky
```

This example shows how to configure guest anchoring:

```
Switch(config-wlan)# mobility anchor 209.165.200.224
```

This example shows how to configure the device as an auto-anchor:

```
Switch(config-wlan)# mobility anchor
```

nac

To enable RADIUS Network Admission Control (NAC) support for a WLAN, use the **nac** command. To disable NAC out-of-band support, use the **no** form of this command.

nac

no nac

Syntax Description

This command has no keywords or arguments.

Command Default

NAC is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You should enable AAA override before you enable the RADIUS NAC state.

Examples

This example shows how to configure RADIUS NAC on the WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# aaa-override
Switch(config-wlan)# nac
```

This example shows how to disable RADIUS NAC on the WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no nac
Switch(config-wlan)# no aaa-override
```

Related Commands

Command	Description
aaa-override	Enables or disables AAA override on a WLAN.

passive-client

To enable the passive client feature on a WLAN, use the **passive-client** command. To disable the passive client feature, use the **no** form of this command.

passive-client

no passive-client

Syntax Description

This command has no keywords or arguments.

Command Default

Passive client feature is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must enable the global multicast mode and multicast-multicast mode before entering this command. Both multicast-multicast mode and multicast unicast modes are supported. The multicast-multicast mode is recommended.

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This show how to enable the passive client feature on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wireless multicast
Switch(config)# wlan test-wlan
Switch(config-wlan)# passive-client
```

This example shows how to disable the passive client feature on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wireless multicast
Switch(config)# wlan test-wlan
Switch(config-wlan)# no passive-client
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

peer-blocking

To configure peer-to-peer blocking on a WLAN, use the **peer-blocking** command. To disable peer-to-peer blocking, use the **no** form of this command.

peer-blocking {**drop**| **forward-upstream**}

no peer-blocking

Syntax Description

drop	Specifies the switch to discard the packets.
forward-upstream	Specifies the packets to be forwarded on the upstream VLAN. The device next in the hierarchy to the switch decides what action to take regarding the packets.

Command Default

Peer blocking is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to enable the drop and forward-upstream options for peer-to-peer blocking:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# peer-blocking  drop
Switch(config-wlan)# peer-blocking forward-upstream
```

This example shows how to disable the drop and forward-upstream options for peer-to-peer blocking:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no peer-blocking  drop
Switch(config-wlan)# no peer-blocking forward-upstream
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

radio

To enable the Cisco radio policy on a WLAN, use the **radio** command. To disable the Cisco radio policy on a WLAN, use the **no** form of this command.

radio {**all**| **dot11a**| **dot11ag**| **dot11bg**| **dot11g**}

no radio

Syntax Description

all	Configures the WLAN on all radio bands.
dot11a	Configures the WLAN on only 802.11a radio bands.
dot11ag	Configures the WLAN on 802.11a/g radio bands.
dot11bg	Configures the wireless LAN on only 802.11b/g radio bands (only 802.11b if 802.11g is disabled).
dot11g	Configures the wireless LAN on 802.11g radio bands only.

Command Default

Radio policy is enabled on all bands.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to configure the WLAN on all radio bands:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# radio all
```

This example shows how to disable all radio bands on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no radio all
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

radio-policy

To configure the radio policy on a WLAN access point group, use the **radio-policy** command. To disable the radio policy on the WLAN, use the **no** form of this command.

radio-policy {**all**| **dot11a**| **dot11bg**| **dot11g**}

no radio{**all**| **dot11a**| **dot11bg**| **dot11g**}

Syntax Description

all	Configures the wireless LAN on all radio bands.
dot11a	Configures the wireless LAN on only 802.11a radio bands.
dot11bg	Configures the wireless LAN on only 802.11b/g (only 802.11b if 802.11g is disabled) radio bands.
dot11g	Configures the wireless LAN on only 802.11g radio bands.

Command Default

Radio policy is enabled on all the bands.

Command Modes

WLAN AP Group configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The WLAN must be restarted for the changes to take effect. See Related Commands section for more information on how to shutdown a WLAN.

