VLAN Configuration Guide, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)

First Published: May 28, 2014

Last Modified: September 29, 2014

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

Text Part Number: OL-32318-01

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 controller, refer to the controller release notes.

- Cisco Catalyst 3850 Switch documentation, located at:

  http://www.cisco.com/go/cat3850_docs

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

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

- Cisco Validated Designs documents, located at:

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

- Error Message Decoder, located at:

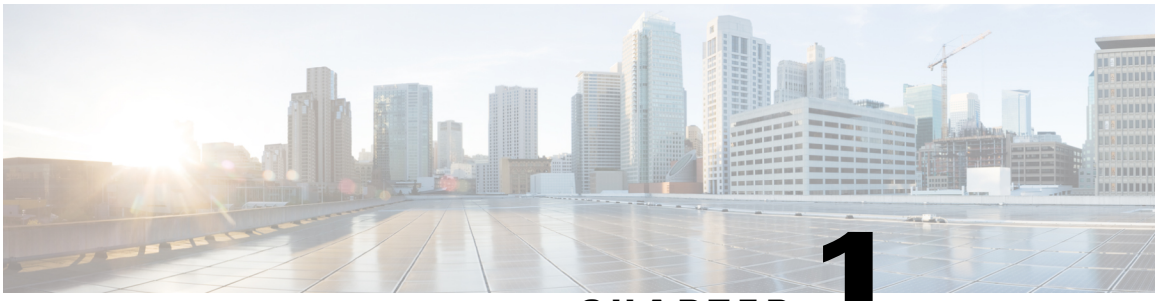
  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Obtaining Documentation and Submitting a Service Request

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

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

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



CHAPTER 1

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, a SSH, or by using the browser.

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

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

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

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

Table 1: Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session using Telnet, SSH, or console.	`Controller>`	Enter **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.	`Controller#`	Enter **disable** to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode. Use this mode to execute privilege EXEC commands for access points. These commands are not part of the running config of the controller, they are sent to the IOS config of the access point.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	`Controller(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 controller. Use this mode to configure access point commands that are part of the running config of the controller.
VLAN configuration	While in global configuration mode, enter the **vlan** *vlan-id* command.	`Controller(config-vlan)#`		

Mode	Access Method	Prompt	Exit Method	About This Mode
			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 controller startup configuration file.
Interface configuration	While in global configuration mode, enter the **interface** command (with a specific interface).	`Controller(config-if)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure parameters for the Ethernet ports.
Line configuration	While in global configuration mode, specify a line with the **line vty** or **line console** command.	`Controller(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 controller to recognize the command as unique.

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

```
Controller# show conf
```

No and Default Forms of Commands

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

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

CLI Error Messages

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

Table 2: Common CLI Error Messages

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

Configuration Logging

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

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

Note Only CLI or HTTP changes are logged.

Using the Help System

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

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

Step 4	**?** **Example:** `Controller> ?`	Lists all commands available for a particular command mode.

	Command or Action	Purpose
Step 5	*command* **?** **Example:** `Controller> show ?`	Lists the associated keywords for a command.

Step 6	*command keyword* **?**
	
	Example:
	`Controller(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 controller records ten command lines in its history buffer. You can alter this number for a current terminal session or for all sessions on a particular line. This procedure is optional.

SUMMARY STEPS

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

DETAILED STEPS

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

Recalling Commands

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**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:** `Controller# 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:** `Controller# 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:** `Controller# terminal editing`	Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.
Step 2	**terminal no editing** **Example:** `Controller# 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 controller suddenly sends a message to your screen.

Editing Command Lines That Wrap

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

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

Step 1	**access-list**
	
	Example:
	`Controller(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35`
	`Controller(config)# $ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25`
	`Controller(config)# $t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq`
	`Controller(config)# $15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45`
		Displays the global configuration command entry that extends beyond one line.
		
		When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign ($) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.

Step 2	**Ctrl-A** **Example:** `Controller(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.

