VLAN Command Reference, Cisco IOS Release 15.2(2)E (Catalyst 2960-XR Switch)

First Published: January 15, 2016

Last Modified: January 15, 2016

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:

© 2016 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Document Conventions

This document uses the following conventions:

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

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

Reader Alert Conventions

This document may use the following conventions for reader alerts:

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

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Documentation

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

- Catalyst 2960-XR Switch documentation, located at:

  http://www.cisco.com/go/cat2960xr_docs

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

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

- Error Message Decoder, located at:

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

Obtaining Documentation and Submitting a Service Request

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

http://www.cisco.com/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

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 switch reboots.

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

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

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

Table 1: Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session using Telnet, SSH, or console.	`Switch>`	Enter **logout** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	While in user EXEC mode, enter the **enable** command.	`Switch#`	Enter **disable** to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	`Switch(config)#`	To exit to privileged EXEC mode, enter **exit** or **end**, or press **Ctrl-Z**.	Use this mode to configure parameters that apply to the entire switch.
VLAN configuration	While in global configuration mode, enter the **vlan** *vlan-id* command.	`Switch(config-vlan)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the switch startup configuration file.
Interface configuration	While in global configuration mode, enter the **interface** command (with a specific interface).	`Switch(config-if)#`		Use this mode to configure parameters for the Ethernet ports.

Mode	Access Method	Prompt	Exit Method	About This Mode
			To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	
Line configuration	While in global configuration mode, specify a line with the **line vty** or **line console** command.	`Switch(config-line)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure parameters for the terminal line.

Understanding Abbreviated Commands

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

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

```
Switch# show conf
```

No and Default Forms of Commands

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

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

CLI Error Messages

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

Table 2: Common CLI Error Messages

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

Configuration Logging

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

Note Only CLI or HTTP changes are logged.

Using the Help System

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**help** **Example:** `Switch# help`	Obtains a brief description of the help system in any command mode.

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

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

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

Step 6	*command keyword* **?**
	
	Example:
	`Switch(config)# cdp holdtime ?`
	`<10-255> Length of time (in sec) that receiver must keep this packet`
		Lists the associated arguments for a keyword.

How to Use the CLI to Configure Features

Configuring the Command History

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

Changing the Command History Buffer Size

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**terminal history** [**size** *number-of-lines*] **Example:** `Switch# terminal history size 200`	Changes the number of command lines that the switch records during the current terminal session in privileged EXEC mode. You can configure the size from 0 to 256.

Recalling Commands

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**Ctrl-P** or use the **up arrow** key	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Step 2	**Ctrl-N** or use the **down arrow** key	Returns to more recent commands in the history buffer after recalling commands with **Ctrl-P** or the up arrow key. Repeat the key sequence to recall successively more recent commands.
Step 3	**show history** **Example:** `Switch# show history`	Lists the last several commands that you just entered in privileged EXEC mode. The number of commands that appear is controlled by the setting of the **terminal history** global configuration command and the **history** line configuration command.

Disabling the Command History Feature

The command history feature is automatically enabled. You can disable it for the current terminal session or for the command line. This procedure is optional.

SUMMARY STEPS

1. **terminal no history**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**terminal no history** **Example:** `Switch# terminal no history`	Disables the feature during the current terminal session in privileged EXEC mode.

Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it and reenable it.

SUMMARY STEPS

1. **terminal editing**
2. **terminal no editing**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**terminal editing** **Example:** `Switch# terminal editing`	Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.
Step 2	**terminal no editing** **Example:** `Switch# terminal no editing`	Disables the enhanced editing mode for the current terminal session in privileged EXEC mode.

Editing Commands Through Keystrokes

The keystrokes help you to edit the command lines. These keystrokes are optional.

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

Table 3: Editing Commands

Editing Commands	Description
Ctrl-B or use the **left arrow** key	Moves the cursor back one character.
Ctrl-F or use the **right arrow** key	Moves the cursor forward one character.
Ctrl-A	Moves the cursor to the beginning of the command line.
Ctrl-E	Moves the cursor to the end of the command line.
Esc B	Moves the cursor back one word.
Esc F	Moves the cursor forward one word.
Ctrl-T	Transposes the character to the left of the cursor with the character located at the cursor.
Delete or **Backspace** key	Erases the character to the left of the cursor.
Ctrl-D	Deletes the character at the cursor.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.
Ctrl-U or **Ctrl-X**	Deletes all characters from the cursor to the beginning of the command line.
Ctrl-W	Deletes the word to the left of the cursor.
Esc D	Deletes from the cursor to the end of the word.
Esc C	Capitalizes at the cursor.
Esc L	Changes the word at the cursor to lowercase.
Esc U	Capitalizes letters from the cursor to the end of the word.

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

Editing Command Lines That Wrap

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

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**access-list** **Example:** `Switch(config)# access-list 101 permit tcp`	Displays the global configuration command entry that extends beyond one line. When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign ($) shows that the

	Command or Action	Purpose
	10.15.22.25 255.255.255.0 10.15.22.35 Switch(config)# $ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25 Switch(config)# $t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq Switch(config)# $15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45	line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.
Step 2	**Ctrl-A** **Example:** Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2$	Checks the complete syntax. The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right.
Step 3	**Return** key	Execute the commands. The software assumes that you have a terminal screen that is 80 columns wide. If you have a different width, use the **terminal width** privileged EXEC command to set the width of your terminal. Use line wrapping with the command history feature to recall and modify previous complex command entries.

Searching and Filtering Output of show and more Commands

You can search and filter the output for **show** and **more** commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see. Using these commands is optional.

