



## **VLAN Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)**

**First Published:** January 29, 2013

### **Americas Headquarters**

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

Text Part Number: OL-28524-02

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

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

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

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

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

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

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

© 2013 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### Preface

#### Preface v

Document Conventions v

Related Documentation vii

Obtaining Documentation and Submitting a Service Request vii

---

### CHAPTER 1

#### Using the Command-Line Interface 1

Information About Using the Command-Line Interface 1

Command Modes 1

Using the Help System 3

Understanding Abbreviated Commands 4

No and Default Forms of Commands 5

CLI Error Messages 5

Configuration Logging 5

How to Use the CLI to Configure Features 6

Configuring the Command History 6

Changing the Command History Buffer Size 6

Recalling Commands 6

Disabling the Command History Feature 7

Enabling and Disabling Editing Features 7

Editing Commands Through Keystrokes 9

Editing Command Lines That Wrap 10

Searching and Filtering Output of show and more Commands 11

Accessing the CLI 12

Accessing the CLI Through a Console Connection or Through Telnet 12

---

### CHAPTER 2

#### VLAN Commands 13

client vlan 14

clear vmps statistics	15
clear vtp counters	16
debug sw-vlan	17
debug sw-vlan ifs	19
debug sw-vlan notification	20
debug sw-vlan vtp	22
interface vlan	24
remote-span	26
show vlan	28
show vlan filter	32
show vlan group	33
show vtp	34
show wireless vlan group	41
spanning-tree vlan	42
wireless broadcast vlan	45
wireless vlan group	46
wlan	47



## Preface

- [Document Conventions](#), page v
- [Related Documentation](#), page vii
- [Obtaining Documentation and Submitting a Service Request](#), page vii

## Document Conventions

This document uses the following conventions:

Convention	Description
<code>^</code> or <code>Ctrl</code>	Both the <code>^</code> symbol and <code>Ctrl</code> represent the Control (Ctrl) key on a keyboard. For example, the key combination <code>^D</code> or <code>Ctrl-D</code> 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> .
<code>Courier font</code>	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.

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

### Reader Alert Conventions

This document may use the following conventions for reader alerts:



#### Note

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



#### Tip

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



#### Caution

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



#### Timesaver

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



#### Warning

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

## Related Documentation

**Note**

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

- Cisco Catalyst 3850 Switch documentation, located at:  
[http://www.cisco.com/go/cat3850\\_docs](http://www.cisco.com/go/cat3850_docs)
- Cisco 5700 Series Wireless Controller documentation, located at:  
[http://www.cisco.com/go/wlc5700\\_sw](http://www.cisco.com/go/wlc5700_sw)
- Cisco SFP and SFP+ modules documentation, including compatibility matrixes, located at:  
[http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html)
- Cisco Validated Designs documents, located at:  
<http://www.cisco.com/go/designzone>
- Error Message Decoder, located at:  
<https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>

## Obtaining Documentation and Submitting a Service Request

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

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

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







# Using the Command-Line Interface

---

- [Information About Using the Command-Line Interface, page 1](#)
- [How to Use the CLI to Configure Features, page 6](#)

## Information About Using the Command-Line Interface

### Command Modes

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

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

When you start a session, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the 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</b> <i>vlan-id</i> command.	Controller(config-vlan)#		

Mode	Access Method	Prompt	Exit Method	About This Mode
			<p>To exit to global configuration mode, enter the <b>exit</b> command.</p> <p>To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b>.</p>	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)#	<p>To exit to global configuration mode, enter <b>exit</b>.</p> <p>To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b>.</p>	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)#	<p>To exit to global configuration mode, enter <b>exit</b>.</p> <p>To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b>.</p>	Use this mode to configure parameters for the terminal line.

## Using the Help System

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

### SUMMARY STEPS

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

## DETAILED STEPS

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

## Understanding Abbreviated Commands

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

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

```
Controller# show conf
```

## No and Default Forms of Commands

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

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

## CLI Error Messages

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

**Table 2: Common CLI Error Messages**

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

## Configuration Logging

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

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



**Note**

Only CLI or HTTP changes are logged.

# How to Use the CLI to Configure Features

## Configuring the Command History

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

### Changing the Command History Buffer Size

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

#### SUMMARY STEPS

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

#### DETAILED STEPS

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

### Recalling Commands

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



**Note**

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

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<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.
Step 2	<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.
Step 3	<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
Step 1	<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 reenale 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> <code>Controller# terminal editing</code>	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> <code>Controller# terminal no editing</code>	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

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

### 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.



## VLAN Commands

---

- [client vlan](#), page 14
- [clear vmpls statistics](#), page 15
- [clear vtp counters](#), page 16
- [debug sw-vlan](#), page 17
- [debug sw-vlan ifs](#), page 19
- [debug sw-vlan notification](#), page 20
- [debug sw-vlan vtp](#), page 22
- [interface vlan](#), page 24
- [remote-span](#), page 26
- [show vlan](#), page 28
- [show vlan filter](#), page 32
- [show vlan group](#), page 33
- [show vtp](#), page 34
- [show wireless vlan group](#), page 41
- [spanning-tree vlan](#), page 42
- [wireless broadcast vlan](#), page 45
- [wireless vlan group](#), page 46
- [wlan](#), page 47

# client vlan

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

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

**no client vlan**

## Syntax Description

<i>interface--id-name-or-group-name</i>	Interface ID, name, or VLAN group name.
---	---

## Command Default

The default interface is configured.