	Command or Action	Purpose
		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:** `Controller# show interfaces	include protocol` `Vlan1 is up, line protocol is up` `Vlan10 is up, line protocol is down` `GigabitEthernet1/0/1 is up, line protocol is down` `GigabitEthernet1/0/2 is up, line protocol is up`	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

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

Accessing the CLI Through a Console Connection or Through Telnet

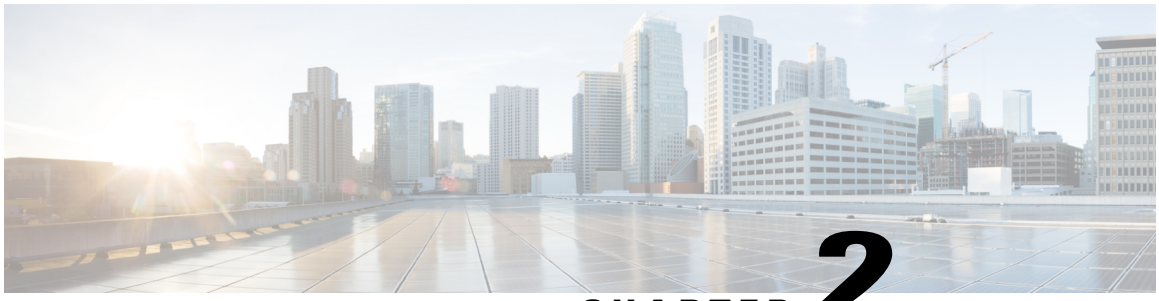
Before you can access the CLI, you must connect a terminal or a PC to the controller console or connect a PC to the Ethernet management port and then power on the controller, as described in the hardware installation guide that shipped with your controller.

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

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

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

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



CHAPTER 2

Using the Web Graphical User Interface

Prerequisites for Using the Web GUI

- The GUI must be used on a PC running Windows 7, Windows Vista, Windows XP, Windows 2003, or Windows 2000.
- The controller GUI is compatible with Microsoft Internet Explorer 6.0 and 7.0, and Mozilla Firefox up to version 26.0.

Information About Using The Web GUI

A web browser, or graphical user interface (GUI), is built into each controller.

You can use either the service port interface or the management interface to access the GUI. We recommend that you use the service-port interface. Click Help at the top of any page in the GUI to display online help. You might need to disable your browser's pop-up blocker to view the online help.

Web GUI Features

The controller web GUI supports the following:

The Configuration Wizard—After initial configuration of the IP address and the local username/password or auth via the authentication server (privilege 15 needed), the wizard provides a method to complete the initial

wireless configuration. Start the wizard through Configuration -> Wizard and follow the nine-step process to configure the following:

- Admin Users
- SNMP System Summary
- Management Port
- Wireless Management
- RF Mobility and Country code
- Mobility configuration
- WLANs
- 802.11 Configuration
- Set Time

The Monitor tab:

- Displays summary details of controller, clients, and access points.
- Displays all radio and AP join statistics.
- Displays air quality on access points.
- Displays list of all Cisco Discovery Protocol (CDP) neighbors on all interfaces and the CDP traffic information.
- Displays all rogue access points based on their classification-friendly, malicious, ad hoc, classified, and unclassified.

The Configuration tab:

- Enables you to configure the controller for all initial operation using the web Configuration Wizard. The wizard allows you to configure user details, management interface, and so on.
- Enables you to configure the system, internal DHCP server, management, and mobility management parameters.
- Enables you to configure the controller, WLAN, and radios.
- Enables you to configure and set security policies on your controller.
- Enables you to access the controller operating system software management commands.

The Administration tab enables you to configure system logs.

Connecting the Console Port of the Controller

Before You Begin

Before you can configure the controller for basic operations, you need to connect it to a PC that uses a VT-100 terminal emulation program (such as HyperTerminal, ProComm, Minicom, or Tip).

Step 1 Connect one end of a null-modem serial cable to the controller's RJ-45 console port and the other end to your PC's serial port.

Step 2 Plug the AC power cord into the controller and a grounded 100 to 240 VAC, 50/60-Hz electrical outlet. Turn on the power supply. The bootup script displays operating system software initialization (code download and power-on self-test verification) and basic configuration. If the controller passes the power-on self-test, the bootup script runs the configuration wizard, which prompts you for basic configuration input.

Step 3 Enter **yes**. Proceed with basic initial setup configuration parameters in the CLI setup wizard. Specify the IP address for the service port which is the gigabitethernet 0/0 interface.
After entering the configuration parameters in the configuration wizard, you can access the Web GUI. Now, the controller is configured with the IP address for service port.