Examples

This example shows how to enable the radio policy on the 802.11b band for an AP group:

```
Switch(config)# ap group test
Switch(config-apgroup)# wlan test-wlan
Switch(config-wlan-apgroup)# radio-policy dot11b
```

This example shows how to disable the radio policy on the 802.11b band of an AP group:

```
Switch(config)# ap group test
Switch(config-apgroup)# wlan test-wlan
Switch(config-wlan-apgroup)# no radio-policy dot11bg
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.
wlan shutdown	Disables a WLAN.

roamed-voice-client re-anchor

To enable the roamed-voice-client re-anchor feature, use the **roamed-voice-client re-anchor** command. To disable the roamed-voice-client re-anchor feature, use the **no** form of this command.

roamed-voice-client re-anchor

no roamed-voice-client re-anchor

Syntax Description

This command has no keywords or arguments.

Command Default

Roamed voice client reanchor feature is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to enable the roamed voice client re-anchor feature:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# roamed-voice-client re-anchor
```

This example shows how to disable the roamed voice client re-anchor feature:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no roamed-voice-client re-anchor
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

security ft

To configure 802.11r fast transition parameters, use the **security ft** command. To configure fast transition **over the air**, use the **no security ft over-the-ds** command.

security ft [**over-the-ds**| **reassociation-timeout** *timeout-jn-seconds*]

no security ft [**over-the-ds**| **reassociation-timeout**]

Syntax Description

over-the-ds	(Optional) Specifies that the 802.11r fast transition occurs over a distributed system. The no form of the command with this parameter configures security ft over the air.
reassociation-timeout	(Optional) Configures the reassociation timeout interval.
timeout-in-seconds	(Optional) Specifies the reassociation timeout interval in seconds. The valid range is between 1 to 100. The default value is 20.

Command Default

The feature is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

None

WLAN Security must be enabled.

Examples

The following example configures security FT configuration for an open WLAN:

```
Switch#wlan test
Switch(config-wlan)# client vlan 0140
Switch(config-wlan)# no mobility anchor sticky
Switch(config-wlan)# no security wpa
Switch(config-wlan)# no security wpa akm dot1x
Switch(config-wlan)# no security wpa wpa2
Switch(config-wlan)# no security wpa wpa2 ciphers aes
Switch(config-wlan)# security ft
Switch(config-wlan)# shutdown
```

The following example shows a sample security FT on a WPA-enabled WLAN:

```
Switch# wlan test
```

```
Switch(config-wlan)# client vlan 0140
Switch(config-wlan)# no security wpa akm dot1x
Switch(config-wlan)# security wpa akm ft psk
Switch(config-wlan)# security wpa akm psk set-key ascii 0 test-test
Switch(config-wlan)# security ft
Switch(config-wlan)# no shutdown
```

security pmf

To configure 802.11w Management Frame Protection (PMF) on a WLAN, use the **security pmf** command. To disable management frame protection, use the **no** form of the command.

security pmf {**association-comeback** *association-comeback-time-seconds*| **mandatory**| **optional**| **saquery-retry-time** *saquery-retry-time-milliseconds*}

no security pmf [**association-comeback** *association-comeback-time-seconds*| **mandatory**| **optional**| **saquery-retry-time** *saquery-retry-time-milliseconds*]

Syntax Description

association-comeback	Configures the 802.11w association comeback time.
association-comeback-time-seconds	Association comeback interval in seconds. Time interval that an associated client must wait before the association is tried again after it is denied with a status code 30. The status code 30 message is "Association request rejected temporarily; Try again later." The range is from 1 through 20 seconds.
mandatory	Specifies that clients are required to negotiate 802.1w PMF protection on the WLAN.
optional	Specifies that the WLAN does not mandate 802.11w support on clients. Clients with no 802.11w capability can also join.
saquery-retry-time	Time interval identified before which the SA query response is expected. If the switch does not get a response, another SA query is tried.
saquery-retry-time-milliseconds	The saquery retry time in milliseconds. The range is from 100 to 500 ms. The value must be specified in multiples of 100 milliseconds.

Command Default

PMF is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

You must have WPA (Wi-Fi Protected Access) and AKM (Authentication Key Management) configured to use this feature. See Related Command section for more information on configuring the security parameters.

802.11w introduces an Integrity Group Temporal Key (IGTK) that is used to protect broadcast or multicast robust management frames. IGTK is a random value, assigned by the authenticator station (switch) used to protect MAC management protocol data units (MMPDUs) from the source STA. The 802.11w IGTK key is derived using the four-way handshake and is used only on WLANs that are configured with WPA2 security at Layer 2.