## Command Modes

WLAN configuration

## Command History

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

## Usage Guidelines

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

## Examples

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

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

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

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

## clear vmps statistics

To clear the VLAN Membership Policy Server (VMPS) statistics maintained by the VLAN Query Protocol (VQP) client, use the **clear vmps statistics** command in privileged EXEC mode.

**clear vmps statistics**

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

<b>Command Default</b>	None
------------------------	------

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

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

**Examples**

This example shows how to clear VLAN Membership Policy Server (VMPS) statistics:

```
Controller# clear vmps statistics
```

You can verify that information was deleted by entering the **show vmps statistics** privileged EXEC command.

# clear vtp counters

To clear the VLAN Trunking Protocol (VTP) and pruning counters, use the **clear vtp counters** command in privileged EXEC mode.

**clear vtp counters**

## Syntax Description

This command has no arguments or keywords.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

## Examples

This example shows how to clear the VTP counters:

```
Controller# clear vtp counters
```

You can verify that information was deleted by entering the **show vtp counters** privileged EXEC command.

## Related Commands

Command	Description
<a href="#">show vtp</a>	Displays general information about VTP management domain, status, and counters.



## debug sw-vlan

To enable debugging of VLAN manager activities, use the **debug sw-vlan** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

**debug sw-vlan** {badpmcookies| cfg-vlan {bootup| cli}| events| ifs| management| mapping| notification| packets| redundancy| registries| vtp}

**no debug sw-vlan** {badpmcookies| cfg-vlan {bootup| cli}| events| ifs| management| mapping| notification| packets| redundancy| registries| vtp}

### Syntax Description

<b>badpmcookies</b>	Displays debug messages for VLAN manager incidents of bad port manager cookies.
<b>cfg-vlan</b>	Displays VLAN configuration debug messages.
<b>bootup</b>	Displays messages when the switch is booting up.
<b>cli</b>	Displays messages when the command-line interface (CLI) is in VLAN configuration mode.
<b>events</b>	Displays debug messages for VLAN manager events.
<b>ifs</b>	Displays debug messages for the VLAN manager IOS file system (IFS). See <a href="#">debug sw-vlan ifs</a> , on page 19 for more information.
<b>management</b>	Displays debug messages for VLAN manager management of internal VLANs.
<b>mapping</b>	Displays debug messages for VLAN mapping.
<b>notification</b>	Displays debug messages for VLAN manager notifications. See <a href="#">debug sw-vlan notification</a> , on page 20 for more information.
<b>packets</b>	Displays debug messages for packet handling and encapsulation processes.
<b>redundancy</b>	Displays debug messages for VTP VLAN redundancy.
<b>registries</b>	Displays debug messages for VLAN manager registries.
<b>vtp</b>	Displays debug messages for the VLAN Trunking Protocol (VTP) code. See <a href="#">debug sw-vlan vtp</a> , on page 22 for more information.

**Command Default** Debugging is disabled.

**Command Modes** Privileged EXEC

**Command History**

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

**Usage Guidelines**

The **undebg sw-vlan** command is the same as the **no debug sw-vlan** command.

**Examples**

This example shows how to display debug messages for VLAN manager events:

```
Controller# debug sw-vlan events
```

**Related Commands**

Command	Description
<a href="#">debug sw-vlan ifs</a>	Enables debugging of the VLAN manager IOS file system (IFS) error tests.
<a href="#">debug sw-vlan notification</a>	Enables debugging of VLAN manager notifications.
<a href="#">debug sw-vlan vtp</a>	Enables debugging of the VTP code.
<a href="#">show vlan</a>	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.
<a href="#">show vtp</a>	Displays general information about VTP management domain, status, and counters.

# debug sw-vlan ifs

To enable debugging of the VLAN manager IOS file system (IFS) error tests, use the **debug sw-vlan ifs** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

**debug sw-vlan ifs** {open {read| write}| read {1| 2| 3| 4}| write}

**no debug sw-vlan ifs** {open {read| write}| read {1| 2| 3| 4}| write}

## Syntax Description

<b>open read</b>	Displays VLAN manager IFS file-read operation debug messages.
<b>open write</b>	Displays VLAN manager IFS file-write operation debug messages.
<b>read</b>	Displays file-read operation debug messages for the specified error test ( <b>1</b> , <b>2</b> , <b>3</b> , or <b>4</b> ).
<b>write</b>	Displays file-write operation debug messages.

## Command Default

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

The **undebug sw-vlan ifs** command is the same as the **no debug sw-vlan ifs** command.

When selecting the file read operation, Operation **1** reads the file header, which contains the header verification word and the file version number. Operation **2** reads the main body of the file, which contains most of the domain and VLAN information. Operation **3** reads type length version (TLV) descriptor structures. Operation **4** reads TLV data.