SUMMARY STEPS

1. {**show** | **more**} *command* | {**begin** | **include** | **exclude**} *regular-expression*

DETAILED STEPS

	Command or Action	Purpose
Step 1	{**show**	**more**} *command*	{**begin**	**include**	**exclude**} *regular-expression* **Example:** Switch# show interfaces	include protocol Vlan1 is up, line protocol is up Vlan10 is up, line protocol is down GigabitEthernet1/0/1 is up, line protocol is down GigabitEthernet1/0/2 is up, line protocol is up	Searches and filters the output. Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain **output** are not displayed, but the lines that contain **output** appear.

Accessing the CLI on a Switch Stack

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

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

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

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

Accessing the CLI Through a Console Connection or Through Telnet

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

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

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

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

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

VLAN Commands

client vlan

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

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

no client vlan

Syntax Description

interface-id-name-or-group-name	Interface ID, name, or VLAN group name. The interface ID can also be in digits too.

Command Default

The default interface is configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

Usage Guidelines

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

Examples

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

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

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

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

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 15.0(2)EX1	This command was introduced.

Examples

This example shows how to clear the VTP counters:

```
Switch# clear vtp counters
```

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

Related Commands

Command	Description
show vtp	Displays general information about VTP management domain, status, and counters.

debug platform vlan

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

debug platform vlan {**error**| **mvid**| **rpc**}

no debug platform vlan {**error**| **mvid**| **rpc**}

Syntax Description

error	Displays VLAN error debug messages.
mvid	Displays mapped VLAN ID allocations and free debug messages.
rpc	Displays remote procedure call (RPC) debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

Usage Guidelines

The **undebug platform vlan** command is the same as the **no debug platform vlan** command.

Examples

This example shows how to display VLAN error debug messages:

```
Switch# debug platform vlan error
```

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**| **mapping**| **notification**| **packets**| **redundancy**| **registries**| **vtp**}

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

Syntax Description

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

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

Usage Guidelines

The **undebug 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:

```
Switch# debug sw-vlan events
```

Related Commands

Command	Description
debug sw-vlan ifs	Enables debugging of the VLAN manager IOS file system (IFS) error tests.
debug sw-vlan notification	Enables debugging of VLAN manager notifications.
debug sw-vlan vtp	Enables debugging of the VTP code.
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.
show vtp	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

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

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX1	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:

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

Related Commands

Command	Description
show vlan	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

accfwdchange	Displays debug messages for VLAN manager notification of aggregated access interface spanning-tree forward changes.
allowedvlancfgchange	Displays debug messages for VLAN manager notification of changes to the allowed VLAN configuration.
fwdchange	Displays debug messages for VLAN manager notification of spanning-tree forwarding changes.
linkchange	Displays debug messages for VLAN manager notification of interface link-state changes.
modechange	Displays debug messages for VLAN manager notification of interface mode changes.
pruningcfgchange	Displays debug messages for VLAN manager notification of changes to the pruning configuration.
statechange	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 15.0(2)EX1	This command was introduced.

Usage Guidelines

The **undebug 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:

```
Switch# debug sw-vlan notification
```

Related Commands

Command	Description
show vlan	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

events	Displays debug messages for general-purpose logic flow and detailed VTP messages generated by the VTP_LOG_RUNTIME macro in the VTP code.
packets	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.
pruning	Displays debug messages generated by the pruning segment of the VTP code.
packets	(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.
xmit	(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.
redundancy	Displays debug messages for VTP redundancy.
xmit	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 15.0(2)EX1	This command was introduced.

Usage Guidelines

The **undebug 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:

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

Related Commands

Command	Description
show vtp	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*

Syntax Description

vlan-id	VLAN number. The range is 1 to 4094.

Command Default

The default VLAN interface is VLAN 1.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX1	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:

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

Related Commands

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

show platform vlan

To display platform-dependent VLAN information, use the **show platform vlan** privileged EXEC command.

show platform vlan {**misc**| **mvid**| **prune**| **refcount**| **rpc** {**receive**| **transmit**}}

Syntax Description

misc	Displays miscellaneous VLAN module information.
mvid	Displays the mapped VLAN ID (MVID) allocation information.
prune	Displays the stack or platform-maintained pruning database.
refcount	Displays the VLAN lock module-wise reference counts.
rpc	Displays remote procedure call (RPC) messages.
receive	Displays received information.
transmit	Displays sent information.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

Usage Guidelines

Use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Examples

This example shows how to display remote procedure call (RPC) messages:

```
Switch# show platform vlan rpc
```

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*| **mtu**| **name** *vlan-name*| **remote-span**| **summary**]

Syntax Description

brief	(Optional) Displays one line for each VLAN with the VLAN name, status, and its ports.
group	(Optional) Displays information about VLAN groups.
id *vlan-id*	(Optional) Displays information about a single VLAN identified by the VLAN ID number. For *vlan-id*, the range is 1 to 4094.
mtu	(Optional) Displays a list of VLANs and the minimum and maximum transmission unit (MTU) sizes configured on ports in the VLAN.
name *vlan-name*	(Optional) Displays information about a single VLAN identified by the VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.
remote-span	(Optional) Displays information about Remote SPAN (RSPAN) VLANs.
summary	(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 15.0(2)EX1	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.

```
Switch> 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:

```
Switch> 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:

```
Switch# 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.
vlan	Adds a VLAN and enters the VLAN configuration mode.

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

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

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

Usage Guidelines

When you enter the **show vtp password** command when the switch 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 switch, the password appears in clear text.

- If the **password** *password* command did not specify the **hidden** keyword and encryption is enabled on the switch, 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 switches in the same domain do not have the same primary server for a database.

