



## **Security Command Reference, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)**

**First Published:** May 26, 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-32328-01

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 ix

Audience ix

Changes to This Document ix

Document Conventions ix

Related Documentation xi

Obtaining Documentation and Submitting a Service Request xii

---

### CHAPTER 1

#### Using the Command-Line Interface 1

Information About Using the Command-Line Interface 1

Command Modes 1

Understanding Abbreviated Commands 3

No and Default Forms of Commands 4

CLI Error Messages 4

Configuration Logging 4

Using the Help System 5

How to Use the CLI to Configure Features 6

Configuring the Command History 6

Changing the Command History Buffer Size 6

Recalling Commands 7

Disabling the Command History Feature 7

Enabling and Disabling Editing Features 8

Editing Commands Through Keystrokes 9

Editing Command Lines That Wrap 10

Searching and Filtering Output of show and more Commands 11

Accessing the CLI Through a Console Connection or Through Telnet 12

---

### CHAPTER 2

#### Security Commands 13

aaa accounting dot1x	17
aaa accounting identity	19
aaa authentication dot1x	21
aaa authentication login	22
aaa authorization credential download default	23
aaa authorization network	24
aaa group server radius	25
access session passthru-access-group	26
address ipv4 auth-port acct-port	27
ap dtls secure-cipher	28
ap name fips key-zeroize	29
authentication host-mode	30
authentication mac-move permit	32
authentication priority	33
authentication violation	36
banner	38
cisp enable	40
clear errdisable interface vlan	42
clear mac address-table	44
consent email	46
deny (MAC access-list configuration)	47
device-role (IPv6 snooping)	51
device-role (IPv6 nd inspection)	52
dot1x critical (global configuration)	53
dot1x pae	54
dot1x supplicant force-multicast	55
dot1x test eapol-capable	56
dot1x test timeout	57
dot1x timeout	58
epm access-control open	61
fips authorization-key	62
fips log-dtls-replay	63
fips zeroize	64
ip admission	65
ip admission name	66

ip device tracking maximum	69
ip device tracking probe	70
ip dhcp snooping database	71
ip dhcp snooping information option format remote-id	73
ip dhcp snooping verify no-relay-agent-address	74
ip dhcp snooping wireless bootp-broadcast enable	75
ip source binding	76
ip verify source	77
ipv6 snooping policy	79
key ww-wireless	81
limit address-count	82
login-auth-bypass	83
mab request format attribute 32	84
match (access-map configuration)	86
map-index map	88
no authentication logging verbose	89
no dot1x logging verbose	90
no mab logging verbose	91
parameter-map type subscriber attribute-to-service	92
parameter map type webauth	93
passthrou-domain-list name	95
permit (MAC access-list configuration)	96
policy-map type control subscriber	100
protocol (IPv6 snooping)	102
radius server	103
security level (IPv6 snooping)	104
security web-auth	105
service-policy type control subscriber	106
service-template	107
session-timeout	108
show aaa clients	109
show aaa command handler	110
show aaa local	111
show aaa servers	113
show aaa sessions	114

show access-session	115
show access-session fqdn	117
show access session interface	118
show device classifier attached detail	119
show authentication sessions	120
show cisp	123
show dot1x	125
show eap pac peer	127
show fips authorization-key	128
show fips status	129
show ip dhcp snooping statistics	130
show nmsp	133
show radius server-group	135
show vlan access-map	137
show vlan group	138
show wireless wps rogue ap summary	139
show wireless wps rogue client detailed	140
show wireless wps rogue client summary	141
show wireless wps wips statistics	142
show wireless wps wips summary	143
tracking (IPv6 snooping)	144
trusted-port	146
virtual-ip	147
wireless mobility dtls secure-cipher	148
wireless security dot1x	149
wireless security dot1x radius accounting mac-delimiter	151
wireless security dot1x radius mac-authentication mac-delimiter	152
wireless security certificate force-sha1-cert	153
wireless security dot1x radius callStationIdCase	154
wireless security web-auth retries	155
wireless dot11-padding	156
wireless wlancc	157
wireless wps rogue ap valid-client	158
wireless wps rogue client	159
wireless wps rogue rule	160

wireless wps rogue detection **162**  
vlan access-map **163**  
vlan filter **165**  
vlan group **167**







## Preface

---

This book describes command reference information and examples for security on the Catalyst 3850 switch.

- [Audience, page ix](#)
- [Changes to This Document, page ix](#)
- [Document Conventions, page ix](#)
- [Related Documentation, page xi](#)
- [Obtaining Documentation and Submitting a Service Request, page xii](#)

## Audience

This guide is for the networking professional managing the Catalyst 3850 switch, hereafter referred to as the switch module. Before using this guide, you should have experience working with the Cisco IOS software and be familiar with the concepts and terminology of Ethernet and local area networking.

## Changes to This Document

This table lists the technical changes made to this document since it was first printed.

Revision	Date	Change Summary
OL-26847-01	January 2013	Initial release of this document.

## 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 <b>^D</b> or <b>Ctrl-D</b> 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.)
<b>bold font</b>	Commands and keywords and user-entered text appear in <b>bold font</b> .
<i>Italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
Courier font	Terminal sessions and information the system displays appear in <code>courier font</code> .
<b>Bold Courier font</b>	<b>Bold Courier</b> 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.
{x   y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y   z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
<>	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

### Reader Alert Conventions

This document may use the following conventions for reader alerts:

**Note**

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

**Tip**

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

**Caution**

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

**Timesaver**

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

**Warning****IMPORTANT SAFETY INSTRUCTIONS**

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

SAVE THESE INSTRUCTIONS

## Related Documentation

**Note**

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

- Cisco 5700 Series Wireless Controller documentation, located at:  
[http://www.cisco.com/go/wlc5700\\_sw](http://www.cisco.com/go/wlc5700_sw)
- *Cisco 5700 Series Wireless Controller Installation Guide and Regulatory Compliance and Safety Information for the Cisco 5700 Series Wireless Controller*, located at:  
[http://www.cisco.com/go/wlc5700\\_hw](http://www.cisco.com/go/wlc5700_hw)
- Cisco Validated Designs documents, located at:  
<http://www.cisco.com/go/designzone>

# 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, an SSH, or by using the browser.

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

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

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

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

**Table 1: Command Mode Summary**

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session using Telnet, SSH, or console.	Controller>	Enter <b>logout</b> or <b>quit</b> .	Use this mode to <ul style="list-style-type: none"> <li>• Change terminal settings.</li> <li>• Perform basic tests.</li> <li>• Display system information.</li> </ul>
Privileged EXEC	While in user EXEC mode, enter the <b>enable</b> command.	Controller#	Enter <b>disable</b> to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.  Use this mode to execute privilege EXEC commands for access points. These commands are not part of the running config of the controller, they are sent to the IOS config of the access point.
Global configuration	While in privileged EXEC mode, enter the <b>configure</b> command.	Controller(config)#	To exit to privileged EXEC mode, enter <b>exit</b> or <b>end</b> , or press <b>Ctrl-Z</b> .	Use this mode to configure parameters that apply to the entire controller.  Use this mode to configure access point commands that are part of the running config of the controller.
VLAN configuration	While in global configuration mode, enter the <b>vlan <i>vlan-id</i></b> command.	Controller(config-vlan)#		

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

## Understanding Abbreviated Commands

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

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

```
Controller# show conf
```

## No and Default Forms of Commands

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

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

## CLI Error Messages

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

**Table 2: Common CLI Error Messages**

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

## Configuration Logging

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



notification to registered applications whenever the configuration changes. You can choose to have the notifications sent to the syslog.

**Note**

Only CLI or HTTP changes are logged.

## 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
<b>Step 1</b>	<b>help</b>  <b>Example:</b> Controller# <b>help</b>	Obtains a brief description of the help system in any command mode.
<b>Step 2</b>	<i>abbreviated-command-entry</i> ?  <b>Example:</b> Controller# <b>di</b> ? dir disable disconnect	Obtains a list of commands that begin with a particular character string.
<b>Step 3</b>	<i>abbreviated-command-entry</i> <Tab>  <b>Example:</b> Controller# <b>sh conf</b> <tab> Controller# <b>show configuration</b>	Completes a partial command name.
<b>Step 4</b>	<b>?</b>  <b>Example:</b> Controller> ?	Lists all commands available for a particular command mode.

	Command or Action	Purpose
<b>Step 5</b>	<p><i>command ?</i></p> <p><b>Example:</b> Controller&gt; <b>show ?</b></p>	Lists the associated keywords for a command.
<b>Step 6</b>	<p><i>command keyword ?</i></p> <p><b>Example:</b> Controller(config)# <b>cdp holdtime ?</b> &lt;10-255&gt; Length of time (in sec) that receiver must keep this packet</p>	Lists the associated arguments for a keyword.

# How to Use the CLI to Configure Features

## Configuring the Command History

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

### Changing the Command History Buffer Size

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

#### SUMMARY STEPS

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

#### DETAILED STEPS

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

## Recalling Commands

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

**Note**

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

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>Ctrl-P</b> or use the <b>up arrow</b> key	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
<b>Step 2</b>	<b>Ctrl-N</b> or use the <b>down arrow</b> key	Returns to more recent commands in the history buffer after recalling commands with <b>Ctrl-P</b> or the up arrow key. Repeat the key sequence to recall successively more recent commands.
<b>Step 3</b>	<b>show history</b>  <b>Example:</b> Controller# <b>show history</b>	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 <b>terminal history</b> global configuration command and the <b>history</b> 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
<b>Step 1</b>	<b>terminal no history</b>  <b>Example:</b> Controller# <b>terminal no history</b>	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
<b>Step 1</b>	<b>terminal editing</b>  <b>Example:</b> Controller# <b>terminal editing</b>	Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.
<b>Step 2</b>	<b>terminal no editing</b>  <b>Example:</b> Controller# <b>terminal no editing</b>	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
<b>Ctrl-B</b> or use the <b>left arrow</b> key	Moves the cursor back one character.
<b>Ctrl-F</b> or use the <b>right arrow</b> key	Moves the cursor forward one character.
<b>Ctrl-A</b>	Moves the cursor to the beginning of the command line.
<b>Ctrl-E</b>	Moves the cursor to the end of the command line.
<b>Esc B</b>	Moves the cursor back one word.
<b>Esc F</b>	Moves the cursor forward one word.
<b>Ctrl-T</b>	Transposes the character to the left of the cursor with the character located at the cursor.
<b>Delete</b> or <b>Backspace</b> key	Erases the character to the left of the cursor.
<b>Ctrl-D</b>	Deletes the character at the cursor.
<b>Ctrl-K</b>	Deletes all characters from the cursor to the end of the command line.
<b>Ctrl-U</b> or <b>Ctrl-X</b>	Deletes all characters from the cursor to the beginning of the command line.
<b>Ctrl-W</b>	Deletes the word to the left of the cursor.
<b>Esc D</b>	Deletes from the cursor to the end of the word.
<b>Esc C</b>	Capitalizes at the cursor.
<b>Esc L</b>	Changes the word at the cursor to lowercase.
<b>Esc U</b>	Capitalizes letters from the cursor to the end of the word.

<b>Ctrl-V</b> or <b>Esc Q</b>	Designates a particular keystroke as an executable command, perhaps as a shortcut.
<b>Return</b> key	<p>Scrolls down a line or screen on displays that are longer than the terminal screen can display.</p> <p><b>Note</b> The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including <b>show</b> command output. You can use the <b>Return</b> and <b>Space</b> bar keystrokes whenever you see the More prompt.</p>
<b>Space</b> bar	Scrolls down one screen.
<b>Ctrl-L</b> or <b>Ctrl-R</b>	Redisplays the current command line if the controller suddenly sends a message to your screen.

## Editing Command Lines That Wrap

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

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



### Note

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

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

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>access-list</b>  <b>Example:</b> <code>Controller(config)# access-list 101 permit</code>	<p>Displays the global configuration command entry that extends beyond one line.</p> <p>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</p>

	Command or Action	Purpose
	<pre> tcp 10.15.22.25 255.255.255.0 10.15.22.35 Controller(config)# \$ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25 Controller(config)# \$t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq Controller(config)# \$15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45 </pre>	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	<b>Ctrl-A</b>  <b>Example:</b> <pre> Controller(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2\$ </pre>	<p>Checks the complete syntax.</p> <p>The dollar sign (\$) appears at the end of the line to show that the line has been scrolled to the right.</p>
Step 3	<b>Return key</b>	<p>Execute the commands.</p> <p>The software assumes that you have a terminal screen that is 80 columns wide. If you have a different width, use the <b>terminal width</b> privileged EXEC command to set the width of your terminal.</p> <p>Use line wrapping with the command history feature to recall and modify previous complex command entries.</p>

## 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	<pre> {show   more} command   {begin   include   exclude} regular-expression </pre> <b>Example:</b> <pre> Controller# show interfaces   include protocol Vlan1 is up, line protocol is up Vlan10 is up, line protocol is down GigabitEthernet1/0/1 is up, line protocol is down GigabitEthernet1/0/2 is up, line protocol is up </pre>	<p>Searches and filters the output.</p> <p>Expressions are case sensitive. For example, if you enter <b>  exclude output</b>, the lines that contain <b>output</b> are not displayed, but the lines that contain <b>output</b> appear.</p>

## Accessing the CLI Through a Console Connection or Through Telnet

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

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

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

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

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





## Security Commands

---

- [aaa accounting dot1x, page 17](#)
- [aaa accounting identity, page 19](#)
- [aaa authentication dot1x, page 21](#)
- [aaa authentication login, page 22](#)
- [aaa authorization credential download default, page 23](#)
- [aaa authorization network, page 24](#)
- [aaa group server radius, page 25](#)
- [access session passthru-access-group, page 26](#)
- [address ipv4 auth-port acct-port, page 27](#)
- [ap dtls secure-cipher, page 28](#)
- [ap name fips key-zeroize, page 29](#)
- [authentication host-mode, page 30](#)
- [authentication mac-move permit, page 32](#)
- [authentication priority, page 33](#)
- [authentication violation, page 36](#)
- [banner, page 38](#)
- [cisp enable, page 40](#)
- [clear errdisable interface vlan, page 42](#)
- [clear mac address-table, page 44](#)
- [consent email, page 46](#)
- [deny \(MAC access-list configuration\), page 47](#)
- [device-role \(IPv6 snooping\), page 51](#)
- [device-role \(IPv6 nd inspection\), page 52](#)
- [dot1x critical \(global configuration\), page 53](#)

- [dot1x pae, page 54](#)
- [dot1x supplicant force-multicast, page 55](#)
- [dot1x test eapol-capable, page 56](#)
- [dot1x test timeout, page 57](#)
- [dot1x timeout, page 58](#)
- [epm access-control open, page 61](#)
- [fips authorization-key, page 62](#)
- [fips log-dtls-replay, page 63](#)
- [fips zeroize, page 64](#)
- [ip admission, page 65](#)
- [ip admission name, page 66](#)
- [ip device tracking maximum, page 69](#)
- [ip device tracking probe, page 70](#)
- [ip dhcp snooping database, page 71](#)
- [ip dhcp snooping information option format remote-id, page 73](#)
- [ip dhcp snooping verify no-relay-agent-address, page 74](#)
- [ip dhcp snooping wireless bootp-broadcast enable , page 75](#)
- [ip source binding, page 76](#)
- [ip verify source, page 77](#)
- [ipv6 snooping policy, page 79](#)
- [key ww-wireless, page 81](#)
- [limit address-count, page 82](#)
- [login-auth-bypass, page 83](#)
- [mab request format attribute 32, page 84](#)
- [match \(access-map configuration\), page 86](#)
- [map-index map, page 88](#)
- [no authentication logging verbose, page 89](#)
- [no dot1x logging verbose, page 90](#)
- [no mab logging verbose, page 91](#)
- [parameter-map type subscriber attribute-to-service, page 92](#)
- [parameter map type webauth, page 93](#)
- [passthrou-domain-list name, page 95](#)
- [permit \(MAC access-list configuration\), page 96](#)

- [policy-map type control subscriber, page 100](#)
- [protocol \(IPv6 snooping\), page 102](#)
- [radius server, page 103](#)
- [security level \(IPv6 snooping\), page 104](#)
- [security web-auth, page 105](#)
- [service-policy type control subscriber, page 106](#)
- [service-template, page 107](#)
- [session-timeout, page 108](#)
- [show aaa clients, page 109](#)
- [show aaa command handler, page 110](#)
- [show aaa local, page 111](#)
- [show aaa servers, page 113](#)
- [show aaa sessions, page 114](#)
- [show access-session, page 115](#)
- [show access-session fqdn, page 117](#)
- [show access session interface, page 118](#)
- [show device classifier attached detail, page 119](#)
- [show authentication sessions, page 120](#)
- [show cisp, page 123](#)
- [show dot1x, page 125](#)
- [show eap pac peer, page 127](#)
- [show fips authorization-key, page 128](#)
- [show fips status, page 129](#)
- [show ip dhcp snooping statistics, page 130](#)
- [show nmsp, page 133](#)
- [show radius server-group, page 135](#)
- [show vlan access-map, page 137](#)
- [show vlan group, page 138](#)
- [show wireless wps rogue ap summary , page 139](#)
- [show wireless wps rogue client detailed, page 140](#)
- [show wireless wps rogue client summary, page 141](#)
- [show wireless wps wips statistics, page 142](#)
- [show wireless wps wips summary, page 143](#)

- [tracking \(IPv6 snooping\), page 144](#)
- [trusted-port, page 146](#)
- [virtual-ip, page 147](#)
- [wireless mobility dtls secure-cipher, page 148](#)
- [wireless security dot1x, page 149](#)
- [wireless security dot1x radius accounting mac-delimiter, page 151](#)
- [wireless security dot1x radius mac-authentication mac-delimiter, page 152](#)
- [wireless security certificate force-sha1-cert, page 153](#)
- [wireless security dot1x radius callStationIdCase, page 154](#)
- [wireless security web-auth retries, page 155](#)
- [wireless dot11-padding, page 156](#)
- [wireless wlancc, page 157](#)
- [wireless wps rogue ap valid-client, page 158](#)
- [wireless wps rogue client, page 159](#)
- [wireless wps rogue rule, page 160](#)
- [wireless wps rogue detection, page 162](#)
- [vlan access-map, page 163](#)
- [vlan filter, page 165](#)
- [vlan group, page 167](#)

## aaa accounting dot1x

To enable authentication, authorization, and accounting (AAA) accounting and to create method lists defining specific accounting methods on a per-line or per-interface basis for IEEE 802.1x sessions, use the **aaa accounting dot1x** command in global configuration mode. To disable IEEE 802.1x accounting, use the **no** form of this command.

```
aaa accounting dot1x {name | default } start-stop {broadcast group {name | radius | tacacs+} [group {name | radius | tacacs+} ... ] | group {name | radius | tacacs+} [group {name | radius | tacacs+} ... ]}
no aaa accounting dot1x {name | default }
```

### Syntax Description

<b>name</b>	Name of a server group. This is optional when you enter it after the <b>broadcast group</b> and <b>group</b> keywords.
<b>default</b>	Specifies the accounting methods that follow as the default list for accounting services.
<b>start-stop</b>	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether or not the start accounting notice was received by the accounting server.
<b>broadcast</b>	Enables accounting records to be sent to multiple AAA servers and sends accounting records to the first server in each group. If the first server is unavailable, the switch uses the list of backup servers to identify the first server.
<b>group</b>	Specifies the server group to be used for accounting services. These are valid server group names: <ul style="list-style-type: none"> <li>• <b>name</b> — Name of a server group.</li> <li>• <b>radius</b> — Lists of all RADIUS hosts.</li> <li>• <b>tacacs+</b> — Lists of all TACACS+ hosts.</li> </ul> <p>The <b>group</b> keyword is optional when you enter it after the <b>broadcast group</b> and <b>group</b> keywords. You can enter more than optional <b>group</b> keyword.</p>
<b>radius</b>	(Optional) Enables RADIUS accounting.
<b>tacacs+</b>	(Optional) Enables TACACS+ accounting.