Examples

This example shows how to enable the association comeback value at 15 seconds.

```
Switch(config-wlan)# security pmf association-comeback 15
```

This example shows how to configure mandatory 802.11w MPF protection for clients on a WLAN:

```
Switch(config-wlan)# security pmf mandatory
```

This example shows how to configure optional 802.11w MPF protection for clients on a WLAN:

```
Switch(config-wlan)# security pmf optional
```

This example shows how to configure the saquery parameter:

```
Switch(config-wlan)# security pmf saquery-retry-time 100
```

This example shows how to disable the PMF feature:

```
Switch(config-wlan)# no security pmf
```

Related Commands

Command	Description
security wpa akm	Configures authentication key-management using Cisco Centralized Key Management on a WLAN.

security web-auth

To change the status of web authentication used on a WLAN, use the **security web-auth** command. To disable web authentication on a WLAN, use the **no** form of the command.

security web-auth [**authentication-list** *authentication-list-name*| **on-macfilter-failure**| **parameter-map** *parameter-map-name*]

no security web-auth [**authentication-list [authentication-list-name]**| **on-macfilter-failure**| **parameter-map [parameter-name]**]

Syntax Description

authentication-list *authentication-list-name*	Sets the authentication list for IEEE 802.1x.
on-macfilter-failure	Enables web authentication on MAC failure.
parameter-map *parameter-map-name*	Configures the parameter map.

Command Default

Web authentication is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following example shows how to configure the authentication-list web authentication on a WLAN:

```
Switch(config-wlan)# security web-auth authentication-list test
```

security wpa akm

To configure authentication key management using Cisco Centralized Key Management (CCKM), use the **security wpa akm** command. To disable the authentication key management for Cisco Centralized Key Management, use the **no** form of the command.

security wpa [**akm** {**cckm**| **dot1x**| **ft**| **pmf**| **psk**}| **wpa1** [**ciphers** {**aes**| **tkip**}]| **wpa2** [**ciphers** {**aes**| **tikp**}]]

no security wpa [**akm** {**cckm**| **dot1x**| **ft**| **pmf**| **psk**}| **wpa1** [**ciphers** {**aes**| **tkip**}]| **wpa2** [**ciphers** {**aes**| **tikp**}]]

Syntax Description

akm	Configures the Authentication Key Management (AKM) parameters.
aes	Configures AES (Advanced Encryption Standard) encryption support.
cckm	Configures Cisco Centralized Key Management support.
ciphers	Configures WPA ciphers.
dot1x	Configures 802.1x support.
ft	Configures fast transition using 802.11r.
pmf	Configures 802.11w management frame protection.
psk	Configures 802.11r fast transition pre-shared key (PSK) support.
tkip	Configures Temporal Key Integrity Protocol (TKIP) encryption support.
wpa2	Configures Wi-Fi Protected Access 2 (WPA2) support.

Command Default

By default Wi-Fi Protected Access2, 802.1x are enabled. WPA2, PSK, CCKM, FT dot1x, FT PSK, PMF dot1x, PMF PSK, FT Support are disabled. The FT Reassociation timeout is set to 20 seconds, PMF SA Query time is set to 200.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Examples

The following example shows how to configure CCKM on the WLAN.

```
Switch(config-wlan)#security wpa akm cckm
```

service-policy (WLAN)

To configure the WLAN quality of service (QoS) service policy, use the **service-policy** command. To disable a QoS policy on a WLAN, use the **no** form of this command.

service-policy [client] {**input**| **output**} *policy-name*

no service-policy [client] {**input**| **output**} *policy-name*

Syntax Description

client	(Optional) Assigns a policy map to all clients in the WLAN.
input	Assigns an input policy map.
output	Assigns an output policy map.
policy-name	The policy name.

Command Default

No policies are assigned and the state assigned to the policy is None.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to configure the input QoS service policy on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# service-policy input policy-test
```

This example shows how to disable the input QoS service policy on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no service-policy input policy-test
```

This example shows how to configure the output QoS service policy on a WLAN to platinum (precious metal policy):

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Switch(config)# wlan wlan1
Switch(config-wlan)# service-policy output platinum
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

session-timeout

To configure session timeout for clients associated to a WLAN, use the **session-timeout** command. To disable a session timeout for clients that are associated to a WLAN, use the **no** form of this command.

session-timeout seconds

no session-timeout

Syntax Description

seconds	Timeout or session duration in seconds. A value of zero (0) is equivalent to no timeout. The range is from 300 to 86400.