```
Switch# show vtp devices
Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Database Conf switch ID      Primary Server Revision   System Name
             lict
------------ ---- --------------- -------------- ---------- ----------------------
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.

```
Switch> 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
                                                   non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
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 switch 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 switch 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 switch 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 switch 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 switch 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 switch 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	Number of revision errors. 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 switch increments. Revision errors increment whenever the switch receives an advertisement whose revision number matches the revision number of the switch, but the MD5 digest values do not match. This error means that the VTP password in the two switches is different or that the switches have different configurations. These errors indicate that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.

Field	Description
Number of configuration digest errors	Number of MD5 digest errors. Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the switch do not match. This error usually means that the VTP password in the two switches is different. To solve this problem, make sure the VTP password on all switches is the same. These errors indicate that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.
Number of V1 summary errors	Number of Version 1 errors. Version 1 summary errors increment whenever a switch in VTP V2 mode receives a VTP Version 1 frame. These errors indicate that at least one neighboring switch is either running VTP Version 1 or VTP Version 2 with V2-mode disabled. To solve this problem, change the configuration of the switches in VTP V2-mode to disabled.
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.

```
Switch> 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 switch.
VTP Version running	Displays the VTP version operating on the switch. By default, the switch implements Version 1 but can be set to Version 2.
VTP Domain Name	Name that identifies the administrative domain for the switch.
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 switch that caused the configuration change to the database.

Field	Description
VTP Operating Mode	Displays the VTP operating mode, which can be server, client, or transparent. **Server—**A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch guarantees that it can recover all the VLAN information in the current VTP database from NVRAM after reboot. By default, every switch is a VTP server. **Note** The switch 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. **Client—**A switch 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. **Transparent—**A switch 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 switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.
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 switch.
MD5 Digest	A 16-byte checksum of the VTP configuration.

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

```
Switch# 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                       : 0cd9.9624.dd80

Feature VLAN:
--------------
VTP Operating Mode                : Off
Number of existing VLANs          : 11
```

```
Number of existing extended VLANs : 0
Maximum VLANs supported locally   : 1005

Feature MST:
--------------
VTP Operating Mode                : Transparent

Feature UNKNOWN:
--------------
VTP Operating Mode                : Transparent
```

Related Commands

Command	Description
clear vtp counters	Clears the VLAN Trunking Protocol (VTP) and pruning counters.

switchport priority extend

To set a port priority for the incoming untagged frames or the priority of frames received by the IP phone connected to the specified port, use the **switchport priority extend** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

switchport priority extend {**cos** *value*| **trust**}

no switchport priority extend

Syntax Description

cos *value*	Sets the IP phone port to override the IEEE 802.1p priority received from the PC or the attached device with the specified class of service (CoS) value. The range is 0 to 7. Seven is the highest priority. The default is 0.
trust	Sets the IP phone port to trust the IEEE 802.1p priority received from the PC or the attached device.

Command Default

The default port priority is set to a CoS value of 0 for untagged frames received on the port.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

Usage Guidelines

When voice VLAN is enabled, you can configure the switch to send the Cisco Discovery Protocol (CDP) packets to instruct the IP phone how to send data packets from the device attached to the access port on the Cisco IP Phone. You must enable CDP on the switch port connected to the Cisco IP Phone to send the configuration to the Cisco IP Phone. (CDP is enabled by default globally and on all switch interfaces.)

You should configure voice VLAN on switch access ports.

Before you enable voice VLAN, we recommend that you enable quality of service (QoS) on the switch by entering the **mls qos** global configuration command and configure the port trust state to trust by entering the **mls qos trust cos** interface configuration command.

Examples

This example shows how to configure the IP phone connected to the specified port to trust the received IEEE 802.1p priority:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport priority extend trust
```

You can verify your settings by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command.

switchport trunk

To set the trunk characteristics when the interface is in trunking mode, use the **switchport trunk** command in interface configuration mode. To reset a trunking characteristic to the default, use the **no** form of this command.

switchport trunk {**allowed vlan** *vlan-list*| **native vlan** *vlan-id*| **pruning vlan** *vlan-list*}

no switchport trunk {**allowed vlan**| **native vlan**| **pruning vlan**}

Syntax Description

allowed vlan *vlan-list*	Sets the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. See the Usage Guidelines for the *vlan-list* choices.
native vlan *vlan-id*	Sets the native VLAN for sending and receiving untagged traffic when the interface is in IEEE 802.1Q trunking mode. The range is 1 to 4094.
pruning vlan *vlan-list*	Sets the list of VLANs that are eligible for VTP pruning when in trunking mode. See the Usage Guidelines for the *vlan-list* choices.

Command Default

VLAN 1 is the default native VLAN ID on the port.

The default for all VLAN lists is to include all VLANs.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

Usage Guidelines

The *vlan-list* format is **all | none | [add | remove | except]** *vlan-atom* [,*vlan-atom*...]:

- **all** specifies all VLANs from 1 to 4094. This is the default. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
- **none** specifies an empty list. This keyword is not allowed on commands that require certain VLANs to be set or at least one VLAN to be set.
- **add** adds the defined list of VLANs to those currently set instead of replacing the list. Valid IDs are from 1 to 1005; extended-range VLANs (VLAN IDs greater than 1005) are valid in some cases.

Note You can add extended-range VLANs to the allowed VLAN list, but not to the pruning-eligible VLAN list.

Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.

- **remove** removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 1 to 1005; extended-range VLAN IDs are valid in some cases.

Note You can remove extended-range VLANs from the allowed VLAN list, but you cannot remove them from the pruning-eligible list.

- **except** lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.) Valid IDs are from 1 to 1005. Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- *vlan-atom* is either a single VLAN number from 1 to 4094 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.

Native VLANs:

- All untagged traffic received on an IEEE 802.1Q trunk port is forwarded with the native VLAN configured for the port.
- If a packet has a VLAN ID that is the same as the sending-port native VLAN ID, the packet is sent without a tag; otherwise, the switch sends the packet with a tag.
- The **no** form of the **native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.

Allowed VLAN:

- To reduce the risk of spanning-tree loops or storms, you can disable VLAN 1 on any individual VLAN trunk port by removing VLAN 1 from the allowed list. When you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), Dynamic Trunking Protocol (DTP), and VLAN Trunking Protocol (VTP) in VLAN 1.
- The **no** form of the **allowed vlan** command resets the list to the default list, which allows all VLANs.

Trunk pruning:

- The pruning-eligible list applies only to trunk ports.
- Each trunk port has its own eligibility list.
- If you do not want a VLAN to be pruned, remove it from the pruning-eligible list. VLANs that are pruning-ineligible receive flooded traffic.
- VLAN 1, VLANs 1002 to 1005, and extended-range VLANs (VLANs 1006 to 4094) cannot be pruned.

Examples

This example shows how to configure VLAN 3 as the default for the port to send all untagged traffic:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport trunk native vlan 3
```