### Command Default

AAA accounting is disabled.

### Command Modes

Global configuration

### Command History

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

### Usage Guidelines

This command requires access to a RADIUS server.

We recommend that you enter the **dot1x reauthentication** interface configuration command before configuring IEEE 802.1x RADIUS accounting on an interface.

### Examples

This example shows how to configure IEEE 802.1x accounting:

```
Controller(config) # aaa new-model  
Controller(config) # aaa accounting dot1x default start-stop group radius
```

# aaa accounting identity

To enable authentication, authorization, and accounting (AAA) accounting for IEEE 802.1x, MAC authentication bypass (MAB), and web authentication sessions, use the **aaa accounting identity** command in global configuration mode. To disable IEEE 802.1x accounting, use the **no** form of this command.

**aaa accounting identity** {*name* | **default** } **start-stop** {**broadcast group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} ... ] | **group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**}... ]}

**no aaa accounting identity** {*name* | **default** }

## Syntax Description

<i>name</i>	Name of a server group. This is optional when you enter it after the <b>broadcast group</b> and <b>group</b> keywords.
<b>default</b>	Uses the accounting methods that follow as the default list for accounting services.
<b>start-stop</b>	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested-user process begins regardless of whether or not the start accounting notice was received by the accounting server.
<b>broadcast</b>	Enables accounting records to be sent to multiple AAA servers and send accounting records to the first server in each group. If the first server is unavailable, the switch uses the list of backup servers to identify the first server.
<b>group</b>	Specifies the server group to be used for accounting services. These are valid server group names: <ul style="list-style-type: none"> <li>• <i>name</i> — Name of a server group.</li> <li>• <b>radius</b> — Lists of all RADIUS hosts.</li> <li>• <b>tacacs+</b> — Lists of all TACACS+ hosts.</li> </ul> <p>The <b>group</b> keyword is optional when you enter it after the <b>broadcast group</b> and <b>group</b> keywords. You can enter more than optional <b>group</b> keyword.</p>
<b>radius</b>	(Optional) Enables RADIUS authorization.
<b>tacacs+</b>	(Optional) Enables TACACS+ accounting.

## Command Default

AAA accounting is disabled.

## Command Modes

Global configuration

**Command History**

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

**Usage Guidelines**

To enable AAA accounting identity, you need to enable policy mode. To enable policy mode, enter the **authentication display new-style** command in privileged EXEC mode.

**Examples**

This example shows how to configure IEEE 802.1x accounting identity:

```
Controller# authentication display new-style
```

Please note that while you can revert to legacy style configuration at any time unless you have explicitly entered new-style configuration, the following caveats should be carefully read and understood.

- (1) If you save the config in this mode, it will be written to NVRAM in NEW-style config, and if you subsequently reload the router without reverting to legacy config and saving that, you will no longer be able to revert.
- (2) In this and legacy mode, Webauth is not IPv6-capable. It will only become IPv6-capable once you have entered new-style config manually, or have reloaded with config saved in 'authentication display new' mode.

```
Controller# configure terminal
```

```
Controller(config)# aaa accounting identity default start-stop group radius
```



# aaa authentication dot1x

To specify the authentication, authorization, and accounting (AAA) method to use on ports complying with the IEEE 802.1x authentication, use the **aaa authentication dot1x** command in global configuration mode on the switch stack or on a standalone switch. To disable authentication, use the **no** form of this command.

**aaa authentication dot1x** {default} *method1*

**no aaa authentication dot1x** {default} *method1*

## Syntax Description

<b>default</b>	The default method when a user logs in. Use the listed authentication method that follows this argument.
<i>method1</i>	Specifies the server authentication. Enter the <b>group radius</b> keywords to use the list of all RADIUS servers for authentication.
<b>Note</b>	Though other keywords are visible in the command-line help strings, only the <b>default</b> and <b>group radius</b> keywords are supported.

## Command Default

No authentication is performed.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

The **method** argument identifies the method that the authentication algorithm tries in the specified sequence to validate the password provided by the client. The only method that is IEEE 802.1x-compliant is the **group radius** method, in which the client data is validated against a RADIUS authentication server.

If you specify **group radius**, you must configure the RADIUS server by entering the **radius-server host** global configuration command.

Use the **show running-config** privileged EXEC command to display the configured lists of authentication methods.

## Examples

This example shows how to enable AAA and how to create an IEEE 802.1x-compliant authentication list. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is not allowed access to the network.

```
Controller(config)# aaa new-model
Controller(config)# aaa authentication dot1x default group radius
```

# aaa authentication login

To set authentication, authorization, and accounting (AAA) authentication at login, use the **aaa authentication login** command in global configuration mode.

**aaa authentication login** *authentication-list-name* {**group** }*group-name*

## Syntax Description

<i>authentication-list-name</i>	Character string used to name the list of authentication methods activated when a user logs in.
<i>group</i>	Uses a subset of RADIUS servers for authentication as defined by the server group <b>group-name</b> .
<i>group-name</i>	Server group name.

## Command Default

None

## Command Modes

Global Configuration

## Command History

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

## Usage Guidelines

None

## Examples

The following example shows how to set an authentication method list named **local\_webauth** to the group type named **local** in local web authentication:

```
Controller(config)# aaa authentication login local_webauth local
```

The following example shows how to set an authentication method to RADIUS server group in local web authentication:

```
Controller(config)# aaa authentication login webauth_radius group ISE_group
```

## aaa authorization credential download default

To set an authorization method list to use local credentials, use the **aaa authorization credential download default** command in global configuration mode.

**aaa authorization credential download default** *group-name*

### Syntax Description

<i>group-name</i>	Server group name.
-------------------	--------------------

### Command Default

None

### Command Modes

Global Configuration

### Command History

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

### Examples

The following example shows how to set an authorization method list to use local credentials:

```
Controller(config)# aaa authorization credential-download default local
```

# aaa authorization network

To set authorization for all network-related service requests, use the **aaa authorization network** command in global configuration mode.

**aaa authorization network** *authorization-list-name* {**group** }*group-name*

## Syntax Description

<i>authorization-list-name</i>	Character string used to name the list of authorization methods activated when a user logs in.
<i>group</i>	Uses a subset of RADIUS servers for authentication as defined by the server group <b>group-name</b> .
<i>group-name</i>	Server group name.

## Command Modes

Global Configuration

## Command History

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

## Examples

The following example shows how to set an authorization method list to the RADIUS server group in local web authentication:

```
Controller(config)# aaa authorization network webauth_radius group ISE_group
```

## aaa group server radius

To group different RADIUS server hosts into distinct lists and distinct methods, use the **aaa group server radius** command in global configuration mode.

**aaa group server radius** *group-name*

Syntax Description	<i>group-name</i> Character string used to name the group of servers.
--------------------	---

Command Default	None
-----------------	------

Command Modes	Global configuration
---------------	----------------------

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

Usage Guidelines	<p>The authentication, authorization, and accounting (AAA) server-group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.</p> <p>A group server is a list of server hosts of a particular type. Currently supported server host types are RADIUS server hosts. A group server is used in conjunction with a global server host list. The group server lists the IP addresses of the selected server hosts.</p>
------------------	--

Examples	<p>The following example shows how to configure an AAA group server named <b>ISE_Group</b> that comprises three member servers:</p>
----------	---

```
Controller(config)# aaa group server radius ISE_Group
```

# access session passthru-access-group

To map the FQDN ACL with the domain name, use the

**access session passthru-access-group** *acl\_name* **passthru-domain-list** *domain\_name*

## Syntax Description

<i>acl_name</i>	Name of the FQDN ACL.
<b>passthru-domain-list</b> <i>domain_name</i>	Configures the domain name list to be mapped to the FQDN ACL.

## Command Default

No domain is mapped to an FQDN ACL.

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

## Examples

This example shows how to map the FQDN ACL with the domain name:

```
Controller(config)# access session passthru-access-group abc passthru-domain-list abc
```

# address ipv4 auth-port acct-port

To configure IPv4 address for a RADIUS server, use the **address ipv4 auth-port acct-port** command in global configuration mode.

**address ipv4** *ipv4-address***auth-port** *auth-port-number***acct-port** *acct-port-number*

## Syntax Description

<i>ipv4-address</i>	IPv4 address of a RADIUS server.
<i>auth-port-number</i>	UDP port to use for RADIUS authentication messages. The default UDP port is 1812. The range is from 0 to 65535.
<i>acct-port-number</i>	UDP port to use for RADIUS accounting messages. The default UDP port is 1812. The range is from 0 to 65535.

## Command Default

None

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

None

## Examples

The following example shows how to configure IPv4 address for a RADIUS server:

```
Controller(config)# radius server ISE
Controller(config-radius-server)# address ipv4 192.168.154.119 auth-port 1812 acct-port 1813
```

## ap dtls secure-cipher

To set AES256 SHA1 or AES256 SHA2 as cipher for CAPWAP control tunnels, use the **ap dtls secure-cipher** command in global configuration mode.

**ap dtls secure-cipher**{AES256\_SHA1| AES256\_SHA2}

### Command Default

None

### Command Modes

Global Configuration

### Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

### Examples

The following example shows how to set AES256 SHA1 as cipher for CAPWAP control tunnels on the controller:

```
Controller(config)# ap dtls secure-cipher AES256_SHA1
Enabling secure-cipher AES256_SHA1 will reset all AP CAPWAP DTLS connections
Are you sure you want to continue? (y/n)[y]: y
Controller(config)#
```



# ap name fips key-zeroize

To zeroize the specified AP, use the **ap name** *ap-name* **fips key-zeroize** command in in privileged EXEC mode.

**ap name** *ap-name* **fips key-zeroize**

## Command Default

None

## Command Modes

Privileged EXEC mode

## Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

## Usage Guidelines

This is done in extreme cases, where, in the process of deleting the keys, the configuration file and IOS image are also deleted from the AP.



### Caution

You must be careful before zeroizing the AP as after performing this operation, the AP becomes unusable.

## Examples

The following example shows how to zeroize the controller:

```
Controller(config)# ap name AP78da.6e59.a340 fips key-zeroize
**Critical Warning** - This command is irreversible
and will zeroize the FVPK by Deleting the IOS
image and config files, please use extreme
caution and confirm with Yes on each of three
iterations to complete. The system will reboot
after the command executes successfully
  Proceed ?? (yes/[no]): no
%Aborting zeroization!
```

# authentication host-mode

To set the authorization manager mode on a port, use the **authentication host-mode** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

**authentication host-mode** {**multi-auth** | **multi-domain** | **multi-host** | **single-host**}

**no authentication host-mode**

## Syntax Description

<b>multi-auth</b>	Enables multiple-authorization mode (multi-auth mode) on the port.
<b>multi-domain</b>	Enables multiple-domain mode on the port.
<b>multi-host</b>	Enables multiple-host mode on the port.
<b>single-host</b>	Enables single-host mode on the port.

## Command Default

Single host mode is enabled.

## Command Modes

Interface configuration

## Command History

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

## Usage Guidelines

Single-host mode should be configured if only one data host is connected. Do not connect a voice device to authenticate on a single-host port. Voice device authorization fails if no voice VLAN is configured on the port.

Multi-domain mode should be configured if data host is connected through an IP phone to the port. Multi-domain mode should be configured if the voice device needs to be authenticated.

Multi-auth mode should be configured to allow devices behind a hub to obtain secured port access through individual authentication. Only one voice device can be authenticated in this mode if a voice VLAN is configured.

Multi-host mode also offers port access for multiple hosts behind a hub, but multi-host mode gives unrestricted port access to the devices after the first user gets authenticated.

## Examples

This example shows how to enable multi-auth mode on a port:

```
Controller(config-if)# authentication host-mode multi-auth
```

This example shows how to enable multi-domain mode on a port:

```
Controller(config-if)# authentication host-mode multi-domain
```

This example shows how to enable multi-host mode on a port:

```
Controller(config-if)# authentication host-mode multi-host
```

This example shows how to enable single-host mode on a port:

```
Controller(config-if)# authentication host-mode single-host
```

You can verify your settings by entering the **show authentication sessions interface *interface* details** privileged EXEC command.

# authentication mac-move permit

To enable MAC move on a controller, use the **authentication mac-move permit** command in global configuration mode. To disable MAC move, use the **no** form of this command.

**authentication mac-move permit**

**no authentication mac-move permit**

**Syntax Description** This command has no arguments or keywords.

**Command Default** MAC move is enabled.

**Command Modes** Global configuration

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

**Usage Guidelines** The command enables authenticated hosts to move between ports on a controller. For example, if there is a device between an authenticated host and port, and that host moves to another port, the authentication session is deleted from the first port, and the host is reauthenticated on the new port.

If MAC move is disabled, and an authenticated host moves to another port, it is not reauthenticated, and a violation error occurs.

**Examples** This example shows how to enable MAC move on a controller:

```
Controller(config)# authentication mac-move permit
```

# authentication priority

To add an authentication method to the port-priority list, use the **authentication priority** command in interface configuration mode. To return to the default, use the **no** form of this command.

**authentication priority** [**dot1x** | **mab**] {**webauth**}

**no authentication priority** [**dot1x** | **mab**] {**webauth**}

## Syntax Description

<b>dot1x</b>	(Optional) Adds 802.1x to the order of authentication methods.
<b>mab</b>	(Optional) Adds MAC authentication bypass (MAB) to the order of authentication methods.
<b>webauth</b>	Adds web authentication to the order of authentication methods.

## Command Default

The default priority is 802.1x authentication, followed by MAC authentication bypass and web authentication.

## Command Modes

Interface configuration

## Command History

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

## Usage Guidelines

Ordering sets the order of methods that the switch attempts when trying to authenticate a new device is connected to a port.

When configuring multiple fallback methods on a port, set web authentication (webauth) last.

Assigning priorities to different authentication methods allows a higher-priority method to interrupt an in-progress authentication method with a lower priority.



### Note

If a client is already authenticated, it might be reauthenticated if an interruption from a higher-priority method occurs.

The default priority of an authentication method is equivalent to its position in execution-list order: 802.1x authentication, MAC authentication bypass (MAB), and web authentication. Use the **dot1x**, **mab**, and **webauth** keywords to change this default order.

**Examples**

This example shows how to set 802.1x as the first authentication method and web authentication as the second authentication method:

```
Controller(config-if) # authentication priority dotx webauth
```

This example shows how to set MAB as the first authentication method and web authentication as the second authentication method:

```
Controller(config-if) # authentication priority mab webauth
```

**Related Commands**

Command	Description
<b>authentication control-direction</b>	Configures the port mode as unidirectional or bidirectional.
<b>authentication event fail</b>	Specifies how the Auth Manager handles authentication failures as a result of unrecognized user credentials.
<b>authentication event no-response action</b>	Specifies how the Auth Manager handles authentication failures as a result of a nonresponsive host.
<b>authentication event server alive action reinitialize</b>	Reinitializes an authorized Auth Manager session when a previously unreachable authentication, authorization, and accounting server becomes available.
<b>authentication event server dead action authorize</b>	Authorizes Auth Manager sessions when the authentication, authorization, and accounting server becomes unreachable.
<b>authentication fallback</b>	Enables a web authentication fallback method.
<b>authentication host-mode</b>	Allows hosts to gain access to a controlled port.
<b>authentication open</b>	Enables open access on a port.
<b>authentication order</b>	Specifies the order in which the Auth Manager attempts to authenticate a client on a port.
<b>authentication periodic</b>	Enables automatic reauthentication on a port.
<b>authentication port-control</b>	Configures the authorization state of a controlled port.
<b>authentication timer inactivity</b>	Configures the time after which an inactive Auth Manager session is terminated.
<b>authentication timer reauthenticate</b>	Specifies the period of time between which the Auth Manager attempts to reauthenticate authorized ports.

Command	Description
<b>authentication timer restart</b>	Specifies the period of time after which the Auth Manager attempts to authenticate an unauthorized port.
<b>authentication violation</b>	Specifies the action to be taken when a security violation occurs on a port.
<b>mab</b>	Enables MAC authentication bypass on a port.
<b>show authentication registrations</b>	Displays information about the authentication methods that are registered with the Auth Manager.
<b>show authentication sessions</b>	Displays information about current Auth Manager sessions.
<b>show authentication sessions interface</b>	Displays information about the Auth Manager for a given interface.

# authentication violation

To configure the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port, use the **authentication violation** command in interface configuration mode.

**authentication violation** { protect|replace|restrict|shutdown }

**no authentication violation** { protect|replace|restrict|shutdown }

## Syntax Description

<b>protect</b>	Drops unexpected incoming MAC addresses. No syslog errors are generated.
<b>replace</b>	Removes the current session and initiates authentication with the new host.
<b>restrict</b>	Generates a syslog error when a violation error occurs.
<b>shutdown</b>	Error-disables the port or the virtual port on which an unexpected MAC address occurs.

## Command Default

Authentication violation shutdown mode is enabled.

## Command Modes

Interface configuration

## Command History

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

## Usage Guidelines

Use the **authentication violation** command to specify the action to be taken when a security violation occurs on a port.

## Examples

This example shows how to configure an IEEE 802.1x-enabled port as error-disabled and to shut down when a new device connects it:

```
Controller(config-if) # authentication violation shutdown
```

This example shows how to configure an 802.1x-enabled port to generate a system error message and to change the port to restricted mode when a new device connects to it:

```
Controller(config-if) # authentication violation restrict
```



This example shows how to configure an 802.1x-enabled port to ignore a new device when it connects to the port:

```
Controller(config-if)# authentication violation protect
```

This example shows how to configure an 802.1x-enabled port to remove the current session and initiate authentication with a new device when it connects to the port:

```
Controller(config-if)# authentication violation replace
```

You can verify your settings by entering the **show authentication** privileged EXEC command.

# banner

To display a banner on the web-authentication login web page, use the **banner** command in parameter map webauth configuration mode. To disable the banner display, use the **no** form of this command.

**banner** { **file** *location:filename* | **text** *banner-text* }

**no banner** { **file** *location:filename* | **text** *banner-text* }

## Syntax Description

<i>location:filename</i>	(Optional) Specifies a file that contains the banner to display on the web authentication login page.
<b>text</b> <i>banner-text</i>	(Optional) Specifies a text string to use as the banner. You must enter a delimiting character before and after the banner text. The delimiting character can be any character of your choice, such as "c" or "@."

## Command Default

No banner displays on the web-authentication login web page.

## Command Modes

Parameter map webauth configuration (config-params-parameter-map)

## Command History

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

## Usage Guidelines

The **banner** command allows you to configure one of three possible scenarios:

- The **banner** command without any keyword or argument—Displays the default banner using the name of the device: "Cisco Systems, <device's hostname> Authentication."
- The **banner** command with the **file** *filename* keyword-argument pair—Displays the banner from the custom HTML file you supply. The custom HTML file must be stored in the disk or flash of the device.
- The **banner** command with the **text** *banner-text* keyword-argument pair—Displays the text that you supply. The text must include any required HTML tags.



### Note

If the banner command is not enabled, nothing displays on the login page except text boxes for entering the username and password.

## Examples

The following example shows that a file in flash named **webauth\_banner.html** is specified for the banner:

```
Controller (config)# parameter-map type webauth MAP_1 type consent  
Controller (config-params-parameter-map)# banner file flash:webauth_banner.html
```

# cisp enable

To enable Client Information Signaling Protocol (CISP) on a switch so that it acts as an authenticator to a supplicant switch, use the **cisp enable** global configuration command.

**cisp enable**

**no cisp enable**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** Global configuration

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

**Usage Guidelines** The link between the authenticator and supplicant switch is a trunk. When you enable VTP on both switches, the VTP domain name must be the same, and the VTP mode must be server.