Logging On to the Web GUI

Step 1 Enter the controller IP address in your browser's address bar. For a secure connection, enter https://**ip-address**. For a less secure connection, enter http://**ip-address**.

Step 2 When prompted, enter a valid username and password and click **OK**.

Note The administrative username and password that you created in the configuration wizard are case sensitive. The default username is admin, and the default password is cisco.

The Accessing page appears.

Enabling Web and Secure Web Modes

Step 1 Choose **Configuration** > **Controller** > **Management** > **Protocol Management** > **HTTP-HTTPS**.

The **HTTP-HTTPS Configuration** page appears.

Step 2 To enable web mode, which allows users to access the controller GUI using "http://ip-address," choose Enabled from the HTTP Access drop-down list. Otherwise, choose Disabled. Web mode (HTTP) is not a secure connection.

Step 3 To enable secure web mode, which allows users to access the controller GUI using "https://ip-address," choose Enabled from the HTTPS Access drop-down list. Otherwise, choose Disabled. Secure web mode (HTTPS) is a secure connection.

Step 4 Choose to track the device in the IP Device Tracking check box.

Step 5 Choose to enable the trust point in the Enable check box.

Step 6 Choose the trustpoints from the Trustpoints drop-down list.

Step 7 Enter the amount of time, in seconds, before the web session times out due to inactivity in the HTTP Timeout-policy (1 to 600 sec) text box.
The valid range is from 1 to 600 seconds.

Step 8 Enter the server life time in the Server Life Time (1 to 86400 sec) text box.
The valid range is from1 to 86400 seconds.

Step 9 Enter the maximum number of connection requests that the server can accept in the Maximum number of Requests (1 to 86400) text box.
The valid range is from 1 to 86400 connections.

Step 10 Click **Apply**.

Step 11 Click **Save Configuration**.

Configuring the Controller Web GUI

The configuration wizard enables you to configure basic settings on the controller. You can run the wizard after you receive the controller from the factory or after the controller has been reset to factory defaults. The configuration wizard is available in both GUI and CLI formats.

Step 1 Connect your PC to the service port and configure an IPv4 address to use the same subnet as the controller. The controller is loaded with IOS XE image and the service port interface is configured as gigabitethernet 0/0.

Step 2 Start Internet Explorer 10 (or later), Firefox 2.0.0.11 (or later), or Google Chrome on your PC and enter the management interface IP address on the browser window. The management interface IP address is same as the gigabitethernet 0/0 (also known as service port interface). When you log in for the first time, you need to enter HTTP username and password. By default, the username is **admin** and the password is **cisco**.
You can use both HTTP and HTTPS when using the service port interface. HTTPS is enabled by default and HTTP can also be enabled.

When you log in for the first time, the **Accessing Cisco Controller <Model Number> <Hostname>** page appears.

Step 3 On the **Accessing Cisco Controller** page, click the **Wireless Web GUI** link to access controller web GUI **Home** page.

Step 4 Choose **Configuration** > **Wizard** to perform all steps that you need to configure the controller initially.
The **Admin Users** page appears.

Step 5 On the **Admin Users** page, enter the administrative username to be assigned to this controller in the User Name text box and the administrative password to be assigned to this controller in the Password and Confirm Password text boxes. Click **Next**.
The default username is **admin** and the default password is **cisco**. You can also create a new administrator user for the controller. You can enter up to 24 ASCII characters for username and password.

The **SNMP System Summary** page appears.

Step 6 On the **SNMP System Summary** page, enter the following SNMP system parameters for the controller, and click **Next**:

- Customer-definable controller location in the Location text box.
- Customer-definable contact details such as phone number with names in the Contact text box.
- Choose **enabled** to send SNMP notifications for various SNMP traps or **disabled** not to send SNMP notifications for various SNMP traps from the SNMP Global Trap drop-down list.
- Choose **enabled** to send system log messages or **disabled** not to send system log messages from the SNMP Logging drop-down list.

Note The SNMP trap server, must be reachable through the distribution ports (and not through the gigabitethernet0/0 service or management interface).

The **Management Port** page appears.

Step 7 In the **Management Port** page, enter the following parameters for the management port interface (gigabitethernet 0/0) and click **Next**.

- Interface IP address that you assigned for the service port in the IP Address text box.
- Network mask address of the management port interface in the Netmask text box.
- The IPv4 Dynamic Host Configuration Protocol (DHCP) address for the selected port in the IPv4 DHCP Server text box.