This example shows how to add VLANs 1, 2, 5, and 6 to the allowed list:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

This example shows how to remove VLANs 3 and 10 to 15 from the pruning-eligible list:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport trunk pruning vlan remove 3,10-15
```

You can verify your settings by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command.

Related Commands

Command	Description
show interfaces	Displays the administrative and operational status of all interfaces or a specified interface.
switchport mode	Configures the VLAN membership mode of a port.

switchport voice vlan

To configure voice VLAN on the port, use the **switchport voice vlan** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

switchport voice vlan {*vlan-id* | **dot1p** | **none** | **untagged** | **name** *vlan_name*}

no switchport voice vlan

Syntax Description

vlan-id	The VLAN to be used for voice traffic. The range is 1 to 4094. By default, the IP phone forwards the voice traffic with an IEEE 802.1Q priority of 5.
dot1p	Configures the telephone to use IEEE 802.1p priority tagging and uses VLAN 0 (the native VLAN). By default, the Cisco IP phone forwards the voice traffic with an IEEE 802.1p priority of 5.
none	Does not instruct the IP telephone about the voice VLAN. The telephone uses the configuration from the telephone key pad.
untagged	Configures the telephone to send untagged voice traffic. This is the default for the telephone.
vlan *vlan_name*	(Optional) Specifies the VLAN name to be used for voice traffic. You can enter up to 128 characters.

Command Default

The default is not to automatically configure the telephone (**none**).

The telephone default is not to tag frames.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.
15.2(4)E	Option to specify a VLAN name for access and voice VLAN. The "**name**" keyword was added.

Usage Guidelines

You should configure voice VLAN on Layer 2 access ports.

You must enable Cisco Discovery Protocol (CDP) on the switch port connected to the Cisco IP phone for the switch to send configuration information to the phone. CDP is enabled by default globally and on the interface.

Before you enable voice VLAN, we recommend that you enable quality of service (QoS) on the switch by entering the **mls qos** global configuration command and configure the port trust state to trust by entering the **mls qos trust cos** interface configuration command.

When you enter a VLAN ID, the IP phone forwards voice traffic in IEEE 802.1Q frames, tagged with the specified VLAN ID. The switch puts IEEE 802.1Q voice traffic in the voice VLAN.

When you select **dot1p**, **none**, or **untagged**, the switch puts the indicated voice traffic in the access VLAN.

In all configurations, the voice traffic carries a Layer 2 IP precedence value. The default is 5 for voice traffic.

When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to 2. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but not on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the Cisco IP phone.

If any type of port security is enabled on the access VLAN, dynamic port security is automatically enabled on the voice VLAN.

You cannot configure static secure MAC addresses in the voice VLAN.

The Port Fast feature is automatically enabled when voice VLAN is configured. When you disable voice VLAN, the Port Fast feature is not automatically disabled.

Examples

This example show how to first populate the VLAN database by associating a VLAN ID with a VLAN name, and then configure the VLAN (using the name) on an interface, in the access mode: You can also verify your configuration by entering the **show interfaces** *interface-id* **switchport** in privileged EXEC command and examining information in the Voice VLAN: row.

Part 1 - Making the entry in the VLAN database:

```
Switch# configure terminal
Switch(config)# vlan 55
Switch(config-vlan)# name test
Switch(config-vlan)# end
Switch#
```

Part 2 - Checking the VLAN database:

```
Switch# show vlan id 55
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
55 test active
VLAN Type  SAID   MTU  Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ------ ---- ------ ------ -------- --- -------- ------ ------
55   enet  100055 1500 -      -      -        -   -        0      0
Remote SPAN VLAN
----------------
Disabled
Primary Secondary Type Ports
------- --------- ----------------- ------------------------------------------
```

Part 3- Setting the VLAN on the interface, by using the vlan_name 'test':

```
Switch# configure terminal
Switch(config)# interface gigabitethernet5/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan name test
Switch(config-if)# end
Switch#
```

Part 4 - Verifying running-config:

```
Switch# show running-config
interface gigabitethernet5/1
```

```
Building configuration...
Current configuration : 113 bytes
!
interface GigabitEthernet5/1
switchport voice vlan 55
switchport mode access
Switch#
```

Part 5 - Also can be verified in interface switchport:

```
Switch# show interface GigabitEthernet5/1 switchport
Name: Gi5/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 55 (test)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Switch#
```

Related Commands

Command	Description
show interfaces	Displays the administrative and operational status of all interfaces or a specified interface.
switchport priority extend	Sets a port priority for the incoming untagged frames or the priority of frames received by the IP phone connected to the specified port.

vlan

To add a VLAN and to enter the VLAN configuration mode, use the **vlan** command in global configuration mode. To delete the VLAN, use the **no** form of this command.

vlan *vlan-id*

no vlan *vlan-id*

Syntax Description

vlan-id	ID of the VLAN to be added and configured. The range is 1 to 4094. You can enter a single VLAN ID, a series of VLAN IDs separated by commas, or a range of VLAN IDs separated by hyphens.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

Usage Guidelines

You can use the **vlan** *vlan-id* global configuration command to add normal-range VLANs (VLAN IDs 1 to 1005) or extended-range VLANs (VLAN IDs 1006 to 4094). Configuration information for normal-range VLANs is always saved in the VLAN database, and you can display this information by entering the **show vlan** privileged EXEC command. If the VTP mode is transparent, VLAN configuration information for normal-range VLANs is also saved in the switch running configuration file. VLAN IDs in the extended range are not saved in the VLAN database, but they are stored in the switch running configuration file, and you can save the configuration in the startup configuration file.

VTP version 3 supports propagation of extended-range VLANs. VTP versions 1 and 2 propagate only VLANs 1 to 1005.

When you save the VLAN and VTP configurations in the startup configuration file and reboot the switch, the configuration is selected as follows:

- If the VTP mode is transparent in the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode or domain name in the startup configuration do not match the VLAN database, the domain name and VTP mode and configuration for VLAN IDs 1 to 1005 use the VLAN database information.

If you enter an invalid VLAN ID, you receive an error message and do not enter VLAN configuration mode.

Entering the **vlan** command with a VLAN ID enables VLAN configuration mode. When you enter the VLAN ID of an existing VLAN, you do not create a new VLAN, but you can modify VLAN parameters for that VLAN. The specified VLANs are added or modified when you exit the VLAN configuration mode. Only the **shutdown** command (for VLANs 1 to 1005) takes effect immediately.

Note Although all commands are visible, the only VLAN configuration command that is supported on extended-range VLANs is **remote-span**. For extended-range VLANs, all other characteristics must remain at the default state.

These configuration commands are available in VLAN configuration mode. The **no** form of each command returns the characteristic to its default state:

- **are** *are-number*—Defines the maximum number of all-routes explorer (ARE) hops for this VLAN. This keyword applies only to TrCRF VLANs. The range is 0 to 13. The default is 7. If no value is entered, 0 is assumed to be the maximum.
- **backupcrf**—Specifies the backup CRF mode. This keyword applies only to TrCRF VLANs.
  - **enable**—Backup CRF mode for this VLAN.
  - **disable**—Backup CRF mode for this VLAN (the default).
- **bridge** {*bridge-number* | **type**}—Specifies the logical distributed source-routing bridge, the bridge that interconnects all logical rings that have this VLAN as a parent VLAN in FDDI-NET, Token Ring-NET, and TrBRF VLANs. The range is 0 to 15. The default bridge number is 0 (no source-routing bridge) for FDDI-NET, TrBRF, and Token Ring-NET VLANs. The **type** keyword applies only to TrCRF VLANs and is one of these:
  - **srb**—Ssource-route bridging
  - **srt**—Source-route transparent) bridging VLAN
- **exit**—Applies changes, increments the VLAN database revision number (VLANs 1 to 1005 only), and exits VLAN configuration mode.
- **media**—Defines the VLAN media type and is one of these:

  Note The switch supports only Ethernet ports. You configure only FDDI and Token Ring media-specific characteristics for VLAN Trunking Protocol (VTP) global advertisements to other switches. These VLANs are locally suspended.

  - **ethernet**—Ethernet media type (the default).
  - **fd-net**—FDDI network entity title (NET) media type.
  - **fddi**—FDDI media type.
  - **tokenring**—Token Ring media type if the VTP v2 mode is disabled, or TrCRF if the VTP Version 2 (v) mode is enabled.

- **tr-net**—Token Ring network entity title (NET) media type if the VTP v2 mode is disabled or TrBRF media type if the VTP v2 mode is enabled.

See the table that follows for valid commands and syntax for different media types.

- **name** *vlan-name*—Names the VLAN with an ASCII string from 1 to 32 characters that must be unique within the administrative domain. The default is VLANxxxx where xxxx represents four numeric digits (including leading zeros) equal to the VLAN ID number.
- **no**—Negates a command or returns it to the default setting.
- **parent** *parent-vlan-id*—Specifies the parent VLAN of an existing FDDI, Token Ring, or TrCRF VLAN. This parameter identifies the TrBRF to which a TrCRF belongs and is required when defining a TrCRF. The range is 0 to 1005. The default parent VLAN ID is 0 (no parent VLAN) for FDDI and Token Ring VLANs. For both Token Ring and TrCRF VLANs, the parent VLAN ID must already exist in the database and be associated with a Token Ring-NET or TrBRF VLAN.
- **remote-span**—Configures the VLAN as a Remote SPAN (RSPAN) VLAN. When the RSPAN feature is added to an existing VLAN, the VLAN is first deleted and is then recreated with the RSPAN feature. Any access ports are deactivated until the RSPAN feature is removed. If VTP is enabled, the new RSPAN VLAN is propagated by VTP for VLAN IDs that are lower than 1024. Learning is disabled on the VLAN.