Command Default

The client timeout is set to 1800 seconds for WLANs that are configured with dot1x security. The client timeout is set to 0 for open WLANs.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure a session timeout to 300 seconds:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# session-timeout 300
```

This example shows how to disable a session timeout:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no session-timeout
```

show wlan

To view WLAN parameters, use the **show wlan** command.

show wlan {**all** | **id** *wlan-id*| **name** *wlan-name* | **summary**}

Syntax Description

all	Displays a summary of parameters of all configured WLANs. The list is ordered by the ascending order of the WLAN IDs.
id *wlan-id*	Specifies the wireless LAN identifier. The range is from 1 to 512.
name *wlan-name*	Specifies the WLAN profile name. The name is from 1 to 32 characters.
summary	Displays a summary of the parameters configured on a WLAN.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display a summary of the WLANs configured on the device:

```
Switch# show wlan summary
Number of WLANs: 1

WLAN Profile Name                    SSID                           VLAN Status
-------------------------------------------------------------------------------
45   test-wlan                       test-wlan-ssid                  1    UP
```

This example shows how to display a summary of parameters configured on a particular WLAN:

```
Switch# show wlan name test-wlan
WLAN Identifier                               : 45
Profile Name                                  : test-wlan
Network Name (SSID)                           : test-wlan-ssid
Status                                        : Enabled
Broadcast SSID                                : Enabled
Maximum number of Associated Clients          : 0
AAA Policy Override                           : Disabled
Network Admission Control
  NAC-State                                   : Disabled
Number of Active Clients                      : 0
Exclusionlist Timeout                         : 60
```

```
Session Timeout                                 : 1800 seconds
CHD per WLAN                                    : Enabled
Webauth DHCP exclusion                          : Disabled
Interface                                       : default
Interface Status                                : Up
Multicast Interface                             : test
WLAN IPv4 ACL                                   : test
WLAN IPv6 ACL                                   : unconfigured
DHCP Server                                     : Default
DHCP Address Assignment Required                : Disabled
DHCP Option 82                                  : Disabled
DHCP Option 82 Format                           : ap-mac
DHCP Option 82 Ascii Mode                       : Disabled
DHCP Option 82 Rid Mode                         : Disabled
QoS Service Policy - Input
  Policy Name                                   : unknown
  Policy State                                  : None
QoS Service Policy - Output
  Policy Name                                   : unknown
  Policy State                                  : None
QoS Client Service Policy
  Input  Policy Name                            : unknown
  Output Policy Name                            : unknown
WifiDirect                                      : Disabled
WMM                                             : Disabled
Channel Scan Defer Priority:
  Priority (default)                            : 4
  Priority (default)                            : 5
  Priority (default)                            : 6
Scan Defer Time (msecs)                         : 100
Media Stream Multicast-direct                   : Disabled
CCX - AironetIe Support                         : Enabled
CCX - Gratuitous ProbeResponse (GPR)            : Disabled
CCX - Diagnostics Channel Capability            : Disabled
Dot11-Phone Mode (7920)                         : Invalid
Wired Protocol                                  : None
Peer-to-Peer Blocking Action                    : Disabled
Radio Policy                                    : All
DTIM period for 802.11a radio                   : 1
DTIM period for 802.11b radio                   : 1
Local EAP Authentication                        : Disabled
Mac Filter Authorization list name              : Disabled
Accounting list name                            : Disabled
802.1x authentication list name                 : Disabled
Security
    802.11 Authentication                       : Open System
    Static WEP Keys                             : Disabled
    802.1X                                      : Disabled
    Wi-Fi Protected Access (WPA/WPA2)           : Enabled
        WPA (SSN IE)                            : Disabled
        WPA2 (RSN IE)                           : Enabled
            TKIP Cipher                         : Disabled
            AES Cipher                          : Enabled
        Auth Key Management
            802.1x                              : Enabled
            PSK                                 : Disabled
            CCKM                                : Disabled
    IP Security                                 : Disabled
    IP Security Passthru                        : Disabled
    L2TP                                        : Disabled
    Web Based Authentication                    : Disabled
    Conditional Web Redirect                    : Disabled
    Splash-Page Web Redirect                    : Disabled
    Auto Anchor                                 : Disabled
    Sticky Anchoring                            : Enabled
    Cranite Passthru                            : Disabled
    Fortress Passthru                           : Disabled
    PPTP                                        : Disabled
    Infrastructure MFP protection               : Enabled
    Client MFP                                  : Optional
    Webauth On-mac-filter Failure               : Disabled
    Webauth Authentication List Name            : Disabled
    Webauth Parameter Map                       : Disabled
```

```
    Tkip MIC Countermeasure Hold-down Timer    : 60
Call Snooping                                  : Disabled
Passive Client                                 : Disabled
Non Cisco WGB                                  : Disabled
Band Select                                    : Disabled
Load Balancing                                 : Disabled
IP Source Guard                                : Disabled
Netflow Monitor                                : test
        Direction                              : Input
        Traffic                                : Datalink

Mobility Anchor List
IP Address
-----------
```