## Examples

This example shows how to display file-write operation debug messages:

```
Controller# debug sw-vlan ifs write
```

## Related Commands

Command	Description
<a href="#">show vlan</a>	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.

# debug sw-vlan notification

To enable debugging of VLAN manager notifications, use the **debug sw-vlan notification** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

**debug sw-vlan notification** {accfwdchange| allowedvlancfgchange| fwdchange| linkchange| modechange| pruningcfgchange| statechange}

**no debug sw-vlan notification** {accfwdchange| allowedvlancfgchange| fwdchange| linkchange| modechange| pruningcfgchange| statechange}

## Syntax Description

<b>accfwdchange</b>	Displays debug messages for VLAN manager notification of aggregated access interface spanning-tree forward changes.
<b>allowedvlancfgchange</b>	Displays debug messages for VLAN manager notification of changes to the allowed VLAN configuration.
<b>fwdchange</b>	Displays debug messages for VLAN manager notification of spanning-tree forwarding changes.
<b>linkchange</b>	Displays debug messages for VLAN manager notification of interface link-state changes.
<b>modechange</b>	Displays debug messages for VLAN manager notification of interface mode changes.
<b>pruningcfgchange</b>	Displays debug messages for VLAN manager notification of changes to the pruning configuration.
<b>statechange</b>	Displays debug messages for VLAN manager notification of interface state changes.

## Command Default

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

The **undebg sw-vlan notification** command is the same as the **no debug sw-vlan notification** command.

### Examples

This example shows how to display debug messages for VLAN manager notification of interface mode changes:

```
Controller# debug sw-vlan notification
```

### Related Commands

Command	Description
<a href="#">show vlan</a>	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.

## debug sw-vlan vtp

To enable debugging of the VLAN Trunking Protocol (VTP) code, use the **debug sw-vlan vtp** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

**debug sw-vlan vtp** {events| packets| pruning [packets| xmit]| redundancy| xmit}

**no debug sw-vlan vtp** {events| packets| pruning| redundancy| xmit}

### Syntax Description

<b>events</b>	Displays debug messages for general-purpose logic flow and detailed VTP messages generated by the VTP_LOG_RUNTIME macro in the VTP code.
<b>packets</b>	Displays debug messages for the contents of all incoming VTP packets that have been passed into the VTP code from the Cisco IOS VTP platform-dependent layer, except for pruning packets.
<b>pruning</b>	Displays debug messages generated by the pruning segment of the VTP code.
<b>packets</b>	(Optional) Displays debug messages for the contents of all incoming VTP pruning packets that have been passed into the VTP code from the Cisco IOS VTP platform-dependent layer.
<b>xmit</b>	(Optional) Displays debug messages for the contents of all outgoing VTP packets that the VTP code requests the Cisco IOS VTP platform-dependent layer to send.
<b>redundancy</b>	Displays debug messages for VTP redundancy.
<b>xmit</b>	Displays debug messages for the contents of all outgoing VTP packets that the VTP code requests the Cisco IOS VTP platform-dependent layer to send, except for pruning packets.

### Command Default

Debugging is disabled.

### Command Modes

Privileged EXEC

### Command History

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

### Usage Guidelines

The **undebg sw-vlan vtp** command is the same as the **no debug sw-vlan vtp** command.

If no additional parameters are entered after the **pruning** keyword, VTP pruning debugging messages appear. They are generated by the VTP\_PRUNING\_LOG\_NOTICE, VTP\_PRUNING\_LOG\_INFO, VTP\_PRUNING\_LOG\_DEBUG, VTP\_PRUNING\_LOG\_ALERT, and VTP\_PRUNING\_LOG\_WARNING macros in the VTP pruning code.

### Examples

This example shows how to display debug messages for VTP redundancy:

```
Controller# debug sw-vlan vtp redundancy
```

### Related Commands

Command	Description
<a href="#">show vtp</a>	Displays general information about VTP management domain, status, and counters.

# interface vlan

To create or access a dynamic switch virtual interface (SVI) and to enter interface configuration mode, use the **interface vlan** command in global configuration mode. To delete an SVI, use the **no** form of this command.

**interface vlan** *vlan-id*  
**no interface vlan** *vlan-id*

<b>Syntax Description</b>	<i>vlan-id</i>	VLAN number. The range is 1 to 4094.
---------------------------	----------------	--------------------------------------

<b>Command Default</b>	The default VLAN interface is VLAN 1.
------------------------	---------------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

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

**Usage Guidelines**

SVIs are created the first time you enter the **interface vlan** *vlan-id* command for a particular VLAN. The *vlan-id* corresponds to the VLAN-tag associated with data frames on an IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port.



**Note** When you create an SVI, it does not become active until it is associated with a physical port.

If you delete an SVI using the **no interface vlan** *vlan-id* command, it is no longer visible in the output from the **show interfaces** privileged EXEC command.



**Note** You cannot delete the VLAN 1 interface.

You can reinstate a deleted SVI by entering the **interface vlan** *vlan-id* command for the deleted interface. The interface comes back up, but the previous configuration is gone.