- **ring** *ring-number*—Defines the logical ring for an FDDI, Token Ring, or TrCRF VLAN. The range is 1 to 4095. The default for Token Ring VLANs is 0. For FDDI VLANs, there is no default.
- **said** *said-value*—Specifies the security association identifier (SAID) as documented in IEEE 802.10. The range is 1 to 4294967294, and the number must be unique within the administrative domain. The default value is 100000 plus the VLAN ID number.
- **shutdown**—Shuts down VLAN switching on the VLAN. This command takes effect immediately. Other commands take effect when you exit VLAN configuration mode.
- **state**—Specifies the VLAN state:
  - **active** means the VLAN is operational (the default).
  - **suspend** means the VLAN is suspended. Suspended VLANs do not pass packets.
- **ste** *ste-number*—Defines the maximum number of spanning-tree explorer (STE) hops. This keyword applies only to TrCRF VLANs. The range is 0 to 13. The default is 7.
- **stp type**—Defines the spanning-tree type for FDDI-NET, Token Ring-NET, or TrBRF VLANs. For FDDI-NET VLANs, the default STP type is ieee. For Token Ring-NET VLANs, the default STP type is ibm. For FDDI and Token Ring VLANs, the default is no type specified.
  - **ieee**—IEEE Ethernet STP running source-route transparent (SRT) bridging.
  - **ibm**—IBM STP running source-route bridging (SRB).
  - **auto**—STP running a combination of source-route transparent bridging (IEEE) and source-route bridging (IBM).
- **tb-vlan1** *tb-vlan1-id* and **tb-vlan2** *tb-vlan2-id*—Specifies the first and second VLAN to which this VLAN is translationally bridged. Translational VLANs translate FDDI or Token Ring to Ethernet, for example. The range is 0 to 1005. If no value is specified, 0 (no transitional bridging) is assumed.

Table 7: Valid Commands and Syntax for Different Media Types

Media Type	Valid Syntax
Ethernet	**name** *vlan-name*, **media ethernet**, **state** {**suspend** | **active**}, **said** *said-value*, **remote-span**, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
FDDI	**name** *vlan-name*, **media fddi**, **state** {**suspend** | **active**}, **said** *said-value*, **ring** *ring-number*, **parent** *parent-vlan-id*, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
FDDI-NET	**name** *vlan-name*, **media fd-net** , **state** {**suspend** | **active**}, **said** *said-value*, **bridge** *bridge-number*, **stp type** {**ieee** | **ibm** | **auto**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id* If VTP v2 mode is disabled, do not set the **stp type** to **auto.**
Token Ring	VTP v1 mode is enabled. **name** *vlan-name*, **media tokenring**, **state** {**suspend** | **active**}, **said** *said-value*, **ring** *ring-number*, **parent** *parent-vlan-id*, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
Token Ring concentrator relay function (TrCRF)	VTP v2 mode is enabled. **name** *vlan-name*, **media tokenring**, **state** {**suspend** | **active**}, **said** *said-value*, **ring** *ring-number*, **parent** *parent-vlan-id*, **bridge type** {**srb** | **srt**}, **are** *are-number*, **ste** *ste-number*, **backupcrf** {**enable** | **disable**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
Token Ring-NET	VTP v1 mode is enabled. **name** *vlan-name*, **media tr-net**, **state** {**suspend** | **active**}, **said** *said-value*, **bridge** *bridge-number*, **stp type** {**ieee** | **ibm**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
Token Ring bridge relay function (TrBRF)	VTP v2 mode is enabled. **name** *vlan-name*, **media tr-net**, **state** {**suspend** | **active**}, **said** *said-value*, **bridge** *bridge-number*, **stp type** {**ieee** | **ibm** | **auto**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*

The following table describes the rules for configuring VLANs:

Table 8: VLAN Configuration Rules

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrCRF VLAN media type.	Specify a parent VLAN ID of a TrBRF that already exists in the database. Specify a ring number. Do not leave this field blank. Specify unique ring numbers when TrCRF VLANs have the same parent VLAN ID. Only one backup concentrator relay function (CRF) can be enabled.
VTP v2 mode is enabled, and you are configuring VLANs other than TrCRF media type.	Do not specify a backup CRF.
VTP v2 mode is enabled, and you are configuring a TrBRF VLAN media type.	Specify a bridge number. Do not leave this field blank.
VTP v1 mode is enabled.	No VLAN can have an STP type set to auto. This rule applies to Ethernet, FDDI, FDDI-NET, Token Ring, and Token Ring-NET VLANs.
Add a VLAN that requires translational bridging (values are not set to zero).	The translational bridging VLAN IDs that are used must already exist in the database. The translational bridging VLAN IDs that a configuration points to must also contain a pointer to the original VLAN in one of the translational bridging parameters (for example, Ethernet points to FDDI, and FDDI points to Ethernet). The translational bridging VLAN IDs that a configuration points to must be different media types than the original VLAN (for example, Ethernet can point to Token Ring). If both translational bridging VLAN IDs are configured, these VLANs must be different media types (for example, Ethernet can point to FDDI and Token Ring).

Examples

This example shows how to add an Ethernet VLAN with default media characteristics. The default includes a *vlan-name* of VLAN *xxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number. The default media is ethernet; the state is active. The default said-value is 100000 plus the VLAN ID; the mtu-size variable is 1500; the stp-type is ieee. When you enter the **exit** VLAN configuration command, the VLAN is added if it did not already exist; otherwise, this command does nothing.

This example shows how to create a new VLAN with all default characteristics and enter VLAN configuration mode:

```
Switch(config)# vlan 200
Switch(config-vlan)# exit
```

```
Switch(config)#
```

This example shows how to create a new extended-range VLAN with all the default characteristics, to enter VLAN configuration mode, and to save the new VLAN in the switch startup configuration file:

```
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

You can verify your setting by entering the **show vlan** privileged EXEC command.