The **Wireless Management** page appears.

Step 8 In the **Wireless Management** page, enter the following wireless interface management details, and click **Next**.

- Choose the interface—VLAN, or Ten Gigabit Ethernet from the Select Interface drop-down list.
- VLAN tag identifier, or 0 for no VLAN tag in the VLAN id text box.
- IP address of wireless management interface where access points are connected in the IP Address text box.
- Network mask address of the wireless management interface in the Netmask text box.
- DHCP IPv4 IP address in the IPv4 DHCP Server text box.

When selecting VLAN as interface, you can specify the ports as –Trunk or Access ports from the selected list displayed in the Switch Port Configuration text box.

The **RF Mobility and Country Code** page appears.

Step 9 In the **RF Mobility and Country Code** page, enter the RF mobility domain name in the RF Mobility text box, choose current country code from the Country Code drop-down list, and click **Next**. From the GUI, you can select only one country code.

Note Before configuring RF grouping parameters and mobility configuration, ensure that you refer to the relevant conceptual content and then proceed with the configuration.

The **Mobility Configuration** page with mobility global configuration settings appears.

Step 10 In the **Mobility Configuration** page, view and enter the following mobility global configuration settings, and click **Next**.

- Displays Mobility Controller in the Mobility Role text box.

- Displays mobility protocol port number in the Mobility Protocol Port text box.
- Displays the mobility group name in the Mobility Group Name text box.
- Displays whether DTLS is enabled in the DTLS Mode text box.

  DTLS is a standards-track Internet Engineering Task Force (IETF) protocol based on TLS.
- Displays mobility domain identifier for 802.11 radios in the Mobility Domain ID for 802.11 radios text box.
- Displays the number of members configured on the controller in the Mobility Domain Member Count text box.
- To enable the controller as a Mobility Oracle, select the Mobility Oracle Enabled check box.

  Note Only the controller can be configured as Mobility Oracle. You cannot configure the switch as Mobility Oracle.

  The Mobility Oracle is optional, it maintains the client database under one complete mobility domain.
- The amount of time (in seconds) between each ping request sent to an peer controller in the Mobility Keepalive Interval (1-30)sec text box.

  Valid range is from 1 to 30 seconds, and the default value is 10 seconds.
- Number of times a ping request is sent to an peer controller before the peer is considered to be unreachable in the Mobility Keepalive Count (3-20) text box.

  The valid range is from 3 to 20, and the default value is 3.
- The DSCP value that you can set for the mobility controller in the Mobility Control Message DSCP Value (0-63) text box.

  The valid range is 0 to 63, and the default value is 0.

The **WLANs** page appears.

Step 11 In the **Mobility Configuration** page, view and enter the following mobility global configuration settings, and click **Next**.

- Choose **Mobility Controller** or **Mobility Agent** from the Mobility Role drop-down list:
  - If Mobility Agent is chosen, enter the mobility controller IP address in the Mobility Controller IP Address text box and mobility controller IP address in the Mobility Controller Public IP Address text box.
  - If Mobility Controller is chosen, then the mobility controller IP address and mobility controller public IP address are displayed in the respective text boxes.
- Displays mobility protocol port number in the Mobility Protocol Port text box.
- Displays the mobility switch peer group name in the Mobility Switch Peer Group Name text box.
- Displays whether DTLS is enabled in the DTLS Mode text box.

  DTLS is a standards-track Internet Engineering Task Force (IETF) protocol based on TLS.
- Displays mobility domain identifier for 802.11 radios in the Mobility Domain ID for 802.11 radios text box.
- The amount of time (in seconds) between each ping request sent to an peer controller in the Mobility Keepalive Interval (1-30)sec text box.

  Valid range is from 1 to 30 seconds, and the default value is 10 seconds.
- Number of times a ping request is sent to an peer controller before the peer is considered to be unreachable in the Mobility Keepalive Count (3-20) text box.

The valid range is from 3 to 20, and the default value is 3.

- The DSCP value that you can set for the mobility controller in the Mobility Control Message DSCP Value (0-63) text box.

  The valid range is 0 to 63, and the default value is 0.

- Displays the number of mobility switch peer group member configured in the Switch Peer Group Members Configured text box.

The **WLANs** page appears.