The interrelationship between the number of SVIs configured on a switch or a switch stack and the number of other features being configured might have an impact on CPU utilization due to hardware limitations. You can use the **sdm prefer** global configuration command to reallocate system hardware resources based on templates and feature tables.



You can verify your setting by entering the **show interfaces** and **show interfaces vlan *vlan-id*** privileged EXEC commands.

### Examples

This example shows how to create a new SVI with VLAN ID 23 and enter interface configuration mode:

```
Controller(config)# interface vlan 23  
Controller(config-if)#
```

### Related Commands

Command	Description
show interfaces	Displays the administrative and operational status of all interfaces or a specified interface.

## remote-span

To configure a VLAN as a Remote Switched Port Analyzer (RSPAN) VLAN, use the **remote-span** command in VLAN configuration mode on the switch stack or on a standalone switch. To remove the RSPAN designation from the VLAN, use the **no** form of this command.

**remote-span**

**no remote-span**

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

**Command Default** No RSPAN VLANs are defined.

**Command Modes** VLAN configuration (config-VLAN)

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

**Usage Guidelines** If VLAN Trunking Protocol (VTP) is enabled, the RSPAN feature is propagated by VTP for VLAN IDs that are lower than 1005. If the RSPAN VLAN ID is in the extended range, you must manually configure intermediate switches (those in the RSPAN VLAN between the source switch and the destination switch).

Before you configure the RSPAN **remote-span** command, use the **vlan** (global configuration) command to create the VLAN.

The RSPAN VLAN has these characteristics:

- No MAC address learning occurs on it.
- RSPAN VLAN traffic flows only on trunk ports.
- Spanning Tree Protocol (STP) can run in the RSPAN VLAN, but it does not run on RSPAN destination ports.

When an existing VLAN is configured as an RSPAN VLAN, the VLAN is first deleted and then recreated as an RSPAN VLAN. Any access ports are made inactive until the RSPAN feature is disabled.

**Examples** This example shows how to configure a VLAN as an RSPAN VLAN:

```
Controller(config) # vlan 901
Controller(config-vlan) # remote-span
```

This example shows how to remove the RSPAN feature from a VLAN:

```
Controller(config)# vlan 901  
Controller(config-vlan)# no remote-span
```

You can verify your settings by entering the **show vlan remote-span** user EXEC command.

#### Related Commands

Command	Description
monitor session destination	Configures a FSPAN or FRSPAN destination session.
monitor session filter	Configures a FSPAN or FRSPAN session filter.
monitor session source	Configures a FSPAN or FRSPAN source session.
<a href="#">show vlan</a>	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.

# show vlan

To display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch, use the **show vlan** command in user EXEC mode.

**show vlan** [**brief**] **group** | **id** *vlan-id* | **group-name** *WORD user\_count* | **mtu** | **name** *vlan-name* | **remote-span** | **summary**]

## Syntax Description

<b>brief</b>	(Optional) Displays one line for each VLAN with the VLAN name, status, and its ports.
<b>group</b>	(Optional) Displays information about VLAN groups.
<b>id</b> <i>vlan-id</i>	(Optional) Displays information about a single VLAN identified by the VLAN ID number. For <i>vlan-id</i> , the range is 1 to 4094.
<b>group-name</b> <i>WORD vlan-id vlan-id</i>	(Optional) Displays information about a specific VLAN group.
<b>mtu</b>	(Optional) Displays a list of VLANs and the minimum and maximum transmission unit (MTU) sizes configured on ports in the VLAN.
<b>name</b> <i>vlan-name</i>	(Optional) Displays information about a single VLAN identified by the VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.
<b>remote-span</b>	(Optional) Displays information about Remote SPAN (RSPAN) VLANs.
<b>summary</b>	(Optional) Displays VLAN summary information.



### Note

The **ifindex** keyword is not supported, even though it is visible in the command-line help string.

## Command Default

None

## Command Modes

User EXEC

## Command History

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

**Usage Guidelines**

In the **show vlan mtu** command output, the MTU\_Mismatch column shows whether all the ports in the VLAN have the same MTU. When yes appears in the column, it means that the VLAN has ports with different MTUs, and packets that are switched from a port with a larger MTU to a port with a smaller MTU might be dropped. If the VLAN does not have an SVI, the hyphen (-) symbol appears in the SVI\_MTU column. If the MTU-Mismatch column displays yes, the names of the ports with the MinMTU and the MaxMTU appear.