To avoid the MD5 checksum mismatch error when you configure VTP mode, verify that:

- VLANs are not configured on two different switches, which can be caused by two VTP servers in the same domain.
- Both switches have different configuration revision numbers.

**Examples** This example shows how to enable CISP:

```
Controller(config)# cisp enable
```

## Related Commands

Command	Description
<b>dot1x credentials</b> <i>profile</i>	Configures a profile on a supplicant switch.
<b>dot1x supplicant force-multicast</b>	Forces 802.1X supplicant to send multicast packets.
<b>dot1x supplicant controlled transient</b>	Configures controlled access by 802.1X supplicant.
<b>show cisp</b>	Displays CISP information for a specified interface.



# clear errdisable interface vlan

To reenable a VLAN that was error-disabled, use the **clear errdisable interface** command in privileged EXEC mode.

**clear errdisable interface** *interface-id* **vlan** [*vlan-list*]

## Syntax Description

<i>interface-id</i>	Specifies an interface.
<i>vlan list</i>	(Optional) Specifies a list of VLANs to be reenabled. If a VLAN list is not specified, then all VLANs are reenabled.

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

You can reenable a port by using the **shutdown** and **no shutdown** interface configuration commands, or you can clear error-disable for VLANs by using the **clear errdisable** interface command.

## Examples

This example shows how to reenable all VLANs that were error-disabled on Gigabit Ethernet port 4/0/2:

```
Controller# clear errdisable interface gigabitethernet4/0/2 vlan
```

## Related Commands

Command	Description
<b>errdisable detect cause</b>	Enables error-disabled detection for a specific cause or all causes.
<b>errdisable recovery</b>	Configures the recovery mechanism variables.
<b>show errdisable detect</b>	Displays error-disabled detection status.
<b>show errdisable recovery</b>	Displays error-disabled recovery timer information.

Command	Description
<b>show interfaces status err-disabled</b>	Displays interface status of a list of interfaces in error-disabled state.

# clear mac address-table

To delete from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, all dynamic addresses on stack members, or all dynamic addresses on a particular VLAN, use the **clear mac address-table** command in privileged EXEC mode. This command also clears the MAC address notification global counters.

**clear mac address-table** {dynamic [**address** *mac-addr* | **interface** *interface-id* | **vlan** *vlan-id*] | **move update** | **notification**}

## Syntax Description

<b>dynamic</b>	Deletes all dynamic MAC addresses.
<b>address</b> <i>mac-addr</i>	(Optional) Deletes the specified dynamic MAC address.
<b>interface</b> <i>interface-id</i>	(Optional) Deletes all dynamic MAC addresses on the specified physical port or port channel.
<b>vlan</b> <i>vlan-id</i>	(Optional) Deletes all dynamic MAC addresses for the specified VLAN. The range is 1 to 4094.
<b>move update</b>	Clears the MAC address table move-update counters.
<b>notification</b>	Clears the notifications in the history table and reset the counters.

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

You can verify that the information was deleted by entering the **show mac address-table** privileged EXEC command.

## Examples

This example shows how to remove a specific MAC address from the dynamic address table:

```
Controller# clear mac address-table dynamic address 0008.0070.0007
```



**Related Commands**

Command	Description
<b>mac address-table notification</b>	Enables the MAC address notification feature.
<b>mac address-table move update {receive   transmit}</b>	Configures MAC address-table move update on the switch.
<b>show mac address-table</b>	Displays the MAC address table static and dynamic entries.
<b>show mac address-table move update</b>	Displays the MAC address-table move update information on the switch.
<b>show mac address-table notification</b>	Displays the MAC address notification settings for all interfaces or on the specified interface when the <b>interface</b> keyword is appended.
<b>snmp trap mac-notification change</b>	Enables the SNMP MAC address notification trap on a specific interface.

# consent email

To request a user's e-mail address on the consent login web page, use the **consent email** command in parameter map webauth configuration mode. To remove the consent parameter file from the map, use the **no** form of this command.

**consent email**

**no consent email**

## Command Default

The e-mail address is not requested on the consent login page.

## Command Modes

Parameter map webauth configuration (config-params-parameter-map)

## Command History

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

## Usage Guidelines

Use the consent email command to display a text box on the consent login page prompting the user to enter his or her e-mail address for identification. The device sends this e-mail address to the authentication, authorization, and accounting (AAA) server instead of sending the client's MAC address.

The consent feature allows you to provide temporary Internet and corporate access to end users through their wired and wireless networks by presenting a consent web page. This web page lists the terms and conditions under which the organization is willing to grant access to end users. Users can connect to the network only after they accept the terms on the consent web page.

If you create a parameter map with the type command set to consent, the device does not prompt the user for his or her username and password credentials. Users instead get a choice of two radio buttons: accept or do not accept. For accounting purposes, the device sends the client's MAC address to the AAA server if no username is available (because consent is enabled).

This command is supported in named parameter maps only.

## Examples

The following example shows how to configure a parameter map with the consent e-mail feature enabled:

```
Controller (config)# parameter-map type webauth MAP_1 type webauth
Controller(config-params-parameter-map)# consent email
Controller(config-params-parameter-map)# banner file flash:webauth_banner.html
```

## deny (MAC access-list configuration)

To prevent non-IP traffic from being forwarded if the conditions are matched, use the **deny** MAC access-list configuration command on the switch stack or on a standalone switch. To remove a deny condition from the named MAC access list, use the **no** form of this command.

**deny** {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lvc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**][**cos** *cos*]

**no deny** {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lvc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**][**cos** *cos*]

### Syntax Description

<b>any</b>	Denies any source or destination MAC address.
<b>host</b> <i>src-MAC-addr</i>   <i>src-MAC-addr mask</i>	Defines a host MAC address and optional subnet mask. If the source address for a packet matches the defined address, non-IP traffic from that address is denied.
<b>host</b> <i>dst-MAC-addr</i>   <i>dst-MAC-addr mask</i>	Defines a destination MAC address and optional subnet mask. If the destination address for a packet matches the defined address, non-IP traffic to that address is denied.
<i>type mask</i>	(Optional) Specifies the EtherType number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet.  The type is 0 to 65535, specified in hexadecimal.  The mask is a mask of don't care bits applied to the EtherType before testing for a match.
<b>aarp</b>	(Optional) Specifies EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
<b>amber</b>	(Optional) Specifies EtherType DEC-Amber.
<b>appletalk</b>	(Optional) Specifies EtherType AppleTalk/EtherTalk.
<b>dec-spanning</b>	(Optional) Specifies EtherType Digital Equipment Corporation (DEC) spanning tree.
<b>decnet-iv</b>	(Optional) Specifies EtherType DECnet Phase IV protocol.
<b>diagnostic</b>	(Optional) Specifies EtherType DEC-Diagnostic.

<b>dsm</b>	(Optional) Specifies EtherType DEC-DSM.
<b>etype-6000</b>	(Optional) Specifies EtherType 0x6000.
<b>etype-8042</b>	(Optional) Specifies EtherType 0x8042.
<b>lat</b>	(Optional) Specifies EtherType DEC-LAT.
<b>lavc-sca</b>	(Optional) Specifies EtherType DEC-LAVC-SCA.
<b>lsap</b> <i>lsap-number mask</i>	(Optional) Specifies the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet.  <i>mask</i> is a mask of don't care bits applied to the LSAP number before testing for a match.
<b>mop-console</b>	(Optional) Specifies EtherType DEC-MOP Remote Console.
<b>mop-dump</b>	(Optional) Specifies EtherType DEC-MOP Dump.
<b>msdos</b>	(Optional) Specifies EtherType DEC-MSDOS.
<b>mumps</b>	(Optional) Specifies EtherType DEC-MUMPS.
<b>netbios</b>	(Optional) Specifies EtherType DEC- Network Basic Input/Output System (NetBIOS).
<b>vines-echo</b>	(Optional) Specifies EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
<b>vines-ip</b>	(Optional) Specifies EtherType VINES IP.
<b>xns-idp</b>	(Optional) Specifies EtherType Xerox Network Systems (XNS) protocol suite (0 to 65535), an arbitrary EtherType in decimal, hexadecimal, or octal.
<b>cos</b> <i>cos</i>	(Optional) Specifies a class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message reminds the user if the <b>cos</b> option is configured.

**Command Default**

This command has no defaults. However, the default action for a MAC-named ACL is to deny.

**Command Modes**

Mac-access list configuration

**Command History**

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

**Usage Guidelines**

You enter MAC-access list configuration mode by using the **mac access-list extended** global configuration command.

If you use the **host** keyword, you cannot enter an address mask; if you do not use the **host** keyword, you must enter an address mask.

When an access control entry (ACE) is added to an access control list, an implied **deny-any-any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

To filter IPX traffic, you use the *type mask* or **lsap lsap mask** keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS terminology are listed in the table.

**Table 4: IPX Filtering Criteria**

IPX Encapsulation Type		Filter Criterion
Cisco IOS Name	Novel Name	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

**Examples**

This example shows how to define the named MAC extended access list to deny NETBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is denied.

```
Controller(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
```

This example shows how to remove the deny condition from the named MAC extended access list:

```
Controller(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

This example denies all packets with EtherType 0x4321:

```
Controller(config-ext-macl)# deny any any 0x4321 0
```

You can verify your settings by entering the **show access-lists** privileged EXEC command.

**Related Commands**

Command	Description
<b>mac access-list extended</b>	Creates an access list based on MAC addresses for non-IP traffic.
<b>permit</b>	Permits from the MAC access-list configuration. Permits non-IP traffic to be forwarded if conditions are matched.
<b>show access-lists</b>	Displays access control lists configured on a switch.

## device-role (IPv6 snooping)

To specify the role of the device attached to the port, use the **device-role** command in IPv6 snooping configuration mode.

**device-role** {**node** | **switch**}

### Syntax Description

<b>node</b>	Sets the role of the attached device to node.
<b>switch</b>	Sets the role of the attached device to switch.

### Command Default

The device role is node.

### Command Modes

IPv6 snooping configuration

### Command History

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

### Usage Guidelines

The **device-role** command specifies the role of the device attached to the port. By default, the device role is node.

The **switch** keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with trunk\_port preference level. If the port is configured as a trust-port, binding entries will be marked with trunk\_trusted\_port preference level.

### Examples

This example shows how to define an IPv6 snooping policy name as policy1, place the device in IPv6 snooping configuration mode, and configure the device as the node:

```
Controller(config)# ipv6 snooping policy policy1
Controller(config-ipv6-snooping)# device-role node
```

## device-role (IPv6 nd inspection)

To specify the role of the device attached to the port, use the **device-role** command in neighbor discovery (ND) inspection policy configuration mode.

**device-role** {**host** | **monitor** | **router** | **switch**}

### Syntax Description

<b>host</b>	Sets the role of the attached device to host.
<b>monitor</b>	Sets the role of the attached device to monitor.
<b>router</b>	Sets the role of the attached device to router.
<b>switch</b>	Sets the role of the attached device to switch.

### Command Default

The device role is host.

### Command Modes

ND inspection policy configuration

### Command History

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

### Usage Guidelines

The **device-role** command specifies the role of the device attached to the port. By default, the device role is host, and therefore all the inbound router advertisement and redirect messages are blocked. If the device role is enabled using the **router** keyword, all messages (router solicitation [RS], router advertisement [RA], or redirect) are allowed on this port.

When the **router** or **monitor** keyword is used, the multicast RS messages are bridged on the port, regardless of whether limited broadcast is enabled. However, the monitor keyword does not allow inbound RA or redirect messages. When the monitor keyword is used, devices that need these messages will receive them.

The **switch** keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with trunk\_port preference level. If the port is configured as a trust-port, binding entries will be marked with trunk\_trusted\_port preference level.

### Examples

The following example defines a Neighbor Discovery Protocol (NDP) policy name as policy1, places the device in ND inspection policy configuration mode, and configures the device as the host:

```
Controller(config)# ipv6 nd inspection policy policy1
Controller(config-nd-inspection)# device-role host
```



## dot1x critical (global configuration)

To configure the IEEE 802.1X critical authentication parameters, use the **dot1x critical** command in global configuration mode.

### dot1x critical eapol

#### Syntax Description

<b>eapol</b>	Specifies that the switch send an EAPOL-Success message when the switch successfully authenticates the critical port.
--------------	---

#### Command Default

**eapol** is disabled

#### Command Modes

Global configuration

#### Command History

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

#### Examples

This example shows how to specify that the switch sends an EAPOL-Success message when the switch successfully authenticates the critical port:

```
Controller(config)# dot1x critical eapol
```

# dot1x pae

To set the Port Access Entity (PAE) type, use the **dot1x pae** command in interface configuration mode. To disable the PAE type that was set, use the **no** form of this command.

**dot1x pae** {supplicant | authenticator}

**no dot1x pae** {supplicant | authenticator}

## Syntax Description

<b>supplicant</b>	The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.
<b>authenticator</b>	The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.

## Command Default

PAE type is not set.

## Command Modes

Interface configuration

## Command History

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

## Usage Guidelines

Use the **no dot1x pae** interface configuration command to disable IEEE 802.1x authentication on the port.

When you configure IEEE 802.1x authentication on a port, such as by entering the **dot1x port-control** interface configuration command, the switch automatically configures the port as an IEEE 802.1x authenticator. After the **no dot1x pae** interface configuration command is entered, the Authenticator PAE operation is disabled.

## Examples

The following example shows that the interface has been set to act as a supplicant:

```
Controller(config)# interface g1/0/3
Controller(config-if)# dot1x pae supplicant
```

# dot1x supplicant force-multicast

To force a supplicant switch to send only multicast Extensible Authentication Protocol over LAN (EAPOL) packets whenever it receives multicast or unicast EAPOL packets, use the **dot1x supplicant force-multicast** command in global configuration mode. To return to the default setting, use the **no** form of this command.

**dot1x supplicant force-multicast**

**no dot1x supplicant force-multicast**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The supplicant switch sends unicast EAPOL packets when it receives unicast EAPOL packets. Similarly, it sends multicast EAPOL packets when it receives multicast EAPOL packets.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

Enable this command on the supplicant switch for Network Edge Access Topology (NEAT) to work in all host modes.

## Examples

This example shows how force a supplicant switch to send multicast EAPOL packets to the authenticator switch:

```
Controller(config)# dot1x supplicant force-multicast
```

## Related Commands

Command	Description
<b>cisp enable</b>	Enable Client Information Signalling Protocol (CISP) on a switch so that it acts as an authenticator to a supplicant switch.
<b>dot1x credentials</b>	Configure the 802.1x supplicant credentials on the port.
<b>dot1x pae supplicant</b>	Configure an interface to act only as a supplicant.

# dot1x test eapol-capable

To monitor IEEE 802.1x activity on all the switch ports and to display information about the devices that are connected to the ports that support IEEE 802.1x, use the **dot1x test eapol-capable** command in privileged EXEC mode on the switch stack or on a standalone switch.

**dot1x test eapol-capable** [**interface** *interface-id*]

Syntax Description	<b>interface</b> <i>interface-id</i>	(Optional) Port to be queried.
--------------------	--------------------------------------	--------------------------------

**Command Default** There is no default setting.

**Command Modes** Privileged EXEC

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

**Usage Guidelines** Use this command to test the IEEE 802.1x capability of the devices connected to all ports or to specific ports on a switch.

There is not a no form of this command.

**Examples** This example shows how to enable the IEEE 802.1x readiness check on a switch to query a port. It also shows the response received from the queried port verifying that the device connected to it is IEEE 802.1x-capable:

```
Controller# dot1x test eapol-capable interface gigabitethernet1/0/13
```

```
DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL capable
```

## Related Commands

Command	Description
<b>dot1x test timeout</b> <i>timeout</i>	Configures the timeout used to wait for EAPOL response to an IEEE 802.1x readiness query.

# dot1x test timeout

To configure the timeout used to wait for EAPOL response from a port being queried for IEEE 802.1x readiness, use the **dot1x test timeout** command in global configuration mode on the switch stack or on a standalone switch.

**dot1x test timeout** *timeout*

## Syntax Description

<i>timeout</i>	Time in seconds to wait for an EAPOL response. The range is from 1 to 65535 seconds.
----------------	--

## Command Default

The default setting is 10 seconds.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

Use this command to configure the timeout used to wait for EAPOL response.

There is not a no form of this command.

## Examples

This example shows how to configure the switch to wait 27 seconds for an EAPOL response:

```
Controller# dot1x test timeout 27
```

You can verify the timeout configuration status by entering the **show run** privileged EXEC command.

## Related Commands

Command	Description
<b>dot1x test eapol-capable</b> [ <i>interface interface-id</i> ]	Checks for IEEE 802.1x readiness on devices connected to all or to specified IEEE 802.1x-capable ports.

## dot1x timeout

To configure the value for retry timeouts, use the **dot1x timeout** command in global configuration or interface configuration mode. To return to the default value for retry timeouts, use the **no** form of this command.

**dot1x timeout** {**auth-period** *seconds* | **held-period** *seconds* | **quiet-period** *seconds* | **ratelimit-period** *seconds* | **server-timeout** *seconds* | **start-period** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds*}

### Syntax Description

<b>auth-period</b> <i>seconds</i>	Configures the time, in seconds for which a supplicant will stay in the HELD state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt).  The range is from 1 to 65535. The default is 30.
<b>held-period</b> <i>seconds</i>	Configures the time, in seconds for which a supplicant will stay in the HELD state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt).  The range is from 1 to 65535. The default is 60
<b>quiet-period</b> <i>seconds</i>	Configures the time, in seconds, that the authenticator (server) remains quiet (in the HELD state) following a failed authentication exchange before trying to reauthenticate the client.  The range is from 1 to 65535. The default is 60
<b>ratelimit-period</b> <i>seconds</i>	Throttles the EAP-START packets that are sent from misbehaving client PCs (for example, PCs that send EAP-START packets that result in the wasting of switch processing power). <ul style="list-style-type: none"> <li>• The authenticator ignores EAPOL-Start packets from clients that have successfully authenticated for the rate-limit period duration.</li> <li>• The range is from 1 to 65535. By default, rate limiting is disabled.</li> </ul>
<b>server-timeout</b> <i>seconds</i>	Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted. <ul style="list-style-type: none"> <li>• The range is from 1 to 65535. The default is 30.</li> </ul> <p>If the server does not send a response to an 802.1X packet within the specified period, the packet is sent again.</p>
<b>start-period</b> <i>seconds</i>	Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted.  The range is from 1 to 65535. The default is 30.

<b>supp-timeout</b> <i>seconds</i>	Sets the authenticator-to-suppliant retransmission time for all EAP messages other than EAP Request ID.  The range is from 1 to 65535. The default is 30.
<b>tx-period</b> <i>seconds</i>	Configures the number of seconds between retransmission of EAP request ID packets (assuming that no response is received) to the client.  <ul style="list-style-type: none"> <li>• The range is from 1 to 65535. The default is 30.</li> <li>• If an 802.1X packet is sent to the supplicant and the supplicant does not send a response after the retry period, the packet will be sent again.</li> </ul>

**Command Default** Periodic reauthentication and periodic rate-limiting are done.

**Command Modes** Interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines**

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The **dot1x timeout reauth-period** interface configuration command affects the behavior of the switch only if you have enabled periodic re-authentication by using the **dot1x reauthentication** interface configuration command.

During the quiet period, the switch does not accept or initiate any authentication requests. If you want to provide a faster response time to the user, enter a number smaller than the default.

When the **ratelimit-period** is set to 0 (the default), the switch does not ignore EAPOL packets from clients that have been successfully authenticated and forwards them to the RADIUS server.

**Examples** The following example shows that various 802.1X retransmission and timeout periods have been set:

```

Controller(config)# configure terminal
Controller(config)# interface g1/0/3
Controller(config-if)# dot1x port-control auto
Controller(config-if)# dot1x timeout auth-period 2000
Controller(config-if)# dot1x timeout held-period 2400
Controller(config-if)# dot1x timeout quiet-period 600
Controller(config-if)# dot1x timeout start-period 90
Controller(config-if)# dot1x timeout supp-timeout 300
Controller(config-if)# dot1x timeout tx-period 60

```

```
Controller(config-if)# dot1x timeout server-timeout 60
```



# epm access-control open

To configure an open directive for ports that do not have an access control list (ACL) configured, use the **epm access-control open** command in global configuration mode. To disable the open directive, use the **no** form of this command.

**epm access-control open**

**no epm access-control open**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The default directive applies.

**Command Modes** Global configuration

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

**Usage Guidelines** Use this command to configure an open directive that allows hosts without an authorization policy to access ports configured with a static ACL. If you do not configure this command, the port applies the policies of the configured ACL to the traffic. If no static ACL is configured on a port, both the default and open directives allow access to the port.

You can verify your settings by entering the **show running-config** privileged EXEC command.

**Examples** This example shows how to configure an open directive.