Step 12 In the **WLANs** page, enter the following WLAN configuration parameters, and click **Next**.

- WLAN identifier in the WLAN ID text box.
- SSID of the WLAN that the client is associated with in the SSID text box.
- Name of the WLAN used by the client in the Profile Name text box.

The **802.11 Configuration** page appears.

Step 13 In the **802.11 Configuration** page, check either one or both 802.11a/n/ac and 802.11b/g/n check boxes to enable the 802.11 radios, and click **Next**.
The **Set Time** page appears.

Step 14 In the **Set Time** page, you can configure the time and date on the controller based on the following parameters, and click **Next**.

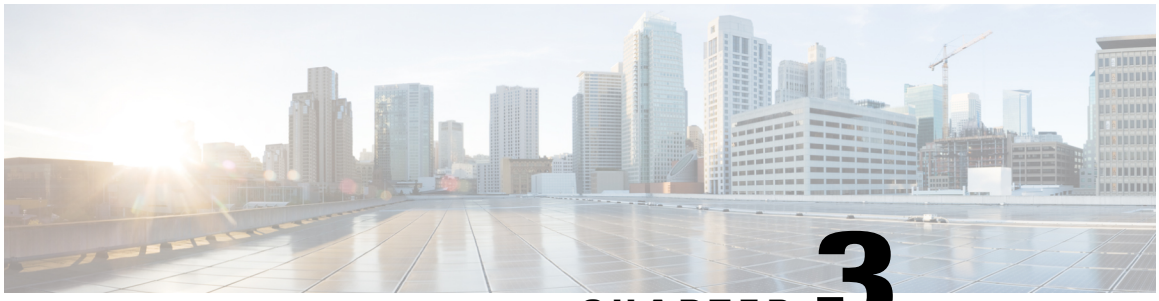
- Displays current timestamp on the controller in the Current Time text box.
- Choose either Manual or NTP from the Mode drop-down list.

  On using the NTP server, all access points connected to the controller, synchronizes its time based on the NTP server settings available.

- Choose date on the controller from the Year, Month, and Day drop-down list.
- Choose time from the Hours, Minutes, and Seconds drop-down list.
- Enter the time zone in the Zone text box and select the off setting required when compared to the current time configured on the controller from the Offset drop-down list.

The **Save Wizard** page appears.

Step 15 In the **Save Wizard** page, you can review the configuration settings performed on the controller using these steps, and if you wish to change any configuration value, click **Previous** and navigate to that page.
You can save the controller configuration created using the wizard only if a success message is displayed for all the wizards. If the **Save Wizard** page displays errors, you must recreate the wizard for initial configuration of the controller.



CHAPTER 3

Configuring VTP

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VTP

Before you create VLANs, you must decide whether to use the VLAN Trunking Protocol (VTP) in your network. Using VTP, you can make configuration changes centrally on one or more controllers and have those changes automatically communicated to all the other controllers in the network. Without VTP, you cannot send information about VLANs to other controllers.

VTP is designed to work in an environment where updates are made on a single controller and are sent through VTP to other controllers in the domain. It does not work well in a situation where multiple updates to the VLAN database occur simultaneously on controllers in the same domain, which would result in an inconsistency in the VLAN database.

The controller supports a total of 4094 VLANs. However, the number of configured features affects the usage of the controller hardware. If the controller is notified by VTP of a new VLAN and the controller is already using the maximum available hardware resources, it sends a message that there are not enough hardware resources available and shuts down the VLAN. The output of the **show vlan** user EXEC command shows the VLAN in a suspended state.

Because trunk ports send and receive VTP advertisements, you must ensure that at least one trunk port is configured on the controller and that this trunk port is connected to the trunk port of another controller. Otherwise, the controller cannot receive any VTP advertisements.

Related Topics

VTP Advertisements, on page 24

Adding a VTP Client Controller to a VTP Domain , on page 39

VTP Domain, on page 23

VTP Modes, on page 23

Restrictions for VTP

The following are restrictions for a VTP:

- You cannot have a controller stack containing a mix of Catalyst 3850 and Catalyst 3650 switches.

Caution Before adding a VTP client controller to a VTP domain, always verify that its VTP configuration revision number is lower than the configuration revision number of the other controllers in the VTP domain. Controllers in a VTP domain always use the VLAN configuration of the controller with the highest VTP configuration revision number. If you add a controller that has a revision number higher than the revision number in the VTP domain, it can erase all VLAN information from the VTP server and VTP domain.