**Examples**

This is an example of output from the **show vlan** command. See the table that follows for descriptions of the fields in the display.

```

Controller> show vlan
VLAN Name                                     Status      Ports
-----
1    default                                  active      Gi1/0/2, Gi1/0/3, Gi1/0/4
                                           Gi1/0/5, Gi1/0/6, Gi1/0/7
                                           Gi1/0/8, Gi1/0/9, Gi1/0/10
                                           Gi1/0/11, Gi1/0/12, Gi1/0/13
                                           Gi1/0/14, Gi1/0/15, Gi1/0/16
                                           Gi1/0/17, Gi1/0/18, Gi1/0/19
                                           Gi1/0/20, Gi1/0/21, Gi1/0/22
                                           Gi1/0/23, Gi1/0/24, Gi1/0/25
                                           Gi1/0/26, Gi1/0/27, Gi1/0/28
                                           Gi1/0/29, Gi1/0/30, Gi1/0/31
                                           Gi1/0/32, Gi1/0/33, Gi1/0/34
                                           Gi1/0/35, Gi1/0/36, Gi1/0/37
                                           Gi1/0/38, Gi1/0/39, Gi1/0/40
                                           Gi1/0/41, Gi1/0/42, Gi1/0/43
                                           Gi1/0/44, Gi1/0/45, Gi1/0/46
                                           Gi1/0/47, Gi1/0/48
2    VLAN0002                                active
40   vlan-40                                  active
300  VLAN0300                                active
1002 fddi-default                           act/unsup
1003 token-ring-default                     act/unsup
1004 fddinet-default                        act/unsup
1005 trnet-default                          act/unsup

VLAN Type  SAID      MTU    Parent  RingNo BridgeNo  Stp    BrdgMode Trans1 Trans2
-----
1    enet    100001    1500   -       -       -       -       -       0       0
2    enet    100002    1500   -       -       -       -       -       0       0
40   enet    100040    1500   -       -       -       -       -       0       0
300  enet    100300    1500   -       -       -       -       -       0       0
1002 fddi    101002    1500   -       -       -       -       -       0       0
1003 tr     101003    1500   -       -       -       -       -       0       0
1004 fdnet  101004    1500   -       -       -       ieee   -       0       0
1005 trnet  101005    1500   -       -       -       ibm    -       0       0
2000 enet    102000    1500   -       -       -       -       -       0       0
3000 enet    103000    1500   -       -       -       -       -       0       0

Remote SPAN VLANs
-----
2000,3000

Primary Secondary Type           Ports
-----

```

**Table 4: show vlan Command Output Fields**

Field	Description
VLAN	VLAN number.

Field	Description
Name	Name, if configured, of the VLAN.
Status	Status of the VLAN (active or suspend).
Ports	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.
BrdgNo	Bridge number for the VLAN, if applicable.
Stp	Spanning Tree Protocol type used on the VLAN.
BrdgMode	Bridging mode for this VLAN—possible values are source-route bridging (SRB) and source-route transparent (SRT); the default is SRB.
Trans1	Translation bridge 1.
Trans2	Translation bridge 2.
Remote SPAN VLANs	Identifies any RSPAN VLANs that have been configured.

This is an example of output from the **show vlan summary** command:

```
Controller> show vlan summary
Number of existing VLANs           : 45
Number of existing VTP VLANs      : 45
Number of existing extended VLANs : 0
```

This is an example of output from the **show vlan id** command:

```
Controller# show vlan id 2
VLAN Name                Status    Ports
-----
2    VLAN0200              active    Gi1/0/7, Gi1/0/8
2    VLAN0200              active    Gi2/0/1, Gi2/0/2

VLAN Type  SAID      MTU    Parent RingNo BridgeNo  Stp  BrdgMode Trans1 Trans2
-----
2    enet    100002    1500    -      -      -      -    -        0      0

Remote SPAN VLANs
-----
Disabled
```

**Related Commands**

Command	Description
switchport mode	Configures the VLAN membership mode of a port.

# show vlan filter

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

**show vlan filter** {**access-map** *name*| **vlan** *vlan-id*}

## Syntax Description

<b>access-map</b> <i>name</i>	(Optional) Displays filtering information for the specified VLAN access map.
<b>vlan</b> <i>vlan-id</i>	(Optional) Displays filtering information for the specified VLAN. The range is 1 to 4094.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

## Examples

This is an example of output from the **show vlan filter** command:

```
Controller# show vlan filter
VLAN Map map_1 is filtering VLANs:
 20-22
```

## Related Commands

Command	Description
show vlan access-map	Displays the VLAN access maps created on the switch.
vlan access-map	Defines a VLAN map and enters access-map configuration mode where you can specify a MAC ACL to match and the action to be taken.



# 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	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:

```
Controller# show vlan group group-name group2
vlan group group1 :40-45
```

This example shows how to display number of users in each of the VLANs in a group:

```
Controller# show vlan group group-name group2 user_count
VLAN      : Count
-----
40         : 5
41         : 8
42         : 12
43         : 2
44         : 9
45         : 0
```

# show vtp

To display general information about the VLAN Trunking Protocol (VTP) management domain, status, and counters, use the **show vtp** command in EXEC mode.

**show vtp** {**counters**| **devices** [**conflicts**]| **interface** [*interface-id*]| **password**| **status**}

## Syntax Description

<b>counters</b>	Displays the VTP statistics for the controller.
<b>devices</b>	Displays information about all VTP version 3 devices in the domain. This keyword applies only if the controller is not running VTP version 3.
<b>conflicts</b>	(Optional) Displays information about VTP version 3 devices that have conflicting primary servers. This command is ignored when the controller is in VTP transparent or VTP off mode.
<b>interface</b>	Displays VTP status and configuration for all interfaces or the specified interface.
<i>interface-id</i>	(Optional) Interface for which to display VTP status and configuration. This can be a physical interface or a port channel.
<b>password</b>	Displays the configured VTP password (available in privileged EXEC mode only).
<b>status</b>	Displays general information about the VTP management domain status.