```
Controller(config)# epm access-control open
```

Related Commands	Command	Description
	<b>show running-config</b>	Displays the contents of the current running configuration file.

# fips authorization-key

To configure the FIPS authorization key on the controller, use the **fips authorization-key** command in global configuration mode.

**fips authorization-key** *key*

## Syntax Description

<i>key</i>	FIPS authorization key. Authentication key should be 32-hexadecimal character.
<b>Note</b>	The key is also used to encrypt traffic between members of a stack. You should always set the keys before creating the stack (so that each physical member has a key). Also, the stack traffic slows down with encryption (about 30% slower).

## Command Default

None

## Command Modes

Global Configuration

## Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

## Usage Guidelines

Authorization keys should be same for all the controllers in a stack.

## Examples

The following example shows how to create a FIPS authorization key on the controller:

```
Controller(config) # fips authorization-key 123456789012345678901234567890
```

# fips log-dtls-replay

To generate logs for events related to replay attack of DTLS packets, use the **fips log-dtls-replay** command in global configuration mode.

**fips log-dtls-replay**

## Command Default

None

## Command Modes

Global Configuration

## Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

## Examples

The following example generates logs for events related to replay attack of DTLS packets on the controller:

```
Controller(config)# fips log-dtls-replay
```

# fips zeroize

To zeroize the controller, use the **fips zeroize** command in global configuration mode.

## fips zeroize

### Command Default

None

### Command Modes

Global Configuration

### Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

### Usage Guidelines

This is done in extreme cases, where, in the process of deleting the keys, the configuration file and IOS image are also deleted from the controller or AP.



#### Caution

You must be careful before zeroizing the controller or AP as after performing this operation, the controller or AP becomes unusable.

### Examples

The following example shows how to zeroize the controller:

```
Controller(config)# fips zeroize
**Critical Warning** - This command is irreversible
and will zeroize the FVPK by Deleting the IOS
image and config files, please use extreme
caution and confirm with Yes on each of three
iterations to complete. The system will reboot
after the command executes successfully
Proceed ?? (yes/[no]): no
%Aborting zeroization!
```

# ip admission

To enable web authentication, use the **ip admission** command in interface configuration mode. You can also use this command in fallback-profile configuration mode. To disable web authentication, use the **no** form of this command.

**ip admission** *rule*

**no ip admission** *rule*

## Syntax Description

<i>rule</i>	IP admission rule name.
-------------	-------------------------

## Command Default

Web authentication is disabled.

## Command Modes

Interface configuration

Fallback-profile configuration

## Command History

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

## Usage Guidelines

The **ip admission** command applies a web authentication rule to a switch port.

## Examples

This example shows how to apply a web authentication rule to a switchport:

```
Controller# configure terminal
Controller(config)# interface gigabitethernet1/0/1
Controller(config-if)# ip admission rule1
```

This example shows how to apply a web authentication rule to a fallback profile for use on an IEEE 802.1x enabled switch port.

```
Controller# configure terminal
Controller(config)# fallback profile profile1
Controller(config-fallback-profile)# ip admission rule1
```

# ip admission name

To enable web authentication, use the **ip admission name** command in global configuration mode. To disable web authentication, use the **no** form of this command.

**ip admission name** *name* {**consent** | **proxy http**} [**absolute timer** *minutes* | **inactivity-time** *minutes* | **list** {*acl* | *acl-name*} | **service-policy type tag** *service-policy-name*]

**no ip admission name** *name* {**consent** | **proxy http**} [**absolute timer** *minutes* | **inactivity-time** *minutes* | **list** {*acl* | *acl-name*} | **service-policy type tag** *service-policy-name*]

## Syntax Description

<i>name</i>	Name of network admission control rule.
<b>consent</b>	Associates an authentication proxy consent web page with the IP admission rule specified using the <i>admission-name</i> argument.
<b>proxy http</b>	Configures web authentication custom page.
<b>absolute-timer</b> <i>minutes</i>	(Optional) Elapsed time, in minutes, before the external server times out.
<b>inactivity-time</b> <i>minutes</i>	(Optional) Elapsed time, in minutes, before the external file server is deemed unreachable.
<b>list</b>	(Optional) Associates the named rule with an access control list (ACL).
<i>acl</i>	Applies a standard, extended list to a named admission control rule. The value ranges from 1 through 199, or from 1300 through 2699 for expanded range.
<i>acl-name</i>	Applies a named access list to a named admission control rule.
<b>service-policy type tag</b>	(Optional) A control plane service policy is to be configured.
<i>service-policy-name</i>	Control plane tag service policy that is configured using the <b>policy-map type control tag</b> <i>polycyname</i> command, keyword, and argument. This policy map is used to apply the actions on the host when a tag is received.

## Command Default

Web authentication is disabled.

**Command Modes**

Global configuration

**Command History**

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

**Usage Guidelines**

The **ip admission name** command globally enables web authentication on a switch.

After you enable web authentication on a switch, use the **ip access-group in** and **ip admission web-rule** interface configuration commands to enable web authentication on a specific interface.

**Examples**

This example shows how to configure only web authentication on a switch port:

```
Controller# configure terminal
Controller(config)# ip admission name http-rule proxy http
Controller(config)# interface gigabitethernet1/0/1
Controller(config-if)# ip access-group 101 in
Controller(config-if)# ip admission rule
Controller(config-if)# end
```

This example shows how to configure IEEE 802.1x authentication with web authentication as a fallback mechanism on a switch port:

```
Controller# configure terminal
Controller(config)# ip admission name rule2 proxy http
Controller(config)# fallback profile profile1
Controller(config)# ip access group 101 in
Controller(config)# ip admission name rule2
Controller(config)# interface gigabitethernet1/0/1
Controller(config-if)# dot1x port-control auto
Controller(config-if)# dot1x fallback profile1
Controller(config-if)# end
```

**Related Commands**

Command	Description
<b>dot1x fallback</b>	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
<b>fallback profile</b>	Creates a web authentication fallback profile.
<b>ip admission</b>	Enables web authentication on a port.
<b>show authentication sessions interface <i>interface</i> detail</b>	Displays information about the web authentication session status.

Command	Description
<b>show ip admission</b>	Displays information about NAC cached entries or the NAC configuration.



# ip device tracking maximum

To configure IP device tracking parameters on a Layer 2 access port, use the **ip device tracking maximum** command in interface configuration mode. To remove the maximum value, use the **no** form of the command.

**ip device tracking maximum** *number*

**no ip device tracking maximum**

<b>Syntax Description</b>	<div><div><i>number</i></div><div>Number of bindings created in the IP device tracking table for a port. The range is 0 (disabled) to 65535.</div></div>				
<b>Command Default</b>	None				
<b>Command Modes</b>	Interface configuration mode				
<b>Command History</b>	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>Cisco IOS XE 3.2SE</td><td>This command was introduced.</td></tr></table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				

**Usage Guidelines**

To remove the maximum value, use the **no ip device tracking maximum** command.

To disable IP device tracking, use the **ip device tracking maximum 0** command.

**Examples**

This example shows how to configure IP device tracking parameters on a Layer 2 access port:

```

Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# ip device tracking
Controller(config)# interface gigabitethernet1/0/3
Controller(config-if)# switchport mode access
Controller(config-if)# switchport access vlan 1
Controller(config-if)# ip device tracking maximum 5
Controller(config-if)# switchport port-security
Controller(config-if)# switchport port-security maximum 5
Controller(config-if)# end

```

# ip device tracking probe

To configure the IP device tracking table for Address Resolution Protocol (ARP) probes, use the **ip device tracking probe** command in global configuration mode. To disable ARP probes, use the **no** form of this command.

**ip device tracking probe** {*count number*| *delay seconds*| *interval seconds*| **use-svi** *address*}

**no ip device tracking probe** {*count number*| *delay seconds*| *interval seconds*| **use-svi** *address*}

## Syntax Description

<b>count</b> <i>number</i>	Sets the number of times that the controller sends the ARP probe. The range is from 1 to 255.
<b>delay</b> <i>seconds</i>	Sets the number of seconds that the controller waits before sending the ARP probe. The range is from 1 to 120.
<b>interval</b> <i>seconds</i>	Sets the number of seconds that the controller waits for a response before resending the ARP probe. The range is from 30 to 1814400 seconds.
<b>use-svi</b>	Uses the switch virtual interface (SVI) IP address as source of ARP probes.

## Command Default

The count number is 3.

There is no delay.

The interval is 30 seconds.

The ARP probe default source IP address is the Layer 3 interface and 0.0.0.0 for switchports.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

Use the **use-svi** keyword to configure the IP device tracking table to use the SVI IP address for ARP probes in cases when the default source IP address 0.0.0.0 for switch ports is used and the ARP probes drop.

## Examples

This example shows how to set SVI as the source for ARP probes:

```
Controller(config)# ip device tracking probe use-svi
```

# ip dhcp snooping database

To configure the Dynamic Host Configuration Protocol (DHCP)-snooping database, use the **ip dhcp snooping database** command in global configuration mode. To disable the DHCP-snooping database, use the **no** form of this command.

**no ip dhcp snooping database** [ **timeout** | **write-delay** ]

## Syntax Description

<b>flash:</b> <i>url</i>	Specifies the database URL for storing entries using flash.
<b>ftp:</b> <i>url</i>	Specifies the database URL for storing entries using FTP.
<b>http:</b> <i>url</i>	Specifies the database URL for storing entries using HTTP.
<b>https:</b> <i>url</i>	Specifies the database URL for storing entries using secure HTTP (https).
<b>rcp:</b> <i>url</i>	Specifies the database URL for storing entries using remote copy (rcp).
<b>scp:</b> <i>url</i>	Specifies the database URL for storing entries using Secure Copy (SCP).
<b>tftp:</b> <i>url</i>	Specifies the database URL for storing entries using TFTP.
<b>timeout</b> <i>seconds</i>	Specifies the abort timeout interval; valid values are from 0 to 86400 seconds.
<b>write-delay</b> <i>seconds</i>	Specifies the amount of time before writing the DHCP-snooping entries to an external server after a change is seen in the local DHCP-snooping database; valid values are from 15 to 86400 seconds.

## Command Default

The DHCP-snooping database is not configured.

**Command Modes**

Global configuration

**Command History**

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

**Usage Guidelines**

You must enable DHCP snooping on the interface before entering this command. Use the **ip dhcp snooping** command to enable DHCP snooping.

**Examples**

This example shows how to specify the database URL using TFTP:

```
Controller(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
```

This example shows how to specify the amount of time before writing DHCP snooping entries to an external server:

```
Controller(config)# ip dhcp snooping database write-delay 15
```

# ip dhcp snooping information option format remote-id

To configure the option-82 remote-ID suboption, use the **ip dhcp snooping information option format remote-id** command in global configuration mode on the switch to configure the option-82 remote-ID suboption. To configure the default remote-ID suboption, use the **no** form of this command.

**ip dhcp snooping information option format remote-id** {hostname | string *string*}

**no ip dhcp snooping information option format remote-id** {hostname | string *string*}

## Syntax Description

<b>hostname</b>	Specify the switch hostname as the remote ID.
<b>string</b> <i>string</i>	Specify a remote ID, using from 1 to 63 ASCII characters (no spaces).

## Command Default

The switch MAC address is the remote ID.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

You must globally enable DHCP snooping by using the **ip dhcp snooping** global configuration command for any DHCP snooping configuration to take effect.

When the option-82 feature is enabled, the default remote-ID suboption is the switch MAC address. This command allows you to configure either the switch hostname or a string of up to 63 ASCII characters (but no spaces) to be the remote ID.



### Note

If the hostname exceeds 63 characters, it will be truncated to 63 characters in the remote-ID configuration.

## Examples

This example shows how to configure the option- 82 remote-ID suboption:

```
Controller(config)# ip dhcp snooping information option format remote-id hostname
```

# ip dhcp snooping verify no-relay-agent-address

To disable the DHCP snooping feature from verifying that the relay agent address (giaddr) in a DHCP client message matches the client hardware address on an untrusted port, use the **ip dhcp snooping verify no-relay-agent-address** command in global configuration mode. To enable verification, use the **no** form of this command.

**ip dhcp snooping verify no-relay-agent-address**

**no ip dhcp snooping verify no-relay-agent-address**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The DHCP snooping feature verifies that the relay-agent IP address (giaddr) field in DHCP client message on an untrusted port is 0.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

By default, the DHCP snooping feature verifies that the relay-agent IP address (giaddr) field in DHCP client message on an untrusted port is 0; the message is dropped if the giaddr field is not 0. Use the **ip dhcp snooping verify no-relay-agent-address** command to disable the verification. Use the **no ip dhcp snooping verify no-relay-agent-address** to reenale verification.

## Examples

This example shows how to enable verification of the giaddr in a DHCP client message:

```
Controller(config)# no ip dhcp snooping verify no-relay-agent-address
```

# ip dhcp snooping wireless bootp-broadcast enable

To enable broadcast address sent by the server to be retained by the switch when it forwards DHCP packets to wireless clients, use the **ip dhcp snooping wireless bootp-broadcast enable** form of this command.

**ip dhcp snooping wireless bootp-broadcast enable**

Syntax Description	<b>enable</b>	Enables broadcast address sent by the server to be retained by the switch when it forwards DHCP packets to wireless clients.
--------------------	---------------	--

Command Modes	Global configuration
---------------	----------------------

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

**Examples**

This example shows how to enable broadcast address sent by the server to be retained by the switch when it forwards DHCP packets to wireless clients.

```
Controller(config)# ip dhcp snooping wireless bootp-broadcast enable
```

# ip source binding

To add a static IP source binding entry, use the **ip source binding** command. Use the **no** form of this command to delete a static IP source binding entry.

**ip source binding** *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id*

**no ip source binding** *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id*

## Syntax Description

<i>mac-address</i>	Binding MAC address.
<b>vlan</b> <i>vlan-id</i>	Specifies the Layer 2 VLAN identification; valid values are from 1 to 4094.
<i>ip-address</i>	Binding IP address.
<b>interface</b> <i>interface-id</i>	ID of the physical interface.

## Command Default

No IP source bindings are configured.

## Command Modes

Global configuration.

## Command History

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

## Usage Guidelines

You can use this command to add a static IP source binding entry only.

The **no** format deletes the corresponding IP source binding entry. It requires the exact match of all required parameter in order for the deletion to be successful. Note that each static IP binding entry is keyed by a MAC address and a VLAN number. If the command contains the existing MAC address and VLAN number, the existing binding entry is updated with the new parameters instead of creating a separate binding entry.

## Examples

This example shows how to add a static IP source binding entry:

```
Controller# configure terminal
Controller(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet1/0/1
```



# ip verify source

To enable IP source guard on an interface, use the **ip verify source** command in interface configuration mode. To disable IP source guard, use the **no** form of this command.

**ip verify source**

**no ip verify source**

## Syntax Description

**mac-check** (Optional) Enables IP source guard with MAC address verification.

## Command Default

IP source guard is disabled.

## Command Modes

Interface configuration

## Command History

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

## Usage Guidelines

To enable IP source guard with source IP address filtering, use the **ip verify source** interface configuration command.

## Examples

This example shows how to enable IP source guard with source IP address filtering on an interface:

```

Controller(config)# interface gigabitethernet1/0/1
Controller(config-if)# ip verify source

Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# ip dhcp snooping
Controller(config)# ip dhcp snooping vlan 10 20
Controller(config)# interface gigabitethernet1/0/1
Controller(config-if)# switchport trunk encapsulation dot1q
Controller(config-if)# switchport mode trunk
Controller(config-if)# switchport trunk native vlan 10
Controller(config-if)# switchport trunk allowed vlan 11-20
Controller(config-if)# no ip dhcp snooping trust
Controller(config-if)# ip verify source vlan dhcp-snooping
Controller(config)# end
Controller# show ip verify source interface fastethernet0/1

```

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
Gil/0/1	ip-mac	active	10.0.0.1		10
Gil/0/1	ip-mac	active	deny-all		11-20

Controller#

```
Controller# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Controller(config)# ip device tracking  
Controller(config)# interface gigabitethernet1/0/3  
Controller(config-if)# switchport mode access  
Controller(config-if)# switchport access vlan 1  
Controller(config-if)# ip device tracking maximum 5  
Controller(config-if)# switchport port-security  
Controller(config-if)# switchport port-security maximum 5  
Controller(config-if)# ip verify source tracking port-security  
Controller(config-if)# end
```

You can verify your settings by entering the **show ip verify source** privileged EXEC command.

# ipv6 snooping policy

To configure an IPv6 snooping policy and enter IPv6 snooping configuration mode, use the **ipv6 snooping policy** command in global configuration mode. To delete an IPv6 snooping policy, use the **no** form of this command.

**ipv6 snooping policy** *snooping-policy*

**no ipv6 snooping policy** *snooping-policy*

## Syntax Description

<i>snooping-policy</i>	User-defined name of the snooping policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).
------------------------	---

## Command Default

An IPv6 snooping policy is not configured.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

Use the **ipv6 snooping policy** command to create an IPv6 snooping policy. When the **ipv6 snooping policy** command is enabled, the configuration mode changes to IPv6 snooping configuration mode. In this mode, the administrator can configure the following IPv6 first-hop security commands:

- The **device-role** command specifies the role of the device attached to the port.
- The **limit address-count** *maximum* command limits the number of IPv6 addresses allowed to be used on the port.
- The **protocol** command specifies that addresses should be gleaned with Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP).
- The **security-level** command specifies the level of security enforced.
- The **tracking** command overrides the default tracking policy on a port.
- The **trusted-port** command configures a port to become a trusted port; that is, limited or no verification is performed when messages are received.

## Examples

This example shows how to configure an IPv6 snooping policy:

```
Controller(config)# ipv6 snooping policy policy1
```

```
Controller(config-ipv6-snooping)#
```

# key ww-wireless

To configure the RADIUS server encryption key, use the **key ww-wireless** command in global configuration mode.

**key ww-wireless**

## Command Default

None

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

None

## Examples

The following example shows how to configure the RADIUS server encryption key:

```
Controller(config)# radius server ISE
Controller(config-radius-server)# address ipv4 192.168.154.119 auth-port 1812 acct-port 1813
Controller(config-radius-server)# key ww-wireless
```

# limit address-count

To limit the number of IPv6 addresses allowed to be used on the port, use the **limit address-count** command in Neighbor Discovery Protocol (NDP) inspection policy configuration mode or IPv6 snooping configuration mode. To return to the default, use the **no** form of this command.

**limit address-count** *maximum*

**no limit address-count**

## Syntax Description

*maximum*

The number of addresses allowed on the port. The range is from 1 to 10000.

## Command Default

The default is no limit.

## Command Modes

ND inspection policy configuration

IPv6 snooping configuration

## Command History

### Release

Cisco IOS XE 3.2SE

### Modification

This command was introduced.

## Usage Guidelines

The **limit address-count** command limits the number of IPv6 addresses allowed to be used on the port on which the policy is applied. Limiting the number of IPv6 addresses on a port helps limit the binding table size. The range is from 1 to 10000.

## Examples

This example shows how to define an NDP policy name as policy1, place the switch in NDP inspection policy configuration mode, and limit the number of IPv6 addresses allowed on the port to 25:

```
Controller(config)# ipv6 nd inspection policy policy1
Controller(config-nd-inspection)# limit address-count 25
```

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and limit the number of IPv6 addresses allowed on the port to 25:

```
Controller(config)# ipv6 snooping policy policy1
Controller(config-ipv6-snooping)# limit address-count 25
```

# login-auth-bypass

To configure the domain name and FQDN ACL that are to be bypassed for a parameter map, use the **login-auth-bypass fqdn** command in the parameter map configuration mode.

**login-auth-bypass ip-access-list** *acl-name* **domain-name-list** *domain-name*

## Syntax Description

<b>ip-access-list</b> <i>acl-name</i>	Configures a FQDN standard, extended list to a named admission control rule. The value ranges from 1 through 199, or from 1300 through 2699 for expanded range.
<b>domain-name-list</b> <i>domain-name</i>	Configures a domain.

## Command Default

No domain name and FQDN ACL is defined for bypass.

## Command Modes

Parameter map configuration mode

## Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

## Usage Guidelines

The FQDN ACL determines which IP addresses should redirect the BYOD to the ISE onboarding portal page. This ACL is same as the redirect ACL from ISE onboarding.

## Examples

This example shows how to configure the domain name and FQDN ACL that are to be bypassed for a parameter map:

```
Controller(config)# parameter-map type webauth Mymap
Controller(config-params-parameter-map)# login auth-bypass ip-access-list byod
domain-name-list abc
```

## mab request format attribute 32

To enable VLAN ID-based MAC authentication on a switch, use the **mab request format attribute 32 vlan access-vlan** command in global configuration mode. To return to the default setting, use the **no** form of this command.

**mab request format attribute 32 vlan access-vlan**

**no mab request format attribute 32 vlan access-vlan**

### Syntax Description

This command has no arguments or keywords.

### Command Default

VLAN-ID based MAC authentication is disabled.

### Command Modes

Global configuration

### Command History

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

### Usage Guidelines

Use this command to allow a RADIUS server to authenticate a new user based on the host MAC address and VLAN.

Use this feature on networks with the Microsoft IAS RADIUS server. The Cisco ACS ignores this command.

### Examples

This example shows how to enable VLAN-ID based MAC authentication on a switch:

```
Controller(config)# mab request format attribute 32 vlan access-vlan
```

### Related Commands

Command	Description
<b>authentication event</b>	Sets the action for specific authentication events.
<b>authentication fallback</b>	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
<b>authentication host-mode</b>	Sets the authorization manager mode on a port.
<b>authentication open</b>	Enables or disables open access on a port.
<b>authentication order</b>	Sets the order of authentication methods used on a port.



Command	Description
<b>authentication periodic</b>	Enables or disables reauthentication on a port.
<b>authentication port-control</b>	Enables manual control of the port authorization state.
<b>authentication priority</b>	Adds an authentication method to the port-priority list.
<b>authentication timer</b>	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
<b>authentication violation</b>	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port with the maximum number of devices already connected to that port.
<b>mab</b>	Enables MAC-based authentication on a port.
<b>mab eap</b>	Configures a port to use the Extensible Authentication Protocol (EAP).
<b>show authentication</b>	Displays information about authentication manager events on the switch.

## match (access-map configuration)

To set the VLAN map to match packets against one or more access lists, use the **match** command in access-map configuration mode on the switch stack or on a standalone switch. To remove the match parameters, use the **no** form of this command.

**match** {ip address {*name*|*number*} [*name*|*number*] [*name*|*number*]...| mac address {*name*} [*name*] [*name*]...}  
**no match** {ip address {*name*|*number*} [*name*|*number*] [*name*|*number*]...| mac address {*name*} [*name*] [*name*]...}

### Syntax Description

<b>ip address</b>	Sets the access map to match packets against an IP address access list.
<b>mac address</b>	Sets the access map to match packets against a MAC address access list.
<i>name</i>	Name of the access list to match packets against.
<i>number</i>	Number of the access list to match packets against. This option is not valid for MAC access lists.

### Command Default

The default action is to have no match parameters applied to a VLAN map.

### Command Modes

Access-map configuration

### Command History

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

### Usage Guidelines

You enter access-map configuration mode by using the **vlan access-map** global configuration command.

You must enter one access list name or number; others are optional. You can match packets against one or more access lists. Matching any of the lists counts as a match of the entry.

In access-map configuration mode, use the **match** command to define the match conditions for a VLAN map applied to a VLAN. Use the **action** command to set the action that occurs when the packet matches the conditions.

Packets are matched only against access lists of the same protocol type; IP packets are matched against IP access lists, and all other packets are matched against MAC access lists.

Both IP and MAC addresses can be specified for the same map entry.

## Examples

This example shows how to define and apply a VLAN access map vmap4 to VLANs 5 and 6 that will cause the interface to drop an IP packet if the packet matches the conditions defined in access list al2:

```
Controller(config)# vlan access-map vmap4  
Controller(config-access-map)# match ip address al2  
Controller(config-access-map)# action drop  
Controller(config-access-map)# exit  
Controller(config)# vlan filter vmap4 vlan-list 5-6
```

You can verify your settings by entering the **show vlan access-map** privileged EXEC command.

# map-index map

To configure parameter map attributes, use the *map-index* **map** command.

*map-index***map**{*device-type*|*mac-address*|*oui* |*user-role*|*username*} {*eq*|*not-eq* |*regex*} *filter-name*

## Syntax Description

<i>map-index</i>	Parameter map index.
<i>filter-name</i>	Parameter map filter criteria name.

## Command Default

None

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

## Usage Guidelines

None

## Examples

This example shows how to configure parameter map attribute filter criteria:

```
Controller#configure terminal
Controller(config)#parameter-map type subscriber attribute-to-service Aironet-policy-para
Controller(config-parameter-map-filter)#10 map device-type eq "WindowsXP-Workstation"
```

# no authentication logging verbose

To filter detailed information from authentication system messages, use the **no authentication logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

**no authentication logging verbose**

**Syntax Description** This command has no arguments or keywords.

**Command Default** All details are displayed in the system messages.

**Command Modes** Global configuration

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

**Usage Guidelines** This command filters details, such as anticipated success, from authentication system messages. Failure messages are not filtered.

**Examples** To filter verbose authentication system messages:

```
Controller(config)# no authentication logging verbose
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands	Command	Description
	<b>no authentication logging verbose</b>	Filters details from authentication system messages.
	<b>no dot1x logging verbose</b>	Filters details from 802.1x system messages.
	<b>no mab logging verbose</b>	Filters details from MAC authentication bypass (MAB) system messages.

# no dot1x logging verbose

To filter detailed information from 802.1x system messages, use the **no dot1x logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

**no dot1x logging verbose**

## Syntax Description

This command has no arguments or keywords.

## Command Default

All details are displayed in the system messages.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

This command filters details, such as anticipated success, from 802.1x system messages. Failure messages are not filtered.

## Examples

To filter verbose 802.1x system messages:

```
Controller(config)# no dot1x logging verbose
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

## Related Commands

Command	Description
<b>no authentication logging verbose</b>	Filters details from authentication system messages.
<b>no dot1x logging verbose</b>	Filters details from 802.1x system messages.
<b>no mab logging verbose</b>	Filters details from MAC authentication bypass (MAB) system messages.

# no mab logging verbose

To filter detailed information from MAC authentication bypass (MAB) system messages, use the **no mab logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

**no mab logging verbose**

**Syntax Description** This command has no arguments or keywords.

**Command Default** All details are displayed in the system messages.

**Command Modes** Global configuration

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

**Usage Guidelines** This command filters details, such as anticipated success, from MAC authentication bypass (MAB) system messages. Failure messages are not filtered.

**Examples** To filter verbose MAB system messages:

```
Controller(config)# no mab logging verbose
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands	Command	Description
	<b>no authentication logging verbose</b>	Filters details from authentication system messages.
	<b>no dot1x logging verbose</b>	Filters details from 802.1x system messages.
	<b>no mab logging verbose</b>	Filters details from MAC authentication bypass (MAB) system messages.

# parameter-map type subscriber attribute-to-service

To configure parameter map, use the **parameter-map type subscriber attribute-to-service** command.

**parameter-map type subscriber attribute-to-service** *parameter-map-name*

**no parameter-map type subscriber attribute-to-service** *parameter-map-name*

## Syntax Description

<i>parameter-map-name</i>	Specifies parameter map type.
---------------------------	-------------------------------

## Command Default

None

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

## Usage Guidelines

None

## Examples

The following example shows how to configure parameter map:

```
Controller#configure terminal
Controller(config)#parameter-map type subscriber attribute-to-service Aironet-Policy-para
```



## parameter map type webauth

To define a parameter map for web authentication, use the **parameter-map type webauth** command in global configuration mode. To delete a parameter map, use the **no** form of this command.

```
parameter map type webauth { parameter-map-name | { banner | consent | custom-page | exit | max-http-conns | no | redirect | timeout | type } | global | { banner | custom-page | exit | max-http-conns | intercept-https-enable | no | ratelimit | redirect | timeout | virtual-ip | watch-list } }
```

### Syntax Description

<i>parameter-map-name</i>	Defines a parameter map name for web authentication.
<b>global</b>	Defines global parameters for web authentication.
<b>banner</b>	Specifies banner file or text.
<b>custom-page</b>	Specifies custom page - login, expired, success or failure page.
<b>exit</b>	Exits from <b>parameter-map params</b> configuration mode.
<b>max-http-conns</b>	Specifies maximum number of HTTP connections per clients.
<b>intercept-https-enable</b>	Enables intercept of HTTPS traffic.
<b>no</b>	Negates a command or set its defaults.
<b>ratelimit</b>	Specifies rate limit on number of web authentication sessions.
<b>redirect</b>	Redirects the URL.
<b>timeout</b>	Specifies timeout for the initial state of web authentication.
<b>virtual-ip</b>	Specifies virtual IP address.
<b>watch-list</b>	Specifies watch list of web authentication clients.
<b>consent</b>	Specifies consent parameters.

### Command Default

A parameter map for web authentication is not defined.

### Command Modes

Global configuration

### Command History

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

### Usage Guidelines

Use the **parameter-map type webauth** command to define a parameter map for web authentication. A parameter map allows you to specify parameters that control the behavior of actions configured under a policy map with the authenticate using **webauth** command.

A global parameter map contains system-wide parameters. This parameter map is not attached to the web authentication action and has parameters for both web authentication and consent. The global parameter map is automatically applied to the authentication action. If you explicitly apply a named parameter map, and there are parameters that are common to both the global and named parameter map, the global parameter map configuration takes precedence.

The configuration parameters supported for a global parameter map defined with the global keyword are different from the parameters supported for a named parameter map defined with the *parameter-map-name* argument.

### Examples

The following example shows how to configure a parameter map named PMAP\_2, which is used by the control policy named POLICY\_1 to authenticate users:

```
Controller(config)# parameter map type webauth global
```

## passthrou-domain-list name

To configure a domain name list of domains with DNS snooping, use the **passthrou-domain-list name** command in global configuration.

**passthrou-domain-list** *name*

### Syntax Description

<i>name</i>	Configures the domain name list.
-------------	----------------------------------

### Command Default

None

### Command Modes

Global configuration.

### Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

### Examples

This example shows how to configure a domain name list of domains with DNS snooping:

```
Controller(config)# passthrou-domain-list name abc  
Controller(config-fqdn-acl-domains)# match google
```

## permit (MAC access-list configuration)

To allow non-IP traffic to be forwarded if the conditions are matched, use the **permit** MAC access-list configuration command on the switch stack or on a standalone switch. To remove a permit condition from the extended MAC access list, use the **no** form of this command.

```
{permit {any | hostsrc-MAC-addr | src-MAC-addr mask} {any | hostdst-MAC-addr | dst-MAC-addr mask}
[type mask | aarp | amber | appletalk | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042
| lat | lavc-sca | lsaplsap mask | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip
| xns-idp][coscos]
```

```
nopermit {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr | dst-MAC-addr mask}
[type mask | aarp | amber | appletalk | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042
| lat | lavc-sca | lsap lsap mask | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip
| xns-idp][coscos]
```

### Syntax Description

<b>any</b>	Denies any source or destination MAC address.
<b>host</b> <i>src-MAC-addr</i>   <i>src-MAC-addr mask</i>	Specifies a host MAC address and optional subnet mask. If the source address for a packet matches the defined address, non-IP traffic from that address is denied.
<b>host</b> <i>dst-MAC-addr</i>   <i>dst-MAC-addr mask</i>	Specifies a destination MAC address and optional subnet mask. If the destination address for a packet matches the defined address, non-IP traffic to that address is denied.
<i>type mask</i>	<p>(Optional) Specifies the EtherType number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet.</p> <ul style="list-style-type: none"> <li>• <i>type</i> is 0 to 65535, specified in hexadecimal.</li> <li>• <i>mask</i> is a mask of don't care bits applied to the EtherType before testing for a match.</li> </ul>
<b>aarp</b>	(Optional) Specifies EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
<b>amber</b>	(Optional) Specifies EtherType DEC-Amber.
<b>appletalk</b>	(Optional) Specifies EtherType AppleTalk/EtherTalk.
<b>dec-spanning</b>	(Optional) Specifies EtherType Digital Equipment Corporation (DEC) spanning tree.
<b>decnet-iv</b>	(Optional) Specifies EtherType DECnet Phase IV protocol.
<b>diagnostic</b>	(Optional) Specifies EtherType DEC-Diagnostic.

<b>dsm</b>	(Optional) Specifies EtherType DEC-DSM.
<b>etype-6000</b>	(Optional) Specifies EtherType 0x6000.
<b>etype-8042</b>	(Optional) Specifies EtherType 0x8042.
<b>lat</b>	(Optional) Specifies EtherType DEC-LAT.
<b>lavc-sca</b>	(Optional) Specifies EtherType DEC-LAVC-SCA.
<b>lsap</b> <i>lsap-number mask</i>	(Optional) Specifies the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet.  The <i>mask</i> is a mask of don't care bits applied to the LSAP number before testing for a match.
<b>mop-console</b>	(Optional) Specifies EtherType DEC-MOP Remote Console.
<b>mop-dump</b>	(Optional) Specifies EtherType DEC-MOP Dump.
<b>msdos</b>	(Optional) Specifies EtherType DEC-MSDOS.
<b>mumps</b>	(Optional) Specifies EtherType DEC-MUMPS.
<b>netbios</b>	(Optional) Specifies EtherType DEC- Network Basic Input/Output System (NetBIOS).
<b>vines-echo</b>	(Optional) Specifies EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
<b>vines-ip</b>	(Optional) Specifies EtherType VINES IP.
<b>xns-idp</b>	(Optional) Specifies EtherType Xerox Network Systems (XNS) protocol suite.
<b>cos</b> <i>cos</i>	(Optional) Specifies an arbitrary class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message appears if the <b>cos</b> option is configured.

**Command Default**

This command has no defaults. However, the default action for a MAC-named ACL is to deny.

**Command Modes**

Mac-access list configuration

**Command History**

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

## Usage Guidelines

Though visible in the command-line help strings, **appletalk** is not supported as a matching condition.

You enter MAC access-list configuration mode by using the **mac access-list extended** global configuration command.

If you use the **host** keyword, you cannot enter an address mask; if you do not use the **any** or **host** keywords, you must enter an address mask.

After an access control entry (ACE) is added to an access control list, an implied **deny-any-any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

To filter IPX traffic, you use the *type mask* or **lsap lsap mask** keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS terminology are listed in the following table.

**Table 5: IPX Filtering Criteria**

IPX Encapsulation Type		Filter Criterion
Cisco IOS Name	Novell Name	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

## Examples

This example shows how to define the MAC-named extended access list to allow NetBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is allowed.

```
Controller(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
```

This example shows how to remove the permit condition from the MAC-named extended access list:

```
Controller(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

This example permits all packets with EtherType 0x4321:

```
Controller(config-ext-macl)# permit any any 0x4321 0
```

You can verify your settings by entering the **show access-lists** privileged EXEC command.

**Related Commands**

Command	Description
<b>deny</b>	Denies from the MAC access-list configuration. Denies non-IP traffic to be forwarded if conditions are matched.
<b>mac access-list extended</b>	Creates an access list based on MAC addresses for non-IP traffic.
<b>show access-lists</b>	Displays access control lists configured on a switch.

# policy-map type control subscriber

To configure policy map type, use the **policy-map type control subscriber** command.