Information About VTP

VTP

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

VTP Domain

A VTP domain (also called a VLAN management domain) consists of one controller or several interconnected controllers or controller stacks under the same administrative responsibility sharing the same VTP domain name. A controller can be in only one VTP domain. You make global VLAN configuration changes for the domain.

By default, the controller is in the VTP no-management-domain state until it receives an advertisement for a domain over a trunk link (a link that carries the traffic of multiple VLANs) or until you configure a domain name. Until the management domain name is specified or learned, you cannot create or modify VLANs on a VTP server, and VLAN information is not propagated over the network.

If the controller receives a VTP advertisement over a trunk link, it inherits the management domain name and the VTP configuration revision number. The controller then ignores advertisements with a different domain name or an earlier configuration revision number.

When you make a change to the VLAN configuration on a VTP server, the change is propagated to all controllers in the VTP domain. VTP advertisements are sent over all IEEE trunk connections, including IEEE 802.1Q. VTP dynamically maps VLANs with unique names and internal index associates across multiple LAN types. Mapping eliminates excessive device administration required from network administrators.

If you configure a controller for VTP transparent mode, you can create and modify VLANs, but the changes are not sent to other controllers in the domain, and they affect only the individual controller. However, configuration changes made when the controller is in this mode are saved in the controller running configuration and can be saved to the controller startup configuration file.

Related Topics

Adding a VTP Client Controller to a VTP Domain , on page 39

Prerequisites for VTP, on page 21

VTP Modes

Table 4: VTP Modes

VTP Mode	Description
VTP server	In VTP server mode, you can create, modify, and delete VLANs, and specify other configuration parameters (such as the VTP version) for the entire VTP domain. VTP servers advertise their VLAN configurations to other controllers in the same VTP domain and synchronize their VLAN configurations with other controllers based on advertisements received over trunk links. VTP server is the default mode. In VTP server mode, VLAN configurations are saved in NVRAM. If the controller detects a failure while writing a configuration to NVRAM, VTP mode automatically changes from server mode to client mode. If this happens, the controller cannot be returned to VTP server mode until the NVRAM is functioning.

VTP Mode	Description
VTP client	A VTP client functions like a VTP server and transmits and receives VTP updates on its trunks, but you cannot create, change, or delete VLANs on a VTP client. VLANs are configured on another controller in the domain that is in server mode. In VTP versions 1 and 2 in VTP client mode, VLAN configurations are not saved in NVRAM. In VTP version 3, VLAN configurations are saved in NVRAM in client mode.
VTP transparent	VTP transparent controllers do not participate in VTP. A VTP transparent controller does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2 or version 3, transparent controllers do forward VTP advertisements that they receive from other controllers through their trunk interfaces. You can create, modify, and delete VLANs on a controller in VTP transparent mode. When the controller is in VTP transparent mode, the VTP and VLAN configurations are saved in NVRAM, but they are not advertised to other controllers. In this mode, VTP mode and domain name are saved in the controller running configuration, and you can save this information in the controller startup configuration file by using the **copy running-config startup-config** privileged EXEC command.
VTP off	A controller in VTP off mode functions in the same manner as a VTP transparent controller, except that it does not forward VTP advertisements on trunks.

Related Topics

Prerequisites for VTP, on page 21
Configuring VTP Mode , on page 30

VTP Advertisements

Each controller in the VTP domain sends periodic global configuration advertisements from each trunk port to a reserved multicast address. Neighboring controllers receive these advertisements and update their VTP and VLAN configurations as necessary.

VTP advertisements distribute this global domain information:

- VTP domain name
- VTP configuration revision number
- Update identity and update timestamp
- MD5 digest VLAN configuration, including maximum transmission unit (MTU) size for each VLAN
- Frame format

VTP advertisements distribute this VLAN information for each configured VLAN:

- VLAN IDs (including IEEE 802.1Q)
- VLAN name

- VLAN type
- VLAN state
- Additional VLAN configuration information specific to the VLAN type

In VTP version 3, VTP advertisements also include the primary server ID, an instance number, and a start index.

Related Topics

Prerequisites for VTP, on page 21

VTP Version 2

If you use VTP in your network, you must decide which version of VTP to use. By default, VTP operates in version 1.