## Command Default

None

## Command Modes

User EXEC  
Privileged EXEC

## Command History

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

## Usage Guidelines

When you enter the **show vtp password** command when the controller is running VTP version 3, the display follows these rules:

- If the **password** *password* global configuration command did not specify the **hidden** keyword and encryption is not enabled on the controller, the password appears in clear text.

- If the **password** *password* command did not specify the **hidden** keyword and encryption is enabled on the controller, the encrypted password appears.
- If the **password** *password* command is included the **hidden** keyword, the hexadecimal secret key is displayed.

## Examples

This is an example of output from the **show vtp devices** command. A Yes in the Conflict column indicates that the responding server is in conflict with the local server for the feature; that is, when two controllers in the same domain do not have the same primary server for a database.

```

Controller# show vtp devices
Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Database Conf controller ID      Primary Server Revision  System Name
      list
-----
VLAN      Yes  00b0.8e50.d000 000c.0412.6300 12354      main.cisco.com
MST       No   00b0.8e50.d000 0004.AB45.6000 24         main.cisco.com
VLAN      Yes  000c.0412.6300=000c.0412.6300 67         qwerty.cisco.com

```

This is an example of output from the **show vtp counters** command. The table that follows describes each field in the display.

```

Controller> show vtp counters
VTP statistics:
Summary advertisements received      : 0
Subset advertisements received      : 0
Request advertisements received     : 0
Summary advertisements transmitted : 0
Subset advertisements transmitted   : 0
Request advertisements transmitted  : 0
Number of config revision errors    : 0
Number of config digest errors      : 0
Number of V1 summary errors         : 0

VTP pruning statistics:

Trunk      Join Transmitted Join Received      Summary advts received from
-----
Gi1/0/47   0                0                0
Gi1/0/48   0                0                0
Gi2/0/1    0                0                0
Gi3/0/2    0                0                0

```

**Table 5: show vtp counters Field Descriptions**

Field	Description
Summary advertisements received	Number of summary advertisements received by this controller on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements received	Number of subset advertisements received by this controller on its trunk ports. Subset advertisements contain all the information for one or more VLANs.

Field	Description
Request advertisements received	Number of advertisement requests received by this controller on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Summary advertisements transmitted	Number of summary advertisements sent by this controller on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements transmitted	Number of subset advertisements sent by this controller on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request advertisements transmitted	Number of advertisement requests sent by this controller on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Number of configuration revision errors	<p>Number of revision errors.</p> <p>Whenever you define a new VLAN, delete an existing one, suspend or resume an existing VLAN, or modify the parameters on an existing VLAN, the configuration revision number of the controller increments.</p> <p>Revision errors increment whenever the controller receives an advertisement whose revision number matches the revision number of the controller, but the MD5 digest values do not match. This error means that the VTP password in the two controllers is different or that the controllers have different configurations.</p> <p>These errors indicate that the controller is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.</p>

Field	Description
Number of configuration digest errors	<p>Number of MD5 digest errors.</p> <p>Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the controller do not match. This error usually means that the VTP password in the two controllers is different. To solve this problem, make sure the VTP password on all controllers is the same.</p> <p>These errors indicate that the controller is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.</p>
Number of V1 summary errors	<p>Number of Version 1 errors.</p> <p>Version 1 summary errors increment whenever a controller in VTP V2 mode receives a VTP Version 1 frame. These errors indicate that at least one neighboring controller is either running VTP Version 1 or VTP Version 2 with V2-mode disabled. To solve this problem, change the configuration of the controllers in VTP V2-mode to disabled.</p>
Join Transmitted	Number of VTP pruning messages sent on the trunk.
Join Received	Number of VTP pruning messages received on the trunk.
Summary Advts Received from non-pruning-capable device	Number of VTP summary messages received on the trunk from devices that do not support pruning.

This is an example of output from the **show vtp status** command. The table that follows describes each field in the display.

```

Controller> show vtp status
VTP Version capable      : 1 to 3
VTP version running      : 1
VTP Domain Name          :
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                 : 2037.06ce.3580
Configuration last modified by 192.168.1.1 at 10-10-12 04:34:02
Local updater ID is 192.168.1.1 on interface LIIN0 (first layer3 interface found
)

```

Feature VLAN:

```

-----
VTP Operating Mode       : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 7
Configuration Revision    : 2
MD5 digest                : 0xA0 0xA1 0xFE 0x4E 0x7E 0x5D 0x97 0x41
                          : 0x89 0xB9 0x9B 0x70 0x03 0x61 0xE9 0x27

```

**Table 6: show vtp status Field Descriptions**

Field	Description
VTP Version capable	Displays the VTP versions that are capable of operating on the controller.
VTP Version running	Displays the VTP version operating on the controller. By default, the controller implements Version 1 but can be set to Version 2.
VTP Domain Name	Name that identifies the administrative domain for the controller.
VTP Pruning Mode	Displays whether pruning is enabled or disabled. Enabling pruning on a VTP server enables pruning for the entire management domain. Pruning restricts flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.
VTP Traps Generation	Displays whether VTP traps are sent to a network management station.
Device ID	Displays the MAC address of the local device.
Configuration last modified	Displays the date and time of the last configuration modification. Displays the IP address of the controller that caused the configuration change to the database.