```
policy-map type control subscriber policy-map-name {event identity-update {match-all | match-first}
{class_number class {class_map_name | always} {do-all | do-until-failure | do-until-success} | action-index
map attribute-to-service table parameter-map-name}
```

## Syntax Description

<i>policy-map-name</i>	Policy map name.
<b>event identity-update { match-all   match-first}</b>	Match criteria to policy map.
<i>class_number</i>	Local profiling policy class map number.
<i>class_map_name</i>	Class map name.
<b>always</b>	Executes without doing any matching but return success.
<b>do-all</b>	Executes all the actions.
<b>do-until-failure</b>	Execute all the actions until any match failure is encountered. This is the default value.
<b>do-until-success</b>	Execute all the actions until any match success happens.
<i>action-index</i>	Parameter map table index.
<i>parameter-map-name</i>	Parameter map name.

## Command Default

**do-until-failure**

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

## Usage Guidelines

None



## Examples

The following example shows how to configure policy map:

```
Controller#configure terminal
Controller(config)#policy-map type control subscriber Aironet-Policy
Controller(config-policy-map)#event identity-update match-all
Controller(config-class-control-policymap)#1 class local_policy1_class do-until-success
Controller(config-policy-map)#10 map attribute-to-service table Aironet-Policy-para
```

## protocol (IPv6 snooping)

To specify that addresses should be gleaned with Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP), or to associate the protocol with an IPv6 prefix list, use the **protocol** command. To disable address glean with DHCP or NDP, use the **no** form of the command.

**protocol** {**dhcp** | **ndp**}

**no protocol** {**dhcp** | **ndp**}

### Syntax Description

<b>dhcp</b>	Specifies that addresses should be gleaned in Dynamic Host Configuration Protocol (DHCP) packets.
<b>ndp</b>	Specifies that addresses should be gleaned in Neighbor Discovery Protocol (NDP) packets.

### Command Default

Snooping and recovery are attempted using both DHCP and NDP.

### Command Modes

IPv6 snooping configuration mode

### Command History

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

### Usage Guidelines

If an address does not match the prefix list associated with DHCP or NDP, then control packets will be dropped and recovery of the binding table entry will not be attempted with that protocol.

- Using the **no protocol {dhcp | ndp}** command indicates that a protocol will not be used for snooping or glean.
- If the **no protocol dhcp** command is used, DHCP can still be used for binding table recovery.
- Data glean can recover with DHCP and NDP, though destination guard will only recovery through DHCP.

### Examples

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and configure the port to use DHCP to glean addresses:

```
Controller(config)# ipv6 snooping policy policy1
Controller(config-ipv6-snooping)# protocol dhcp
```

# radius server

To configure the RADIUS server, use the **radius server** command in global configuration mode.

**radius server** *server-name*

## Syntax Description

*server-name*

RADIUS server name.

## Command Default

None

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

None

## Examples

The following example shows how to configure a radius server:

```
Controller(config)# radius server ISE
```

## security level (IPv6 snooping)

To specify the level of security enforced, use the **security-level** command in IPv6 snooping policy configuration mode.

**security level** {glean | guard | inspect}

### Syntax Description

<b>glean</b>	Extracts addresses from the messages and installs them into the binding table without performing any verification.
<b>guard</b>	Performs both glean and inspect. Additionally, RA and DHCP server messages are rejected unless they are received on a trusted port or another policy authorizes them.
<b>inspect</b>	Validates messages for consistency and conformance; in particular, address ownership is enforced. Invalid messages are dropped.

### Command Default

The default security level is guard.

### Command Modes

IPv6 snooping configuration

### Command History

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

### Examples

This example shows how to define an IPv6 snooping policy name as policy1, place the device in IPv6 snooping configuration mode, and configure the security level as inspect:

```
Controller(config)# ipv6 snooping policy policy1
Controller(config-ipv6-snooping)# security-level inspect
```

# security web-auth

To configure web authentication on a WLAN, use the **security web-auth** command in WLAN configuration mode.

**security web-auth** { **authentication-list** *authentication-list-name* | **parameter-map** *parameter-map-name* }

## Syntax Description

<i>authentication-list-name</i>	Authentication list name from AAA server or RADIUS server.
<i>parameter-map-name</i>	Parameter map name.

## Command Default

None

## Command Modes

WLAN configuration

## Command History

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

## Usage Guidelines

None

## Examples

The following example shows how to configure security web authentication on a WLAN:

```
Controller (config)# wlan user_webauth 7 user_webauth
Controller(config-wlan)# client vlan user1
Controller(config-wlan)# no security wpa
Controller(config-wlan)# no security wpa akm dot1x
Controller(config-wlan)# no security wpa wpa2
Controller(config-wlan)# no security wpa wpa2 ciphers
Controller(config-wlan)# security web-auth
Controller(config-wlan)# security web-auth authentication-list local_webauth
Controller(config-wlan)# security web-auth parameter-map vit_web
Controller(config-wlan)# session-timeout 1800
```

# service-policy type control subscriber

To apply local policy on a WLAN, use the **service-policy type control subscriber** command.

**service-policy type control subscriber** *polycymapname* **profiling** {**local http** | **radius http**}

## Syntax Description

<i>polycymapname</i>	Policy map name.
<b>profiling local http</b>	Enables only profiling of devices based on HTTP protocol.
<b>profiling local http</b>	Enables only profiling of devices on ISE.

## Command Default

None

## Command Modes

WLAN configuration.

## Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

## Usage Guidelines

None

## Examples

This example shows how to apply local policy for a device on a WLAN:

```
Controller#configure terminal
Controller#wlan-wlan1
Controller(config-wlan)#service-policy type control subscriber Aironet-Policy
Controller(config-wlan)#profiling local http
Controller(config-wlan)#no shutdown
Controller(config-wlan)#end
```

# service-template

To configure service template, use the **service-template** command.

**service-template** *service-template-name* {**access-group** *acl\_list* | **vlan** *vlan\_id* | **absolute-timer** *seconds* | **service-policy qos** {**input** | **output**}}

## Syntax Description

<i>service-template-name</i>	Name of the service template.
<i>acl_list</i>	Access list name to be applied.
<i>vlan_id</i>	VLAN ID. The VLAN ID value ranges from 1 to 4094.
<i>seconds</i>	Session timeout value for service template. The session timeout value ranges from 1 to 65535 seconds.
<b>service-policy qos</b> { <b>input</b>   <b>output</b> }	QoS policies for client.

## Command Default

None

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

## Usage Guidelines

None

## Examples

The following example shows how to configure service template:

```
Controller#configure terminal
Controller(config)#service-template cisco-phone-template
Controller(config-service-template)#access-group foo-acl
Controller(config-service-template)#vlan 100
Controller(config-service-template)#service-policy qos input foo-qos
Controller(config-service-template)#end
```

# session-timeout

To configure session timeout for clients associated to a WLAN, use the **session-timeout** command in WLAN configuration mode.

**session-timeout** *seconds*

## Syntax Description

<i>seconds</i>	Session timeout for clients associated to a WLAN.  A value of zero (0) is equivalent to no timeout. The range is from 300 to 86400 seconds.
----------------	---

## Command Default

None

## Command Modes

WLAN configuration

## Command History

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

## Usage Guidelines

None

## Examples

The following example shows how to configure session timeout for clients associated to a WLAN for local web authentication:

```
Controller (config)# wlan user_webauth 7 user_webauth
Controller(config-wlan)# client vlan user1
Controller(config-wlan)# no security wpa
Controller(config-wlan)# no security wpa akm dot1x
Controller(config-wlan)# no security wpa wpa2
Controller(config-wlan)# no security wpa wpa2 ciphers
Controller(config-wlan)# security web-auth
Controller(config-wlan)# security web-auth authentication-list local_webauth
Controller(config-wlan)# security web-auth parameter-map vit_web
Controller(config-wlan)# session-timeout 1800
```



# show aaa clients

To show AAA client statistics, use the **show aaa clients** command.

**show aaa clients [detailed]**

## Syntax Description

<b>detailed</b>	(Optional) Shows detailed AAA client statistics.
-----------------	--

## Command Modes

User EXEC

## Command History

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

## Examples

This is an example of output from the **show aaa clients** command:

```
Controller# show aaa clients
Dropped request packets: 0
```

# show aaa command handler

To show AAA command handler statistics, use the **show aaa command handler** command.

**show aaa command handler**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Command Modes</b>	User EXEC
----------------------	-----------

<b>Command History</b>	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

<b>Examples</b>	This is an example of output from the <b>show aaa command handler</b> command:
-----------------	--

```
Controller# show aaa command handler

AAA Command Handler Statistics:
  account-logon: 0, account-logout: 0
  account-query: 0, pod: 0
  service-logon: 0, service-logout: 0
  user-profile-push: 0, session-state-log: 0
  reauthenticate: 0, bounce-host-port: 0
  disable-host-port: 0, update-rbacl: 0
  update-sgt: 0, update-cts-policies: 0
  invalid commands: 0
  async message not sent: 0
```

# show aaa local

To show AAA local method options, use the **show aaa local** command.

**show aaa local** {*netuser* {*name* | **all**} | **statistics** | **user lockout**}

## Syntax Description

<b>netuser</b>	Specifies the AAA local network or guest user database.
<i>name</i>	Network user name.
<b>all</b>	Specifies the network and guest user information.
<b>statistics</b>	Displays statistics for local authentication.
<b>user lockout</b>	Specifies the AAA local locked-out user.

## Command Modes

User EXEC

## Command History

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

## Examples

This is an example of output from the **show aaa local statistics** command:

```

Controller# show aaa local statistics


Local EAP statistics

EAP Method          Success      Fail
-----
Unknown              0            0
EAP-MD5               0            0
EAP-GTC              0            0
LEAP                  0            0
PEAP                  0            0
EAP-TLS               0            0
EAP-MSCHAPV2         0            0
EAP-FAST              0            0

Requests received from AAA:                0
Responses returned from EAP:               0
Requests dropped (no EAP AVP):              0
Requests dropped (other reasons):            0
Authentication timeouts from EAP:           0

Credential request statistics
Requests sent to backend:                    0
Requests failed (unable to send):            0
Authorization results received

```

 show aaa local

```
Success:          0
Fail:             0
```

# show aaa servers

To shows all AAA servers as seen by the AAA server MIB, use the **show aaa servers** command.

**show aaa servers** [ **private**|**public**[[**detailed**]]

## Syntax Description

<b>detailed</b>	(Optional) Displays private AAA servers as seen by the AAA Server MIB.
<b>public</b>	(Optional) Displays public AAA servers as seen by the AAA Server MIB.
<b>detailed</b>	(Optional) Displays detailed AAA server statistics.

## Command Modes

User EXEC

## Command History

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

## Examples

This is an example of output from the **show aaa servers** command:

```
Controller# show aaa servers
RADIUS: id 1, priority 1, host 172.20.128.2, auth-port 1645, acct-port 1646
State: current UP, duration 9s, previous duration 0s
Dead: total time 0s, count 0
Quarantined: No
Authen: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Author: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Account: request 0, timeouts 0, failover 0, retransmission 0
Request: start 0, interim 0, stop 0
Response: start 0, interim 0, stop 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Elapsed time since counters last cleared: 0m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
```

# show aaa sessions

To show AAA sessions as seen by the AAA Session MIB, use the **show aaa sessions** command.

**show aaa sessions**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC

## Command History

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

## Examples

This is an example of output from the **show aaa sessions** command:

```
Controller# show aaa sessions
Total sessions since last reload: 7
Session Id: 4007
  Unique Id: 4025
  User Name: *not available*
  IP Address: 0.0.0.0
  Idle Time: 0
  CT Call Handle: 0
```

# show access-session

To display details of access session for clients, use the **show access-session** command in privileged EXEC mode.

**show access-session** {*cache* | *mac**mac-address* {*details* | *policy* } }

<b>Syntax Description</b>	<table> <tr> <td><i>mac-address</i></td><td>MAC address of the client.</td></tr> </table>	<i>mac-address</i>	MAC address of the client.		
<i>mac-address</i>	MAC address of the client.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC				
<b>Command History</b>	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>Cisco IOS XE 3E</td><td>This command was introduced.</td></tr> </table>	Release	Modification	Cisco IOS XE 3E	This command was introduced.
Release	Modification				
Cisco IOS XE 3E	This command was introduced.				

## Examples

The following is a sample output of the **show access-session** command:

```
Controller# show access-session
Interface    MAC Address      Method  Domain  Status  Fg  Session ID
Tel1/0/1     0027.0c06.2783  N/A     UNKNOWN Unauth   090C895F00000FAB0001995F
Ca13         20aa.4b60.00da  dot1x   DATA   Auth     090c895f53b174cc000000c9
```

Session count = 2

The following is a sample output of the **show access-session cache** command:

```
Controller# show access-session cache
Access session cache details
-----
MAC Address:  8853.9528.93eb
Device-type:  Apple-Device
User-role:
Protocol-map: 0x00000001
-----
MAC Address:  0040.96b9.4b27
Device-type:  Microsoft-Workstation
User-role:    employee
Protocol-map: 0x00000009
```

The following is a sample output of the **show access-session mac 20aa.4b60.00da policy** command:

```
Controller# show access-session mac 20aa.4b60.00da policy

Interface:  Capwap13
IIF-ID:     0x7A4180000000F6
MAC Address: 20aa.4b60.00da
IPv6 Address: FE80::22AA:4BFF:FE60:DA
IPv4 Address: 9.12.139.107
User-Name:   joseph
User-role:    employee
```

```
Device-type: WindowsXP-Workstation
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Common Session ID: 090c895f53b174cc000000c9
Acct Session ID: Unknown
Handle: 0x1A0000C0
Current Policy: test-poll

Local Policies:
Service Template: test2 (priority 150)
Filter-ID: josephallow
Input QoS:: http-ingress
Vlan Group: Vlan: 139

Resultant Policies:
Filter-ID: josephallow
Input QoS:: http-ingress
Vlan Group: Vlan: 139

Method status list:
Method      State
dot1x      Authc Success
```



# show access-session fqdn

To display the FQDN configurations, use the **show access-session fqdn** command in EXEC mode.

**show access-session fqdn** {**passthru-domain-list** | **list-domain** *list-domain* | **fqdn-maps**}

## Syntax Description

<b>passthru-domain-list</b>	Displays the lists of domains for the access session.
<b>list-domain</b> <i>list-domain</i>	Displays all the domains in the list.
<b>fqdn-maps</b>	Displays mapping of FQDN ACL to the domain name list.

## Command Default

None

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

## Examples

This example shows how to display the lists of domains for the access session:

```
Controller# sh access-sess fqdn passthru-domain-list
Domain-name-lists
-----
abc
```

This example shows how to display the domains in the list for the access session:

```
Controller# sh access-sess fqdn list-domain abc
Domain's associated with the list
-----
abc
google
```

# show access session interface

To display policies applied to an interface of access session, use the **show access session interface** command in EXEC mode.

**show access session interface** *interface-name* **details**

## Syntax Description

<i>interface-name</i>	Specifies the interface number.
<b>details</b>	Displays detailed information about the policies applied to an interface.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

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

## Usage Guidelines

You can use this command to check the ACLs present on an interface (for example, client VLAN interface) when the ACL is pushed dynamically from ISE.

## Examples

This example shows how to display the policies applied to an interface:

```

Controller# show access session interface Ethernet0/0 details
Interface: Ethernet0/0
      MAC Address: aabb.cc01.ff00
      IPv6 Address: Unknown
      IPv4 Address: Unknown
      Status: Authorized
      Domain: DATA
      Oper host mode: multi-host
      Oper control dir: both
      Session timeout: N/A
      Common Session ID: 0D0102330000000F000CF07D
      Acct Session ID: Unknown
      Handle: 0x3C000004
      Current Policy: MY_POLICY1

Server Policies:
FQDN ACL Handle           : Hex 0x8000003      Dec 134217731
FQDN ACL Domain Name      : abc
Domain Names              : google google. yahoo
IP Address                : 192.0.2.1 192.0.2.2 192.0.2.3

```

# show device classifier attached detail

To display the latest classification for the client based on parameters such as MAC, DHCP, or HTTP on the controller, use the **show device classifier attached detail** command in privileged EXEC mode.

**show device classifier attached detail**

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

## Examples

The following is a sample output of the **show device classifier attached detail** command:

```
Controller# show device classifier attached detail
DC default profile file version supported = 1
```

Detail:

MAC_Address	Port_Id	Cert	Parent	Proto	ProfileType	Profile Name
Device_Name						
0027.0c06.2783	Te1/0/1	20	1	C	M	Default Cisco-Switch
cisco WS-C3750E-24PD						
20aa.4b60.00da	Ca13	20	1	D M	Default	Linksys-Device
MSFT 5.0						

# show authentication sessions

To display information about current Auth Manager sessions, use the **show authentication sessions** command.

**show authentication sessions** [**database**][**handle** *handle-id* [**details**]][**interface** *type number* [**details**][**mac** *mac-address* [**interface** *type number*][**method** *method-name* [**interface** *type number* [**details**] [**session-id** *session-id* [**details**]]]

## Syntax Description

<b>database</b>	(Optional) Shows only data stored in session database.
<b>handle</b> <i>handle-id</i>	(Optional) Specifies the particular handle for which Auth Manager information is to be displayed.
<b>details</b>	(Optional) Shows detailed information.
<b>interface</b> <i>type number</i>	(Optional) Specifies a particular interface type and number for which Auth Manager information is to be displayed.
<b>mac</b> <i>mac-address</i>	(Optional) Specifies the particular MAC address for which you want to display information.
<b>method</b> <i>method-name</i>	(Optional) Specifies the particular authentication method for which Auth Manager information is to be displayed. If you specify a method ( <b>dot1x</b> , <b>mab</b> , or <b>webauth</b> ), you may also specify an interface.
<b>session-id</b> <i>session-id</i>	(Optional) Specifies the particular session for which Auth Manager information is to be displayed.

## Command Modes

User EXEC

## Command History

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

## Usage Guidelines

Use the **show authentication sessions** command to display information about all current Auth Manager sessions. To display information about specific Auth Manager sessions, use one or more of the keywords. This table shows the possible operating states for the reported authentication sessions.

**Table 6: Authentication Method States**

State	Description
Not run	The method has not run for this session.
Running	The method is running for this session.
Failed over	The method has failed and the next method is expected to provide a result.
Success	The method has provided a successful authentication result for the session.
Authc Failed	The method has provided a failed authentication result for the session.

This table shows the possible authentication methods.

**Table 7: Authentication Method States**

State	Description
dot1x	802.1X
mab	MAC authentication bypass
webauth	web authentication

## Examples

The following example shows how to display all authentication sessions on the switch:

```

Controller# show authentication sessions
Interface  MAC Address  Method  Domain  Status  Session ID
Gi1/0/48   0015.63b0.f676  dot1x   DATA   Authz Success  0A3462B1000000102983C05C
Gi1/0/5    000f.23c4.a401  mab     DATA   Authz Success  0A3462B10000000D24F80B58
Gi1/0/5    0014.bf5d.d26d  dot1x   DATA   Authz Success  0A3462B10000000E29811B94

```

The following example shows how to display all authentication sessions on an interface:

```

Controller# show authentication sessions interface gigabitethernet2/0/47
Interface: GigabitEthernet2/0/47
MAC Address: Unknown
IP Address: Unknown
Status: Authz Success
Domain: DATA
Oper host mode: multi-host
Oper control dir: both
Authorized By: Guest Vlan
Vlan Policy: 20
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A3462C80000000000002763C
Acct Session ID: 0x00000002

```

## show authentication sessions

```

                Handle: 0x25000000
Runnable methods list:
  Method  State
  mab     Failed over
  dot1x   Failed over
-----
                Interface: GigabitEthernet2/0/47
                MAC Address: 0005.5e7c.da05
                IP Address: Unknown
                User-Name: 00055e7cda05
                Status: Authz Success
                Domain: VOICE
                Oper host mode: multi-domain
                Oper control dir: both
                Authorized By: Authentication Server
                Session timeout: N/A
                Idle timeout: N/A
                Common Session ID: 0A3462C8000000010002A238
                Acct Session ID: 0x00000003
                Handle: 0x91000001
Runnable methods list:
  Method  State
  mab     Authc Success
  dot1x   Not run

```

# show cisp

To display CISP information for a specified interface, use the **show cisp** command in privileged EXEC mode.

**show cisp** {[clients | interface *interface-id*] | registrations | summary}

## Syntax Description

<b>clients</b>	(Optional) Display CISP client details.
<b>interface</b> <i>interface-id</i>	(Optional) Display CISP information about the specified interface. Valid interfaces include physical ports and port channels.
<b>registrations</b>	Displays CISP registrations.
<b>summary</b>	(Optional) Displays CISP summary.

## Command Modes

Privileged EXEC

## Command History

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

## Examples

This example shows output from the **show cisp interface** command:

```
Controller# show cisp interface fast 0
CISP not enabled on specified interface
```

This example shows output from the **show cisp registration** command:

```
Controller# show cisp registrations
Interface(s) with CISP registered user(s):
-----
Fa1/0/13
Auth Mgr (Authenticator)
Gi2/0/1
Auth Mgr (Authenticator)
Gi2/0/2
Auth Mgr (Authenticator)
Gi2/0/3
Auth Mgr (Authenticator)
Gi2/0/5
Auth Mgr (Authenticator)
Gi2/0/9
Auth Mgr (Authenticator)
Gi2/0/11
Auth Mgr (Authenticator)
Gi2/0/13
Auth Mgr (Authenticator)
Gi3/0/3
Gi3/0/5
```

Gi3/0/23

**Related Commands**

Command	Description
<b>cisp enable</b>	Enable Client Information Signalling Protocol (CISP)
<b>dot1x credentials</b> <i>profile</i>	Configure a profile on a supplicant switch



# show dot1x

To display IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified port, use the **show dot1x** command in user EXEC mode.

**show dot1x** [**all** [**count** | **details** | **statistics** | **summary**]] [**interface type number** [**details** | **statistics**]] [**statistics**]

## Syntax Description

<b>all</b>	(Optional) Displays the IEEE 802.1x information for all interfaces.
<b>count</b>	(Optional) Displays total number of authorized and unauthorized clients.
<b>details</b>	(Optional) Displays the IEEE 802.1x interface details.
<b>statistics</b>	(Optional) Displays the IEEE 802.1x statistics for all interfaces.
<b>summary</b>	(Optional) Displays the IEEE 802.1x summary for all interfaces.
<b>interface type number</b>	(Optional) Displays the IEEE 802.1x status for the specified port.

## Command Modes

User EXEC

## Command History

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

## Examples

This is an example of output from the **show dot1x all** command:

```
Controller# show dot1x all
Sysauthcontrol          Enabled
Dot1x Protocol Version  3
```

This is an example of output from the **show dot1x all count** command:

```
Controller# show dot1x all count
Number of Dot1x sessions
-----
Authorized Clients      = 0
Unauthorized Clients    = 0
Total No of Client      = 0
```

This is an example of output from the **show dot1x all statistics** command:

```
Controller# show dot1x statistics
Dot1x Global Statistics for
```

```
-----  
RxStart = 0      RxLogoff = 0      RxResp = 0      RxRespID = 0  
RxReq = 0        RxInvalid = 0      RxLenErr = 0  
RxTotal = 0  
  
TxStart = 0      TxLogoff = 0      TxResp = 0  
TxReq = 0        ReTxReq = 0      ReTxReqFail = 0  
TxReqID = 0      ReTxReqID = 0    ReTxReqIDFail = 0  
TxTotal = 0
```

## show eap pac peer

To display stored Protected Access Credentials (PAC) for Extensible Authentication Protocol (EAP) Flexible Authentication via Secure Tunneling (FAST) peers, use the **show eap pac peer** command in privileged EXEC mode.

**show eap pac peer**

### Syntax Description

This command has no arguments or keywords.

### Command Modes

Privileged EXEC

### Command History

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

### Examples

This is an example of output from the **show eap pac peers** privileged EXEC command:

```
Controller> show eap pac peers
No PACs stored
```

### Related Commands

Command	Description
<b>clear eap sessions</b>	Clears EAP session information for the switch or for the specified port.

# show fips authorization-key

To display information about the FIPS authorization key configured on the controller, use the **show fips authorization-key** command in privileged EXEC mode.

**show fips authorization-key**

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

## Examples

The following is a sample output of the **show fips authorization-key** command:

```
Controller# show fips authorization-key
FIPS: Stored key (16) : 12345678901234567890123456789012
```

# show fips status

To display the status of the FIPS mode, use the **show fips status** command in privileged EXEC mode.

**show fips status**

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

## Examples

The following is a sample output of the **show fips status** command:

```
Controller# show fips status
Switch and Stacking are running in fips mode
```

# show ip dhcp snooping statistics

To display DHCP snooping statistics in summary or detail form, use the **show ip dhcp snooping statistics** command in user EXEC mode.

**show ip dhcp snooping statistics [detail ]**

## Syntax Description

<b>detail</b>	(Optional) Displays detailed statistics information.
---------------	--

## Command Modes

User EXEC

## Command History

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

## Usage Guidelines

In a switch stack, all statistics are generated on the stack master. If a new active switch is elected, the statistics counters reset.

## Examples

This is an example of output from the **show ip dhcp snooping statistics** command:

```
Controller> show ip dhcp snooping statistics

Packets Forwarded                = 0
Packets Dropped                  = 0
Packets Dropped From untrusted ports = 0
```

This is an example of output from the **show ip dhcp snooping statistics detail** command:

```
Controller> show ip dhcp snooping statistics detail

Packets Processed by DHCP Snooping          = 0
Packets Dropped Because
  IDB not known                             = 0
  Queue full                                = 0
  Interface is in errdisabled                 = 0
  Rate limit exceeded                        = 0
  Received on untrusted ports                 = 0
  Nonzero giaddr                             = 0
  Source mac not equal to chaddr              = 0
  Binding mismatch                           = 0
  Insertion of opt82 fail                     = 0
  Interface Down                             = 0
  Unknown output interface                   = 0
  Reply output port equal to input port       = 0
  Packet denied by platform                  = 0
```

This table shows the DHCP snooping statistics and their descriptions:

**Table 8: DHCP Snooping Statistics**

DHCP Snooping Statistic	Description
Packets Processed by DHCP Snooping	Total number of packets handled by DHCP snooping, including forwarded and dropped packets.
Packets Dropped Because IDB not known	Number of errors when the input interface of the packet cannot be determined.
Queue full	Number of errors when an internal queue used to process the packets is full. This might happen if DHCP packets are received at an excessively high rate and rate limiting is not enabled on the ingress ports.
Interface is in errdisabled	Number of times a packet was received on a port that has been marked as error disabled. This might happen if packets are in the processing queue when a port is put into the error-disabled state and those packets are subsequently processed.
Rate limit exceeded	Number of times the rate limit configured on the port was exceeded and the interface was put into the error-disabled state.
Received on untrusted ports	Number of times a DHCP server packet (OFFER, ACK, NAK, or LEASEQUERY) was received on an untrusted port and was dropped.
Nonzero giaddr	Number of times the relay agent address field (giaddr) in the DHCP packet received on an untrusted port was not zero, or the <b>no ip dhcp snooping information option allow-untrusted</b> global configuration command is not configured and a packet received on an untrusted port contained option-82 data.
Source mac not equal to chaddr	Number of times the client MAC address field of the DHCP packet (chaddr) does not match the packet source MAC address and the <b>ip dhcp snooping verify mac-address</b> global configuration command is configured.
Binding mismatch	Number of times a RELEASE or DECLINE packet was received on a port that is different than the port in the binding for that MAC address-VLAN pair. This indicates someone might be trying to spoof the real client, or it could mean that the client has moved to another port on the switch and issued a RELEASE or DECLINE. The MAC address is taken from the chaddr field of the DHCP packet, not the source MAC address in the Ethernet header.
Insertion of opt82 fail	Number of times the option-82 insertion into a packet failed. The insertion might fail if the packet with the option-82 data exceeds the size of a single physical packet on the internet.

DHCP Snooping Statistic	Description
Interface Down	Number of times the packet is a reply to the DHCP relay agent, but the SVI interface for the relay agent is down. This is an unlikely error that occurs if the SVI goes down between sending the client request to the DHCP server and receiving the response.
Unknown output interface	Number of times the output interface for a DHCP reply packet cannot be determined by either option-82 data or a lookup in the MAC address table. The packet is dropped. This can happen if option 82 is not used and the client MAC address has aged out. If IPSG is enabled with the port-security option and option 82 is not enabled, the MAC address of the client is not learned, and the reply packets will be dropped.
Reply output port equal to input port	Number of times the output port for a DHCP reply packet is the same as the input port, causing a possible loop. Indicates a possible network misconfiguration or misuse of trust settings on ports.
Packet denied by platform	Number of times the packet has been denied by a platform-specific registry.



# show nmsp

To display the Network Mobility Services Protocol (NMSP) configuration settings, use the **show nmsp** command.

**show nmsp** {**attachment** | {**suppress interfaces**}| **capability**| **notification interval**| **statistics** {**connection**| **summary**}| **status**| **subscription detail** [*ip-addr* ]| **summary**}

## Syntax Description

<b>attachment suppress interfaces</b>	Displays attachment suppress interfaces.
<b>capability</b>	Displays NMSP capabilities.
<b>notification interval</b>	Displays the NMSP notification interval.
<b>statistics connection</b>	Displays all connection-specific counters.
<b>statistics summary</b>	Displays the NMSP counters.
<b>status</b>	Displays status of active NMSP connections.
<b>subscription detail</b> <i>ip-addr</i>	The details are only for the NMSP services subscribed to by a specific IP address.
<b>subscription summary</b>	Displays details for all of the NMSP services to which the controller is subscribed. The details are only for the NMSP services subscribed to by a specific IP address.

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

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

## Examples

The following is sample output from the **show nmsp notification interval** command:

```
Controller# show nmsp notification interval
NMSP Notification Intervals
-----
RSSI Interval:
  Client           : 2 sec
  RFID             : 2 sec
```

```

Rogue AP           : 2 sec
Rogue Client       : 2 sec
Attachment Interval : 30 sec
Location Interval  : 30 sec

```

The following is sample output from the **show nmsp capability** command:

```

Controller# show nmsp capability
Service          Subservice
-----
RSSI              Mobile Station, Tags, Rogue
Spectrum          Subscription
Info              Mobile Station, Rogue
Statistics        Mobile Station, Tags
Attachment        Wired Station
Location          Subscription
AP Monitor        Subscription
IDS Services      WIPS
On Demand Services Device Info

```

# show radius server-group

To display properties for the RADIUS server group, use the **show radius server-group** command.

**show radius server-group** {*name* | **all**}

## Syntax Description

<i>name</i>	Name of the server group. The character string used to name the group of servers must be defined using the <b>aaa group server radius</b> command.
<b>all</b>	Displays properties for all of the server groups.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

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

## Usage Guidelines

Use the **show radius server-group** command to display the server groups that you defined by using the **aaa group server radius** command.

## Examples

This is an example of output from the **show radius server-group all** command:

```
Controller# show radius server-group all
Server group radius
  Sharecount = 1  sg_unconfigured = FALSE
  Type = standard  Memlocks = 1
```

This table describes the significant fields shown in the display.

**Table 9: show radius server-group command Field Descriptions**

Field	Description
Server group	Name of the server group.
Sharecount	Number of method lists that are sharing this server group. For example, if one method list uses a particular server group, the sharecount would be 1. If two method lists use the same server group, the sharecount would be 2.

Field	Description
sg_unconfigured	Server group has been unconfigured.
Type	The type can be either standard or nonstandard. The type indicates whether the servers in the group accept nonstandard attributes. If all servers within the group are configured with the nonstandard option, the type will be shown as "nonstandard".
Memlocks	An internal reference count for the server-group structure that is in memory. The number represents how many internal data structure packets or transactions are holding references to this server group. Memlocks is used internally for memory management purposes.

## show vlan access-map

To display information about a particular VLAN access map or for all VLAN access maps, use the **show vlan access-map** command in privileged EXEC mode.

**show vlan access-map** [*map-name*]

<b>Syntax Description</b>	<i>map-name</i> (Optional) Name of a specific VLAN access map.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 3.2SE	This command was introduced.

### Examples

This is an example of output from the **show vlan access-map** command:

```
Controller# show vlan access-map
Vlan access-map "vmap4" 10
  Match clauses:
    ip address: a12
  Action:
    forward
Vlan access-map "vmap4" 20
  Match clauses:
    ip address: a12
  Action:
    forward
```

# show vlan group

To display the VLANs that are mapped to VLAN groups, use the **show vlan group** command in privileged EXEC mode.

**show vlan group** [**group-name** *vlan-group-name* [**user\_count**]]

## Syntax Description

<b>group-name</b> <i>vlan-group-name</i>	(Optional) Displays the VLANs mapped to the specified VLAN group.
<b>user_count</b>	(Optional) Displays the number of users in each VLAN mapped to a specified VLAN group.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

The **show vlan group** command displays the existing VLAN groups and lists the VLANs and VLAN ranges that are members of each VLAN group. If you enter the **group-name** keyword, only the members of the specified VLAN group are displayed.

## Examples

This example shows how to display the members of a specified VLAN group:

# show wireless wps rogue ap summary

To display a list of all rogue access points detected by the controller, use the **show wireless wps rogue ap summary** command.

**show wireless wps rogue ap summary**

## Command Default

None.

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

None.

## Examples

This example shows how to display a list of all rogue access points detected by the controller:

```
Controller# show wireless wps rogue ap summary
Rogue Location Discovery Protocol      : Disabled
Rogue on wire Auto-Contain            : Disabled
Rogue using our SSID Auto-Contain     : Disabled
Valid client on rogue AP Auto-Contain : Disabled
Rogue AP timeout                      : 1200
Rogue Detection Report Interval       : 10
Rogue AP minimum RSSI                 : -128
Rogue AP minimum transient time       : 0
```

Number of rogue APs detected : 624

MAC Address	Classification	# APs	# Clients	Last Heard
0018.e78d.250a	Unclassified	1	0	Thu Jul 25 05:04:01 2013
0019.0705.d5bc	Unclassified	1	0	Thu Jul 25 05:16:26 2013
0019.0705.d5bd	Unclassified	1	0	Thu Jul 25 05:10:28 2013
0019.0705.d5bf	Unclassified	1	0	Thu Jul 25 05:16:26 2013

# show wireless wps rogue client detailed

To view the detailed information of a specific rogue client, use the **show wireless wps rogue client detailed** *client-mac* command.

**show wireless wps rogue client detailed** *client-mac*

Syntax Description	
<i>client-mac</i>	MAC address of the rogue client.

**Command Default** None.

**Command Modes** Privileged EXEC

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

**Usage Guidelines** None.

**Examples** This example shows how to display the detailed information for a specific rogue client:

```
Controller# show wireless wps rogue client detail 0024.d7f1.2558
Rogue BSSID                : 64d8.146f.379f
Rogue Radio Type           : 802.11n - 5GHz
State                      : Alert
First Time Rogue was Reported : Wed Aug  7 12:51:43 2013
Last Time Rogue was Reported  : Wed Aug  7 12:51:43 2013
Reported by
  AP 2
    MAC Address             : 3cce.7309.0370
    Name                    : AP3502-talwar-ccie
    Radio Type              : 802.11a
    RSSI                    : -42 dBm
    SNR                     : 47 dB
    Channel                 : 52
    Last reported by this AP : Wed Aug  7 12:51:43 2013
```



# show wireless wps rogue client summary

To display summary of WPS rogue clients, use the **show wireless wps rogue client summary** command.

**show wireless wps rogue client summary**

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

### Examples

The following displays the output of the **show wireless wps rogue client summary** command:

```
Controller# show wireless wps rogue client summary
Validate rogue clients against AAA : Disabled
Validate rogue clients against MSE : Enabled
Number of rogue clients detected : 0
```

# show wireless wps wips statistics

To display the current state of the Cisco Wireless Intrusion Prevention System (wIPS) operation on the controller, use the **show wireless wps wips statistics** command.

**show wireless wps wips statistics**

## Command Default

None.

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

None.

## Examples

This example shows how to display the statistics of the wIPS operation:

```
Controller# show wireless wps wips statistics
Policy Assignment Requests..... 1
Policy Assignment Responses..... 1
Policy Update Requests..... 0
Policy Update Responses..... 0
Policy Delete Requests..... 0
Policy Delete Responses..... 0
Alarm Updates..... 13572
Device Updates..... 8376
Device Update Requests..... 0
Device Update Responses..... 0
Forensic Updates..... 1001
Invalid WIPS Payloads..... 0
Invalid Messages Received..... 0
CAPWAP Enqueue failed ..... 0
NMSP Enqueue failed ..... 0
NMSP Transmitted Packets..... 22950
NMSP Transmit Packets Dropped..... 0
NMSP Largest Packet..... 1377
```

## show wireless wps wips summary

To display the adaptive Cisco Wireless Intrusion Prevention System (wIPS) configuration that the Wireless Control System (WCS) forwards to the controller, use the **show wireless wps wips summary** command.

**show wireless wps wips summary**

### Command Default

None.

### Command Modes

Privileged EXEC

### Command History

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

### Usage Guidelines

None.

### Examples

This example shows how to display a summary of the wIPS configuration:

```
Controller# show wireless wps wips summary
Policy Name..... Default
Policy Version..... 3
```

## tracking (IPv6 snooping)

To override the default tracking policy on a port, use the **tracking** command in IPv6 snooping policy configuration mode.

**tracking** {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]}

### Syntax Description

<b>enable</b>	Enables tracking.
<b>reachable-lifetime</b>	<p>(Optional) Specifies the maximum amount of time a reachable entry is considered to be directly or indirectly reachable without proof of reachability.</p> <ul style="list-style-type: none"> <li>The <b>reachable-lifetime</b> keyword can be used only with the <b>enable</b> keyword.</li> <li>Use of the <b>reachable-lifetime</b> keyword overrides the global reachable lifetime configured by the <b>ipv6 neighbor binding reachable-lifetime</b> command.</li> </ul>
<i>value</i>	Lifetime value, in seconds. The range is from 1 to 86400, and the default is 300.
<b>infinite</b>	Keeps an entry in a reachable or stale state for an infinite amount of time.
<b>disable</b>	Disables tracking.
<b>stale-lifetime</b>	<p>(Optional) Keeps the time entry in a stale state, which overwrites the global stale-lifetime configuration.</p> <ul style="list-style-type: none"> <li>The stale lifetime is 86,400 seconds.</li> <li>The <b>stale-lifetime</b> keyword can be used only with the <b>disable</b> keyword.</li> <li>Use of the <b>stale-lifetime</b> keyword overrides the global stale lifetime configured by the <b>ipv6 neighbor binding stale-lifetime</b> command.</li> </ul>

### Command Default

The time entry is kept in a reachable state.

### Command Modes

IPv6 snooping configuration

**Command History**

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

**Usage Guidelines**

The **tracking** command overrides the default tracking policy set by the **ipv6 neighbor tracking** command on the port on which this policy applies. This function is useful on trusted ports where, for example, you may not want to track entries but want an entry to stay in the binding table to prevent it from being stolen.

The **reachable-lifetime** keyword is the maximum time an entry will be considered reachable without proof of reachability, either directly through tracking or indirectly through IPv6 snooping. After the **reachable-lifetime** value is reached, the entry is moved to stale. Use of the **reachable-lifetime** keyword with the tracking command overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.

The **stale-lifetime** keyword is the maximum time an entry is kept in the table before it is deleted or the entry is proven to be reachable, either directly or indirectly. Use of the **reachable-lifetime** keyword with the **tracking** command overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

**Examples**

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and configure an entry to stay in the binding table for an infinite length of time on a trusted port:

```
Controller(config)# ipv6 snooping policy policy1
Controller(config-ipv6-snooping)# tracking disable stale-lifetime infinite
```

# trusted-port

To configure a port to become a trusted port, use the **trusted-port** command in IPv6 snooping policy mode or ND inspection policy configuration mode. To disable this function, use the **no** form of this command.

**trusted-port**

**no trusted-port**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No ports are trusted.

**Command Modes** ND inspection policy configuration  
IPv6 snooping configuration

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

**Usage Guidelines** When the **trusted-port** command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, to protect against address spoofing, messages are analyzed so that the binding information that they carry can be used to maintain the binding table. Bindings discovered from these ports will be considered more trustworthy than bindings received from ports that are not configured to be trusted.

**Examples** This example shows how to define an NDP policy name as policy1, place the switch in NDP inspection policy configuration mode, and configure the port to be trusted:

```
Controller(config)# ipv6 nd inspection policy1
Controller(config-nd-inspection)# trusted-port
```

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and configure the port to be trusted:

```
Controller(config)# ipv6 snooping policy policy1
Controller(config-ipv6-snooping)# trusted-port
```

# virtual-ip

To configure the virtual IPv4 address for web-based authentication clients, use the **virtual-ip ipv4** command in global configuration mode.

**virtual-ip ipv4** *virtual-ip-address*

## Syntax Description

*virtual-ip-address*

IPv4 address.

## Command Default

None

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

None

## Examples

The following example shows how to configure the virtual IPv4 address for web-based authentication clients:

```
Controller(config-params-parameter-map) # virtual-ip ipv4 172.16.16.16
```

# wireless mobility dtls secure-cipher

To set AES256 SHA1 or AES256 SHA2 as cipher for mobility control traffic, use the **wireless mobility dtls secure-cipher** command in global configuration mode.

**wireless mobility dtls secure-cipher**{AES256\_SHA1| AES256\_SHA2}

## Command Default

None

## Command Modes

Global Configuration

## Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

## Examples

The following example shows how to set AES256 SHA2as cipher for mobility control traffic on the controller:

```
Controller(config)# wireless mobility dtls secure-cipher AES256_SHA2
Enabling secure-cipher AES256_SHA2 will reset all
Mobility connections
Are you sure you want to continue? (y/n)[y]: y
Controller(config)#
```



# wireless security dot1x

To configure IEEE 802.1x global configurations, use the **wireless security dot1x** command.