Related Commands

Command	Description
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.

vtp (global configuration)

To set or modify the VLAN Trunking Protocol (VTP) configuration characteristics, use the **vtp** command in global configuration mode. To remove the settings or to return to the default settings, use the **no** form of this command.

vtp {**domain** *domain-name*| **file** *filename*| **interface** *interface-name* [**only**]| **mode** {**client**| **off**| **server**| **transparent**} [**mst**| **unknown**| **vlan**]| **password** *password* [**hidden**| **secret**]| **pruning**| **version** *number*}

no vtp {**file**| **interface**| **mode** [**client**| **off**| **server**| **transparent**] [**mst**| **unknown**| **vlan**]| **password**| **pruning**| **version**}

Syntax Description

domain *domain-name*	Specifies the VTP domain name, an ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the switch. The domain name is case sensitive.
file *filename*	Specifies the Cisco IOS file system file where the VTP VLAN configuration is stored.
interface *interface-name*	Specifies the name of the interface providing the VTP ID updated for this device.
only	(Optional) Uses only the IP address of this interface as the VTP IP updater.
mode	Specifies the VTP device mode as client, server, or transparent.
client	Places the switch in VTP client mode. A switch in VTP client mode is enabled for VTP, and can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on a VTP client. VLANs are configured on another switch in the domain that is in server mode. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.
off	Places the switch in VTP off mode. A switch in VTP off mode functions the same as a VTP transparent device except that it does not forward VTP advertisements on trunk ports.
server	Places the switch in VTP server mode. A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on the switch. The switch can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot.
transparent	Places the switch in VTP transparent mode. A switch in VTP transparent mode is disabled for VTP, does not send advertisements or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received. When VTP mode is transparent, the mode and domain name are saved in the switch running configuration file, and you can save them in the switch startup configuration file by entering the **copy running-config startup config** privileged EXEC command.

mst	(Optional) Sets the mode for the multiple spanning tree (MST) VTP database (only VTP Version 3).
unknown	(Optional) Sets the mode for unknown VTP databases (only VTP Version 3).
vlan	(Optional) Sets the mode for VLAN VTP databases. This is the default (only VTP Version 3).
password *password*	Sets the administrative domain password for the generation of the 16-byte secret value used in MD5 digest calculation to be sent in VTP advertisements and to validate received VTP advertisements. The password can be an ASCII string from 1 to 32 characters. The password is case sensitive.
hidden	(Optional) Specifies that the key generated from the password string is saved in the VLAN database file. When the **hidden** keyword is not specified, the password string is saved in clear text. When the hidden password is entered, you need to reenter the password to issue a command in the domain. This keyword is supported only in VTP Version 3.
secret	(Optional) Allows the user to directly configure the password secret key (only VTP Version 3).
pruning	Enables VTP pruning on the switch.
version *number*	Sets the VTP Version to Version 1, Version 2, or Version 3.

Command Default

The default filename is *flash:vlan.dat*.

The default mode is server mode and the default database is VLAN.

In VTP Version 3, for the MST database, the default mode is transparent.

No domain name or password is defined.

No password is configured.

Pruning is disabled.

The default version is Version 1.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

Usage Guidelines

When you save VTP mode, domain name, and VLAN configurations in the switch startup configuration file and reboot the switch, the VTP and VLAN configurations are selected by these conditions:

- If the VTP mode is transparent in the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode or domain name in the startup configuration do not match the VLAN database, the domain name and VTP mode and configuration for VLAN IDs 1 to 1005 use the VLAN database information.

The **vtp file** *filename* cannot be used to load a new database; it renames only the file in which the existing database is stored.

Follow these guidelines when configuring a VTP domain name:

- The switch is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the switch does not send any VTP advertisements even if changes occur to the local VLAN configuration. The switch leaves the no-management-domain state after it receives the first VTP summary packet on any port that is trunking or after you configure a domain name by using the **vtp domain** command. If the switch receives its domain from a summary packet, it resets its configuration revision number to 0. After the switch leaves the no-management-domain state, it cannot be configured to reenter it until you clear the NVRAM and reload the software.
- Domain names are case-sensitive.
- After you configure a domain name, it cannot be removed. You can only reassign it to a different domain.