shutdown

To disable a WLAN, use the **shutdown** command. To enable a WLAN, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to disable a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan test-wlan
Switch(config-wlan)# shutdown
Switch(config-wlan)# end
Switch# show wlan summary
Number of WLANs: 1

WLAN Profile Name                     SSID                           VLAN Status
-------------------------------------------------------------------------------
45   test-wlan                         test-wlan-ssid                   1    DOWN
```

This example shows how to enable a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan test-wlan
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
Switch# show wlan summary
Number of WLANs: 1

WLAN Profile Name                     SSID                           VLAN Status
-------------------------------------------------------------------------------
45   test-wlan                         test-wlan-ssid                   1    UP
```

sip-cac

To configure the Session Initiation Protocol (SIP) Call Admission Control (CAC) feature on a WLAN, use the **sip-cac** command. To disable the SIP CAC feature, use the **no** form of this command.

sip-cac {**disassoc-client**| **send-486busy**}

no sip-cac {**disassoc-client**| **send-486busy**}

Syntax Description

disassoc-client	Enables a client disassociation if a CAC failure occurs.
send-486busy	Sends a SIP 486 busy message if a CAC failure occurs.

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to enable a client disassociation and 486 busy message on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# sip-cac disassoc-client
Switch(config-wlan)# sip-cac send-486busy
```

This example shows how to disable a client association and 486 busy message on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no sip-cac disassoc-client
Switch(config-wlan)# no sip-cac send-486busy
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

static-ip tunneling

To enable static IP tunneling on a WLAN, use the **static-ip tunneling** command. To disable the static IP tunneling feature, use the **no** form of this command.

static-ip tunneling

no static-ip tunneling

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable static-IP tunneling:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# static-ip tunneling
```

This example shows how to disable static-IP tunneling:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no static-ip tunneling
```

vlan

To assign a VLAN to an AP group, use the **vlan** command. To remove a VLAN ID, use the **no** form of this command.

vlan *interface-name*

no vlan

Syntax Description

interface-name	VLAN interface name.

Command Default

No VALN is assigned to the AP group. See Related Commands section for more information on how to disable a WLAN.

Command Modes

WLAN AP Group configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to configure a VLAN on an AP group:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ap group ap-group-1
Switch(config-apgroup)# wlan test-wlan
Switch(config-wlan-apgroup)# vlan 3
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

wgb non-cisco

To enable non-Cisco Workgroup Bridges (WGB) clients on the WLAN, use the **wgb non-cisco** command. To disable support for non-Cisco WGB clients, use the **no** form of this command.

wgb non-cisco

no wgb non-cisco

Syntax Description

This command has no keywords or arguments.

Command Default

Non-Cisco WGB clients are disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to enable non-Cisco WGBs on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
Switch(config-wlan)# wgb non-cisco
Switch(config-wlan)# no shutdown
```