Field	Description
VTP Operating Mode	<p>Displays the VTP operating mode, which can be server, client, or transparent.</p> <p><b>Server</b>—A controller in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The controller guarantees that it can recover all the VLAN information in the current VTP database from NVRAM after reboot. By default, every controller is a VTP server.</p> <p><b>Note</b> The controller automatically changes from VTP server mode to VTP client mode if it detects a failure while writing the configuration to NVRAM and cannot return to server mode until the NVRAM is functioning.</p> <p><b>Client</b>—A controller in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.</p> <p><b>Transparent</b>—A controller in VTP transparent mode is disabled for VTP, does not send or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The controller receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.</p>
Maximum VLANs Supported Locally	Maximum number of VLANs supported locally.
Number of Existing VLANs	Number of existing VLANs.
Configuration Revision	Current configuration revision number on this controller.
MD5 Digest	A 16-byte checksum of the VTP configuration.

This is an example of output from the **show vtp status** command for a controller running VTP version 3:

```

Controller> show vtp status
VTP Version capable : 1 to 3
VTP version running : 3
VTP Domain Name : Cisco
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 0021.1bcd.c700

Feature VLAN:

```

```

-----
VTP Operating Mode : Server
Number of existing VLANs : 7
Number of existing extended VLANs : 0
Configuration Revision : 0
Primary ID : 0000.0000.0000
Primary Description :
MD5 digest : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Feature MST:
-----
VTP Operating Mode : Client
Configuration Revision : 0
Primary ID : 0000.0000.0000
Primary Description :
MD5 digest : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Feature UNKNOWN:
-----

```

**Related Commands**

Command	Description
<a href="#">clear vtp counters</a>	Clears the VLAN Trunking Protocol (VTP) and pruning counters.



## show wireless vlan group

To display the detailed list of VLANs in a VLAN group and the status of the DHCP failed vlans, use the **show wireless vlan group** command in privileged EXEC mode.

**show wireless vlan group** *group-name*

### Syntax Description

<i>group-name</i>	Name of the wireless VLAN group.
-------------------	----------------------------------

### Command Default

None

### Command Modes

Privileged EXEC

### Command History

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

### Usage Guidelines

Enter this command in the global configuration mode only.

### Examples

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

```
Controller# show wireless vlan group grp1
```

```
Member Vlans Configured
```

VLAN	VLAN Name	DHCP Failed
100	VLAN0100	No
101	VLAN0101	Yes
102	VLAN0102	No
103	VLAN0103	No
104	VLAN0104	Yes
105	VLAN0105	No

## spanning-tree vlan

To configure spanning tree on a per-VLAN basis, use the **spanning-tree vlan** command in global configuration mode on the switch stack or on a standalone switch. To return to the default setting, use the **no** form of this command.

**spanning-tree vlan** *vlan-id* [**forward-time** *seconds*] **hello-time** *seconds* | **max-age** *seconds* | **priority** *priority* | **root** {**primary** | **secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]]

**no spanning-tree vlan** *vlan-id* [**forward-time** | **hello-time** | **max-age** | **priority** | **root**]

### Syntax Description

<i>vlan-id</i>	VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
<b>forward-time</b> <i>seconds</i>	(Optional) Sets the forward-delay time for the specified spanning-tree instance. The forwarding time specifies how long each of the listening and learning states last before the interface begins forwarding. The range is 4 to 30 seconds.
<b>hello-time</b> <i>seconds</i>	(Optional) Sets the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds.
<b>max-age</b> <i>seconds</i>	(Optional) Sets the interval between messages the spanning tree receives from the root switch. If a switch does not receive a BPDU message from the root switch within this interval, it recomputes the spanning-tree topology. The range is 6 to 40 seconds.
<b>priority</b> <i>priority</i>	(Optional) Sets the switch priority for the specified spanning-tree instance. This setting affects the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch.  The range is 0 to 61440 in increments of 4096. Valid priority values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.
<b>root primary</b>	(Optional) Forces this switch to be the root switch.
<b>root secondary</b>	(Optional) Sets this switch to be the root switch should the primary root switch fail.
<b>diameter</b> <i>net-diameter</i>	(Optional) Sets the maximum number of switches between any two end stations. The range is 2 to 7.

### Command Default

Spanning tree is enabled on all VLANs.

The forward-delay time is 15 seconds.

The hello time is 2 seconds.

The max-age is 20 seconds.

The primary root switch priority is 24576.

The secondary root switch priority is 28672.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

Disabling the STP causes the VLAN to stop participating in the spanning-tree topology. Interfaces that are administratively down remain down. Received BPDUs are forwarded like other multicast frames. The VLAN does not detect and prevent loops when STP is disabled.