Follow these guidelines when setting VTP mode:

- The **no vtp mode** command returns the switch to VTP server mode.
- The **vtp mode server** command is the same as **no vtp mode** except that it does not return an error if the switch is not in client or transparent mode.
- If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. If you have switches in client mode, be sure to make all VTP or VLAN configuration changes on a switch in server mode, as it has a higher VTP configuration revision number. If the receiving switch is in transparent mode, the switch configuration is not changed.
- A switch in transparent mode does not participate in VTP. If you make VTP or VLAN configuration changes on a switch in transparent mode, the changes are not propagated to other switches in the network.
- If you change the VTP or VLAN configuration on a switch that is in server mode, that change is propagated to all the switches in the same VTP domain.
- The **vtp mode transparent** command disables VTP from the domain but does not remove the domain from the switch.
- In VTP Versions 1 and 2, the VTP mode must be transparent for VTP and VLAN information to be saved in the running configuration file.
- With VTP Versions 1 and 2, you cannot change the VTP mode to client or server if extended-range VLANs are configured on the switch. Changing the VTP mode is allowed with extended VLANs in VTP Version 3.
- The VTP mode must be transparent for you to add extended-range VLANs or for VTP and VLAN information to be saved in the running configuration file.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.

- The **vtp mode off** command sets the device to off. The **no vtp mode off** command resets the device to the VTP server mode.

Follow these guidelines when setting a VTP password:

- Passwords are case sensitive. Passwords should match on all switches in the same domain.
- When you use the **no vtp password** form of the command, the switch returns to the no-password state.
- The **hidden** and **secret** keywords are supported only in VTP Version 3. If you convert from VTP Version 2 to VTP Version 3, you must remove the hidden or secret keyword before the conversion.

Follow these guidelines when setting VTP pruning:

- VTP pruning removes information about each pruning-eligible VLAN from VTP updates if there are no stations belonging to that VLAN.
- If you enable pruning on the VTP server, it is enabled for the entire management domain for VLAN IDs 1 to 1005.
- Only VLANs in the pruning-eligible list can be pruned.
- Pruning is supported with VTP Version 1 and Version 2.

Follow these guidelines when setting the VTP version:

- Toggling the Version 2 (v2) mode state modifies parameters of certain default VLANs.
- Each VTP switch automatically detects the capabilities of all the other VTP devices. To use Version 2, all VTP switches in the network must support Version 2; otherwise, you must configure them to operate in VTP Version 1 mode.
- If all switches in a domain are VTP Version 2-capable, you only need to configure Version 2 on one switch; the version number is then propagated to the other Version-2 capable switches in the VTP domain.
- If you are using VTP in a Token Ring environment, VTP Version 2 must be enabled.
- If you are configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, you must use Version 2.
- If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use Version 1.
- In VTP Version 3, all database VTP information is propagated across the VTP domain, not only VLAN database information.
- Two VTP Version 3 regions can only communicate over a VTP Version 1 or VTP Version 2 region in transparent mode.

You cannot save password, pruning, and version configurations in the switch configuration file.

Examples

This example shows how to rename the filename for VTP configuration storage to vtpfilename:

```
Switch(config)# vtp file vtpfilename
```

This example shows how to clear the device storage filename:

```
Switch(config)# no vtp file vtpconfig
Clearing device storage filename.
```

This example shows how to specify the name of the interface providing the VTP updater ID for this device:

```
Switch(config)# vtp interface gigabitethernet
```

This example shows how to set the administrative domain for the switch:

```
Switch(config)# vtp domain OurDomainName
```

This example shows how to place the switch in VTP transparent mode:

```
Switch(config)# vtp mode transparent
```

This example shows how to configure the VTP domain password:

```
Switch(config)# vtp password ThisIsOurDomainsPassword
```

This example shows how to enable pruning in the VLAN database:

```
Switch(config)# vtp pruning
Pruning switched ON
```

This example shows how to enable Version 2 mode in the VLAN database:

```
Switch(config)# vtp version 2
```

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

Related Commands

Command	Description
show vtp	Displays general information about VTP management domain, status, and counters.
vtp (interface configuration)	Enables or disables VTP on an interface.

vtp (interface configuration)

To enable the VLAN Trunking Protocol (VTP) on a per-port basis, use the **vtp** command in interface configuration mode. To disable VTP on the interface, use the **no** form of this command.

vtp

no vtp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

Usage Guidelines

Enter this command only on interfaces that are in trunking mode.

Examples

This example shows how to enable VTP on an interface:

```
Switch(config-if)# vtp
```

This example shows how to disable VTP on an interface:

```
Switch(config-if)# no vtp
```

Related Commands

Command	Description
switchport trunk	Configures the trunk characteristics when an interface is in trunking mode.
vtp (global configuration)	Globally configures VTP domain name, password, pruning, version, and mode.

vtp primary

To configure a switch as the VLAN Trunking Protocol (VTP) primary server, use the **vtp primary** command in privileged EXEC mode.

vtp primary [**mst**| **vlan**] **[force]**

Syntax Description

mst	(Optional) Configures the switch as the primary VTP server for the multiple spanning tree (MST) feature.
vlan	(Optional) Configures the switch as the primary VTP server for VLANs.
force	(Optional) Configures the switch to not check for conflicting devices when configuring the primary server.

Command Default

The switch is a VTP secondary server.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

Usage Guidelines

A VTP primary server updates the database information and sends updates that are honored by all devices in the system. A VTP secondary server can only back up the updated VTP configurations received from the primary server to NVRAM.

By default, all devices come up as secondary servers. Primary server status is needed only for database updates when the administrator issues a takeover message in the domain. You can have a working VTP domain without any primary servers.

Primary server status is lost if the device reloads or domain parameters change.

Note This command is supported only when the switch is running VTP Version 3.

Examples

This example shows how to configure the switch as the primary VTP server for VLANs:

```
Switch# vtp primary vlan
Setting device to VTP TRANSPARENT mode.
```

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

Related Commands

Command	Description
show vtp	Displays general information about VTP management domain, status, and counters.
vtp (global configuration)	Globally configures VTP domain name, password, pruning, version, and mode.

INDEX