```
wireless security dot1x [eapol-key {retries retries| timeout milliseconds}| group-key interval sec|
identity-request {retries retries| timeout seconds}| radius [call-station-id] {ap-macaddress|
ap-macaddress-ssid| ipaddress| macaddress}| request {retries retries| timeout seconds}| wep key {index
0| index 3}]
```

## Syntax Description

<b>eapol-key</b>	Configures eapol-key related parameters.
<b>retries</b> <i>retries</i>	(Optional) Specifies the maximum number of times (0 to 4 retries) that the controller retransmits an EAPOL (WPA) key message to a wireless client. The default value is 2.
<b>timeout</b> <i>milliseconds</i>	(Optional) Specifies the amount of time (200 to 5000 milliseconds) that the controller waits before retransmitting an EAPOL (WPA) key message to a wireless client using EAP or WPA/WPA-2 PSK. The default value is 1000 milliseconds.
<b>group-key interval</b> <i>sec</i>	Configures EAP-broadcast key renew interval time in seconds (120 to 86400 seconds).
<b>identity-request</b>	Configures EAP ID request related parameters.
<b>retries</b> <i>retries</i>	(Optional) Specifies the maximum number of times (0 to 4 retries) that the controller request the EAP ID. The default value is 2.
<b>timeout</b> <i>seconds</i>	(Optional) Specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting an EAP Identity Request message to a wireless client. The default value is 30 seconds.
<b>radius</b>	Configures radius messages.
<b>call-station-id</b>	(Optional) Configures Call-Station Id sent in radius messages.
<b>ap-macaddress</b>	Sets Call Station Id Type to the AP's MAC Address.
<b>ap-macaddress-ssid</b>	Sets Call Station Id Type to 'AP MAC address':'SSID'.
<b>ipaddress</b>	Sets Call Station Id Type to the system's IP Address.
<b>macaddress</b>	Sets Call Station Id Type to the system's MAC Address.
<b>request</b>	Configures EAP request related parameters.

<b>retries</b> <i>retries</i>	(Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the maximum number of times (0 to 20 retries) that the controller retransmits the message to a wireless client.  The default value is 2.
<b>timeout</b> <i>seconds</i>	(Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting the message to a wireless client.  The default value is 30 seconds.
<b>wep key</b>	Configures 802.1x WEP related paramters.
<b>index 0</b>	Specifies the WEP key index value as 0
<b>index 3</b>	Specifies the WEP key index value as 3

**Command Default**

Default for eapol-key-timeout: 1 second.  
Default for eapol-key-retries: 2 retries.

**Command Modes**

config

**Command History**

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

**Usage Guidelines**

None.

**Examples**

This example lists all the commands under **wireless security dot1x**.

```

Controller#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)#wireless security dot1x ?
  eapol-key          Configure eapol-key related parameters
  group-key          Configures EAP-broadcast key renew interval time in seconds
  identity-request    Configure EAP ID request related parameters
  radius             Configure radius messages
  request            Configure EAP request related parameters
  wep                Configure 802.1x WEP related parameters
  <cr>

```

# wireless security dot1x radius accounting mac-delimiter

To configure a MAC delimiter for called-station-ID or a calling-station-ID, use the **wireless security dot1x radius accounting mac-delimiter** command.

To remove MAC delimiter for a called-station-ID or a calling-station-ID, use the **no** form of the command.

**wireless security dot1x radius accounting mac-delimiter** {colon | hyphen | none | single-hyphen }

## Syntax Description

<b>colon</b>	Sets the delimiter to colon.
<b>hyphen</b>	Sets the delimiter to hyphen.
<b>none</b>	Disables delimiters.
<b>single-hyphen</b>	Sets the delimiters to single hyphen.

## Command Default

None

## Command Modes

Global Configuration Mode

## Command History

Release	Modification
Cisco IOS XE 3.6.0 E	This command was introduced.

## Examples

This example shows how to configure a MAC delimiter for called-station-ID or a calling-station-ID to colon:

```
Controller(config)# wireless security dot1x radius accounting mac-delimiter colon
```

# wireless security dot1x radius mac-authentication mac-delimiter

To configure MAC-Authentication attributes, use the **wireless security dot1x radius mac-authentication mac-delimiter** command.

To remove MAC-Authentication attributes, use the **no** form of the command.

**wireless security dot1x radius mac-authentication mac-delimiter** {colon | hyphen | none | single-hyphen  
}

## Syntax Description

<b>colon</b>	Sets the delimiter to colon.
<b>hyphen</b>	Sets the delimiter to hyphen.
<b>none</b>	Disables delimiters.
<b>single-hyphen</b>	Sets the delimiters to single hyphen.

## Command Default

None

## Command Modes

Global Configuration Mode

## Command History

Release	Modification
Cisco IOS XE 3.6.0 E	This command was introduced.

## Examples

This example shows how to configure MAC-Authentication attributes to colon:

```
Controller(config)# Scurity dot1x radius mac-authentication mac-delimiter colon
```

# wireless security certificate force-sha1-cert

To disable SHA2 certification for DTLS connections. To enable SHA2 certification for DTLS connections, use the **no** form of the command.

## wireless security certificate force-sha1-cert

There is no keyword or syntax.

### Command Default

None

### Command Modes

Global Configuration Mode

### Command History

Release	Modification
Cisco IOS XE 3.7.0 E	This command was introduced.

### Examples

This example shows how to disable SHA2 certification for DTLS connections:

```
Controller(config)# wireless security certificate force-sha1-cert
```

# wireless security dot1x radius callStationIdCase

To configure Call Station Id CASE send in RADIUS messages, use the **wireless security dot1x radius callStationIdCase** command.

To remove the Call Station Id CASE send in RADIUS messages, use the **no** form of the command.

**wireless security dot1x radius callStationIdCase {lower|upper}**

## Syntax Description

<b>lower</b>	Sends all Call Station Ids to RADIUS in lowercase
<b>upper</b>	Sends all Call Station Ids to RADIUS in uppercase

## Command Default

None

## Command Modes

Global Configuration Mode

## Command History

Release	Modification
Cisco IOS XE 3.6.0 E	This command was introduced.

## Examples

This example shows how to configure Call Station Id CASE send in RADIUS messages in lowercase:

```
Controller(config)# wireless security dot1x radius callstationIdCase lower
```

## wireless security web-auth retries

To enable web authentication retry on a particular WLAN, use the **wireless wireless security web-auth retries** command. To disable, use the **no** form of the command.

**wireless security web-auth retries** *retries*

**no wireless security web-auth retries**

### Syntax Description

<b>wireless security web-auth</b>	Enables web authentication on a particular WLAN.
<b>retries</b> <i>retries</i>	Specifies maximum number of web authentication request retries. The range is from 0 through 30. The default value is 3.

### Command Default

### Command Modes

config

### Command History

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

### Usage Guidelines

None.

### Examples

This example shows how to enable web authentication retry on a particular WLAN.

```
Controller#configure terminal
Controller# wireless security web-auth retries 10
```

# wireless dot11-padding

To enable over-the-air frame padding, use the **wireless dot11-padding** command. To disable, use the **no** form of the command.

**wireless dot11-padding**

**no wireless dot11-padding**

## Command Default

Disabled.

## Command Modes

config

## Command History

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

## Usage Guidelines

None.

## Examples

This example shows how to enable over-the-air frame padding

```
Controller#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)#wireless dot11-padding
```



# wireless wlancc

To disable console write access of all the access points, use the **wireless wlancc** command in global configuration mode. To enable console write access of all the access points, use the no form of this command.

**wireless wlancc**

## Command Default

None

## Command Modes

Global Configuration

## Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

## Examples

The following example shows how to disable console write access of all the access points:

```
Controller(config)# wireless wlancc
```

## wireless wps rogue ap valid-client

To configure auto-contain on detecting valid clients using rogue access points, use the **wireless wps rogue ap valid-client** command.

**wireless wps rogue ap valid client auto-contain**

### Syntax Description

<b>auto-contain</b>	Automatically contains a rogue access point to which a trusted client is associated.
---------------------	--

### Command Default

None

### Command Modes

Global Configuration

### Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

### Usage Guidelines

None

### Examples

The following example shows how to configure auto-contain on detecting valid clients using rogue access points:

```
Controller(config)# wireless wps rogue ap valid-client
```

# wireless wps rogue client

To configure the AAA server or MSE to validate if rogue clients are valid clients, use the **wireless wps rogue client** command.

**wireless wps rogue client**{aaa| mse}

## Syntax Description

<b>aaa</b>	Configures AAA or local database to detect valid MAC addresses.
<b>mse</b>	Configures MSE to detect valid MAC addresses.

## Command Default

None

## Command Modes

Global Configuration

## Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

## Usage Guidelines

None

## Examples

The following example shows how to configure AAA to detect valid MAC addresses.

```
Controllerwireless wps rogue client aaa
```

The following example shows how to configure MSE to detect valid MAC addresses.

```
Controllerwireless wps rogue client mse  
Controller show wireless wps rogue client summary  
Validate rogue clients against AAA : Disabled  
Validate rogue clients against MSE : Enabled  
Number of rogue clients detected : 0
```

# wireless wps rogue rule

To configure rogue classification rule, use the **wireless wps rogue rule** command.

**wireless wps rogue rule** *rule-name* **priority** *priority* {**classify** {**friendly**|**malicious**} | **condition** {**client-count** **number**| **duration**| **encryption**| **infrastructure**| **rss**| **ssid**} | **default** | **exit** | **match** {**all**|**any**} | **no** | **shutdown**}

## Syntax Description

<b>rule</b> <i>rule-name</i>	Specifies a rule name.
<b>priority</b> <i>priority</i>	Changes the priority of a specific rule and shifts others in the list accordingly.
<b>classify</b>	Specifies the classification of a rule.
<b>friendly</b>	Classifies a rule as friendly.
<b>malicious</b>	Classifies a rule as malicious.
<b>condition</b> { <b>client-count</b> <b>number</b>   <b>duration</b>   <b>encryption</b>   <b>infrastructure</b>   <b>rss</b>   <b>ssid</b> }	<p>Specifies the conditions for a rule that the rogue access point must meet.</p> <p>Type of the condition to be configured. The condition types are listed below:</p> <ul style="list-style-type: none"> <li>• <b>client-count</b>—Requires that a minimum number of clients be associated to a rogue access point. The valid range is 1 to 10 (inclusive).</li> <li>• <b>duration</b>—Requires that a rogue access point be detected for a minimum period of time. The valid range is 0 to 3600 seconds (inclusive).</li> <li>• <b>encryption</b>—Requires that the advertised WLAN does not have encryption enabled.</li> <li>• <b>infrastructure</b>—Requires the SSID to be known to the controller</li> <li>• <b>rss</b>—Requires that a rogue access point have a minimum RSSI value. The range is from -95 to -50 dBm (inclusive).</li> <li>• <b>ssid</b>—Requires that a rogue access point have a specific SSID.</li> </ul>
<b>default</b>	Sets the command to its default settings.
<b>exit</b>	Exits the sub-mode.
<b>match</b> { <b>all</b>   <b>any</b> }	Configures matching criteria for a rule. Specifies whether a detected rogue access point must meet all or any of the conditions specified by the rule in order for the rule to be matched and the rogue access point to adopt the classification type of the rule.
<b>no</b>	Negates a command or set its defaults.
<b>shutdown</b>	Shuts down the system.

**Command Default**

None.

**Command Modes**

Global configuration

**Command History**

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

**Usage Guidelines**

None.

**Examples**

This example shows how to create a rule that can organize and display rogue access points as Friendly:

```
Controller# configure terminal
Controller(config)# wireless wps rogue rule ap1 priority 1
Controller(config-rule)# classify friendly
Controller(config)# end
```

# wireless wps rogue detection

To configure various rouge detection parameters, use the **wireless wps rogue detection** command.

**wireless wps rogue detection** [**min-rssi** *rssi* | **min-transient-time** *transtime*]

## Syntax Description

<b>min-rssi</b> <i>rssi</i>	Configures the minimum RSSI value that rogues should have for APs to detect and for rogue entry to be created in the controller.
<b>min-transient-time</b> <i>transtime</i>	Configures the time interval at which rogues have to be consistently scanned for by APs after the first time the rogues are scanned.

## Command Default

None.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

None.

## Examples

This example shows how to configure rogue detection minimum RSSI value and minimum transient time:

```
Controller# configure terminal
Controller(config)# wireless wps rogue detection min-rssi 100
Controller(config)# wireless wps rogue detection min-transient-time 500
Controller(config)# end
```

## vlan access-map

To create or modify a VLAN map entry for VLAN packet filtering, and change the mode to the VLAN access-map configuration, use the **vlan access-map** command in global configuration mode on the switch stack or on a standalone switch. To delete a VLAN map entry, use the **no** form of this command.

**vlan access-map** *name* [*number*]

**no vlan access-map** *name* [*number*]

**Note**

This command is not supported on switches running the LAN Base feature set.

**Syntax Description**

<i>name</i>	Name of the VLAN map.
<i>number</i>	(Optional) The sequence number of the map entry that you want to create or modify (0 to 65535). If you are creating a VLAN map and the sequence number is not specified, it is automatically assigned in increments of 10, starting from 10. This number is the sequence to insert to, or delete from, a VLAN access-map entry.

**Command Default**

There are no VLAN map entries and no VLAN maps applied to a VLAN.

**Command Modes**

Global configuration

**Command History**

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

**Usage Guidelines**

In global configuration mode, use this command to create or modify a VLAN map. This entry changes the mode to VLAN access-map configuration, where you can use the **match** access-map configuration command to specify the access lists for IP or non-IP traffic to match and use the **action** command to set whether a match causes the packet to be forwarded or dropped.

In VLAN access-map configuration mode, these commands are available:

- **action**—Sets the action to be taken (forward or drop).
- **default**—Sets a command to its defaults.
- **exit**—Exits from VLAN access-map configuration mode.
- **match**—Sets the values to match (IP address or MAC address).

- **no**—Negates a command or set its defaults.

When you do not specify an entry number (sequence number), it is added to the end of the map.

There can be only one VLAN map per VLAN and it is applied as packets are received by a VLAN.

You can use the **no vlan access-map** *name* [*number*] command with a sequence number to delete a single entry.

Use the **vlan filter** interface configuration command to apply a VLAN map to one or more VLANs.

For more information about VLAN map entries, see the software configuration guide for this release.

## Examples

This example shows how to create a VLAN map named `vac1` and apply matching conditions and actions to it. If no other entries already exist in the map, this will be entry 10.

```
Controller(config)# vlan access-map vac1  
Controller(config-access-map)# match ip address acl1  
Controller(config-access-map)# action forward
```

This example shows how to delete VLAN map `vac1`:

```
Controller(config)# no vlan access-map vac1
```



# vlan filter

To apply a VLAN map to one or more VLANs, use the **vlan filter** command in global configuration mode on the switch stack or on a standalone switch. To remove the map, use the **no** form of this command.

**vlan filter** *mapname* **vlan-list** {*list*| **all**}

**no vlan filter** *mapname* **vlan-list** {*list*| **all**}



## Note

This command is not supported on switches running the LAN Base feature set.

## Syntax Description

<i>mapname</i>	Name of the VLAN map entry.
<b>vlan-list</b>	Specifies which VLANs to apply the map to.
<i>list</i>	The list of one or more VLANs in the form tt, uu-vv, xx, yy-zz, where spaces around commas and dashes are optional. The range is 1 to 4094.
<b>all</b>	Adds the map to all VLANs.

## Command Default

There are no VLAN filters.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

To avoid accidentally dropping too many packets and disabling connectivity in the middle of the configuration process, we recommend that you completely define the VLAN access map before applying it to a VLAN.

For more information about VLAN map entries, see the software configuration guide for this release.

## Examples

This example applies VLAN map entry map1 to VLANs 20 and 30:

```
Controller(config)# vlan filter map1 vlan-list 20, 30
```

This example shows how to delete VLAN map entry mac1 from VLAN 20:

```
Controller(config)# no vlan filter map1 vlan-list 20
```

You can verify your settings by entering the **show vlan filter** privileged EXEC command.

# vlan group

To create or modify a VLAN group, use the **vlan group** command in global configuration mode. To remove a VLAN list from the VLAN group, use the **no** form of this command.

**vlan group** *group-name* **vlan-list** *vlan-list*

**no vlan group** *group-name* **vlan-list** *vlan-list*

## Syntax Description

<i>group-name</i>	Name of the VLAN group. The group name may contain up to 32 characters and must begin with a letter.
<b>vlan-list</b> <i>vlan-list</i>	Specifies one or more VLANs to be added to the VLAN group. The <i>vlan-list</i> argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID range. Multiple entries are separated by a hyphen (-) or a comma (,).

## Command Default

None

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

If the named VLAN group does not exist, the **vlan group** command creates the group and maps the specified VLAN list to the group. If the named VLAN group exists, the specified VLAN list is mapped to the group.

The **no** form of the **vlan group** command removes the specified VLAN list from the VLAN group. When you remove the last VLAN from the VLAN group, the VLAN group is deleted.

A maximum of 100 VLAN groups can be configured, and a maximum of 4094 VLANs can be mapped to a VLAN group.

## Examples

This example shows how to map VLANs 7 through 9 and 11 to a VLAN group:

```
Controller(config)# vlan group group1 vlan-list 7-9,11
```

This example shows how to remove VLAN 7 from the VLAN group:

```
Controller(config)# no vlan group group1 vlan-list 7
```

 vlan group



## INDEX

### A

aaa authentication login command [22](#)  
aaa authorization credential download default command [23](#)  
aaa authorization network command [24](#)  
aaa group server radius command [25](#)  
address ipv4 auth-port acct-port command [27](#)  
ap dtls secure-cipher command [28](#)  
authentication mac-move permit command [32](#)  
authentication priority command [33](#)

### B

banner [38](#)

### C

cisp enable [40](#)  
clear errdisable interface vlan [42](#)  
clear mac address-table command [44](#)  
consent email [46](#)

### D

deny command [47](#)  
dot1x supplicant force-multicast command [55](#)  
dot1x test timeout [57](#)

### E

epm access-control open command [61](#)

### F

fips authorization-key command [62](#)  
fips log-dtls-replay command [63](#)

fips zeroize command [64](#)

### I

ip admission name command [66](#)  
ip device tracking maximum command [69](#)  
ip device tracking probe command [70](#)  
ip dhcp snooping verify no-relay-agent-address [74](#)  
ip verify source command [77](#)

### K

key ww-wireless command [81](#)

### M

mab request format attribute 32 command [84](#)  
map-index map command [88](#)  
match (access-map configuration) command [86](#)

### N

no authentication logging verbose [89](#)  
no dot1x logging verbose [90](#)  
no mab logging verbose [91](#)

### P

parameter map type webauth command [93](#)  
parameter-map type subscriber attribute-to-service command [92](#)  
permit command [96](#)  
policy-map type control subscriber command [100](#)

**R**

radius server command [103](#)

**S**

security web-auth [105](#)  
service-policy type control subscriber command [106](#)  
service-template command [107](#)  
session-timeout [108](#)  
show access-session command [115](#)  
show cisp command [123](#)  
show device classifier attached detail command [119](#)  
show eap command [127](#)  
show fips authorization-key command [128](#)  
show fips status command [129](#)  
show nmsp command [133](#)  
show vlan access-map command [137](#)  
show vlan group command [138](#)  
show wireless wps rogue ap command [139](#)  
show wireless wps rogue client detailed command [140](#)

show wireless wps wips statistics command [142](#)  
sshow wireless wps wips summary command [143](#)

**V**

virtual-ip [147](#)  
vlan access-map command [163](#)  
vlan filter command [165](#)  
vlan group command [167](#)

**W**

wireless dot11-padding command [156](#)  
wireless mobility dtls secure-cipher command [148](#)  
wireless security dot1x command [149](#)  
wireless security web-auth retries command [155](#)  
wireless wlance command [157](#)  
wireless wps rogue detection command [162](#)  
wireless wps rogue rule command [160](#)