This example shows how to disable support for non-Cisco WGB clients on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
Switch(config-wlan)# no wgb non-cisco
Switch(config-wlan)# no shutdown
```

wifidirect policy

To configure Wi-Fi Direct client policy on a WLAN, use the **wifidirect policy** command. To disable Wi-Fi Direct Client policy, use the **no** form of the command.

wifidirect policy {**permit**| **deny**}

Syntax Description

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 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.

Command Default

Wi-Fi Direct is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Examples

The following example shows how to enable Wi-Fi Direct and configure the Wi-Fi Direct clients to associate with the WLAN:

```
Switch(config-wlan)# wifidirect policy permit
```

wlan (AP Group Configuration)

To configure WLAN parameters of a WLAN in an access point (AP) group, use the **wlan** command. To remove a WLAN from the AP group, use the **no** form of this command.

wlan *wlan-name*

no wlan *wlan-name*

Syntax Description

wlan-name	WLAN profile name. The range is from 1 to 32 alphanumeric characters.

Command Default

WLAN parameters are not configured for an AP group.

Command Modes

AP Group configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to configure WLAN related parameters in the AP group configuration mode:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ap group test
Switch(config-apgroup)# wlan qos-wlan
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

wlan

To create a wireless LAN, use the **wlan** command. To disable a wireless LAN, use the **no** form of this command.

wlan [*wlan-name*| *wlan-name wlan-id*| *wlan-name wlan-id wlan-ssid*]

no wlan [*wlan-name*| *wlan-name wlan-id*| *wlan-name wlan-id wlan-ssid*]

Syntax Description

wlan-name	WLAN profile name. The name is from 1 to 32 alphanumeric characters.
wlan-id	Wireless LAN identifier. The range is from 1 to 512.
wlan-ssid	SSID. The range is from 1 to 32 alphanumeric characters.

Command Default

WLAN is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If you do not specify an SSID, the profile name parameter is used for both the profile name and the SSID. If the management and AP-manager interfaces are mapped to the same port and are members of the same VLAN, you must disable the WLAN before making a port-mapping change to either interface. If the management and AP-manager (Access Point Manager) interfaces are assigned to different VLANs, you do not need to disable the WLAN.

An error message appears if you try to delete a WLAN that is assigned to an access point group. If you proceed, the WLAN is removed from the access point group and from the access point's radio.

Examples

This example shows how to create a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config)# wlan test-wlan-cr 67 test-wlan-cr-ssid
```

This example shows how to delete a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config)# no wlan test-wlan-cr 67 test-wlan-cr-ssid
```

wlan shutdown

To disable a WLAN, use the **wlan shutdown** command. To enable a WLAN, use the **no** form of this command.

wlan shutdown

no wlan shutdown

Command Default

The WLAN is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to shut down a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

wmm

To enable Wi-Fi Multimedia (WMM) on a WLAN, use the **wmm** command. To disable WMM on a WLAN, use the **no** form of this command.

wmm {**allowed**| **require**}

no wmm

Syntax Description

allowed	Allows WMM on a WLAN.
require	Mandates that clients use WMM on the WLAN.

Command Default

WMM is enabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When the switch is in Layer 2 mode and WMM is enabled, you must put the access points on a trunk port in order to allow them to join the switch.

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to enable WMM on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# wmm allowed
```

This example shows how to disable WMM on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no wmm
```

Related Commands

Command	Description
wlan	Creates or disables a WLAN.

INDEX

A

aaa-override command 15
accounting-list command 16
assisted-roaming command 17

B

band-select command 19
broadcast-ssid command 20

C

call-snoop command 21
ccx aironet-iesupport command 29
channel-scan defer-priority command 23
channel-scan defer-time command 24
chd command 25
client association limit command 26
client vlan command 28

D

datalink flow monitor command 30
default command 33
device-classification command 32
dtim dot11 command 36

E

exclusionlist command 37
exit command 38, 39

I

ip access-group command 40
ip flow monitor command 41
ip verify source mac-check command 42

L

load-balance command 43

M

mobility anchor 44

N

nac command 46

P

passive-client command 47
peer-blocking command 48

R

radio command 49
radio-policy command 51
roamed-voice-client re-anchor command 53

S

security web-auth command 58
service-policy command 61
session-timeout command 63
show wlan command 64
shutdown command 67
sip-cac command 68
static-ip tunneling command 69

V

vlan command 70

W

wgb non-cisco command 71
wlan command 73, 74
wlan shutdown command 75
wmm command 76