You can disable the STP on a VLAN that is not currently active and verify the change by using the **show running-config** or the **show spanning-tree vlan *vlan-id*** privileged EXEC command. The setting takes effect when the VLAN is activated.

When disabling or reenabling the STP, you can specify a range of VLANs that you want to disable or enable.

When a VLAN is disabled and then enabled, all assigned VLANs continue to be its members. However, all spanning-tree bridge parameters are returned to their previous settings (the last setting before the VLAN was disabled).

You can enable spanning-tree options on a VLAN that has no interfaces assigned to it. The setting takes effect when you assign interfaces to it.

When setting the **max-age *seconds***, if a switch does not receive BPDUs from the root switch within the specified interval, it recomputes the spanning-tree topology. The max-age setting must be greater than the hello-time setting.

The **spanning-tree vlan *vlan-id* root** command should be used only on backbone switches.

When you enter the **spanning-tree vlan *vlan-id* root** command, the software checks the switch priority of the current root switch for each VLAN. Because of the extended system ID support, the switch sets the switch priority for the specified VLAN to 24576 if this value will cause this switch to become the root for the specified VLAN. If any root switch for the specified VLAN has a switch priority lower than 24576, the switch sets its own priority for the specified VLAN to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree vlan *vlan-id* root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch should fail, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768, and therefore, are unlikely to become the root switch).

## Examples

This example shows how to disable the STP on VLAN 5:

```
Controller(config)# no spanning-tree vlan 5
```

You can verify your setting by entering the **show spanning-tree** privileged EXEC command. In this instance, VLAN 5 does not appear in the list.

This example shows how to set the spanning-tree forwarding time to 18 seconds for VLANs 20 and 25:

```
Controller(config) # spanning-tree vlan 20,25 forward-time 18
```

This example shows how to set the spanning-tree hello-delay time to 3 seconds for VLANs 20 to 24:

```
Controller(config) # spanning-tree vlan 20-24 hello-time 3
```

This example shows how to set spanning-tree max-age to 30 seconds for VLAN 20:

```
Controller(config) # spanning-tree vlan 20 max-age 30
```

This example shows how to reset the max-age parameter to the default value for spanning-tree instance 100 and 105 to 108:

```
Controller(config) # no spanning-tree vlan 100, 105-108 max-age
```

This example shows how to set the spanning-tree priority to 8192 for VLAN 20:

```
Controller(config) # spanning-tree vlan 20 priority 8192
```

This example shows how to configure the switch as the root for VLAN 10 with a network diameter of 4:

```
Controller(config) # spanning-tree vlan 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for VLAN 10 with a network diameter of 4:

```
Controller(config) # spanning-tree vlan 10 root secondary diameter 4
```

You can verify your settings by entering the **show spanning-tree vlan *vlan-id*** privileged EXEC command.

## wireless broadcast vlan

To enable broadcast support on a VLAN, use the **wireless broadcast vlan** command in global configuration mode. To disable Ethernet broadcast support, use the **no** form of the command.

**wireless broadcast vlan** [*vlan-id*]

**no wireless broadcast vlan** [*vlan-id*]

### Syntax Description

<i>vlan-id</i>	(Optional) Specifies the VLAN ID to enable broadcast support to that VLAN. The value ranges from 1 to 4095.
----------------	---

### Command Default

None

### Command Modes

Global configuration mode

### Command History

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

### Usage Guidelines

Use this command in the global configuration mode only.

### Examples

This example shows how to enable broadcasting on VLAN 20:

```
Controller(config)# wireless broadcast vlan 20
```

# wireless vlan group

To create a wireless VLAN group, use the **wlan group** command in interface configuration mode.

**wlan group** *group-name* **wlan-list** *vlan-id*

Syntax Description	<i>group-name</i>	Name of the VLAN group.
	<i>vlan-id</i>	Range of the VLAN IDs to be added to the group.
Command Default	None	
Command Modes	Interface configuration	
Command History	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 3.2SECisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines** The VLAN must be available to be grouped.

**Examples** This example shows how to map VLANs 91 through 125 to a wireless VLAN group:

```
Controller(config)# wireless vlan group grp1 vlan-list 91-125
```

# wlan

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

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

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

## Syntax Description

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

## Command Default

WLAN is disabled.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

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

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

## Examples

This example shows how to create a WLAN:

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

This example shows how to delete a WLAN:

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







## INDEX

### C

clear vmps statistics command [15](#)  
clear vtp counters command [16](#)  
client vlan command [14](#)

### D

debug sw-vlan command [17](#)  
debug sw-vlan ifs command [19](#)  
debug sw-vlan notification command [20](#)  
debug sw-vlan vtp command [22](#)

### I

interface vlan command [24](#)

### R

remote-span command [26](#)

### S

show vlan command [28](#)  
show vlan filter command [32](#)  
show vlan group command [33](#)  
show vtp command [34](#)  
show wireless vlan group command [41, 46](#)  
spanning-tree vlan command [42](#)

### W

wireless broadcast vlan command [45](#)  
wlan command [47](#)