VTP version 2 supports these features that are not supported in version 1:

- Token Ring support—VTP version 2 supports Token Ring Bridge Relay Function (TrBRF) and Token Ring Concentrator Relay Function (TrCRF) VLANs.
- Unrecognized Type-Length-Value (TLV) support—A VTP server or client propagates configuration changes to its other trunks, even for TLVs it is not able to parse. The unrecognized TLV is saved in NVRAM when the controller is operating in VTP server mode.
- Version-Dependent Transparent Mode—In VTP version 1, a VTP transparent controller inspects VTP messages for the domain name and version and forwards a message only if the version and domain name match. Although VTP version 2 supports only one domain, a VTP version 2 transparent controller forwards a message only when the domain name matches.
- Consistency Checks—In VTP version 2, VLAN consistency checks (such as VLAN names and values) are performed only when you enter new information through the CLI or SNMP. Consistency checks are not performed when new information is obtained from a VTP message or when information is read from NVRAM. If the MD5 digest on a received VTP message is correct, its information is accepted.

Related Topics

Enabling the VTP Version , on page 35

VTP Version 3

VTP version 3 supports these features that are not supported in version 1 or version 2:

- Enhanced authentication—You can configure the authentication as **hidden** or **secret**. When **hidden**, the secret key from the password string is saved in the VLAN database file, but it does not appear in plain text in the configuration. Instead, the key associated with the password is saved in hexadecimal format in the running configuration. You must reenter the password if you enter a takeover command in the domain. When you enter the **secret** keyword, you can directly configure the password secret key.
- Support for extended range VLAN (VLANs 1006 to 4094) database propagation—VTP versions 1 and 2 propagate only VLANs 1 to 1005.

Note VTP pruning still applies only to VLANs 1 to 1005, and VLANs 1002 to 1005 are still reserved and cannot be modified.

- Support for any database in a domain—In addition to propagating VTP information, version 3 can propagate Multiple Spanning Tree (MST) protocol database information. A separate instance of the VTP protocol runs for each application that uses VTP.
- VTP primary server and VTP secondary servers—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 its NVRAM.

  By default, all devices come up as secondary servers. You can enter the **vtp primary** privileged EXEC command to specify a primary server. Primary server status is only needed 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, even when a password is configured on the controller.
- The option to turn VTP on or off on a per-trunk (per-port) basis—You can enable or disable VTP per port by entering the [**no**] **vtp** interface configuration command. When you disable VTP on trunking ports, all VTP instances for that port are disabled. You cannot set VTP to *off* for the MST database and *on* for the VLAN database on the same port.

  When you globally set VTP mode to off, it applies to all the trunking ports in the system. However, you can specify on or off on a per-VTP instance basis. For example, you can configure the controller as a VTP server for the VLAN database but with VTP *off* for the MST database.

Related Topics

Enabling the VTP Version , on page 35

VTP Pruning

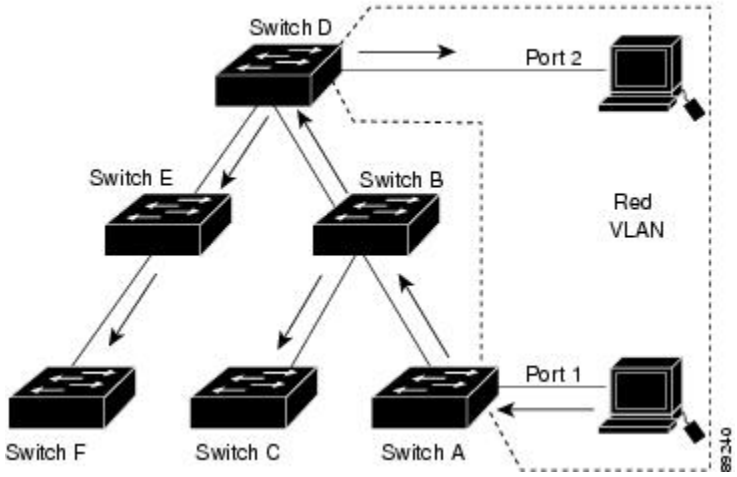
VTP pruning increases network available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to reach the destination devices. Without VTP pruning, a controller floods broadcast, multicast, and unknown unicast traffic across all trunk links within a VTP domain even though receiving controllers might discard them. VTP pruning is disabled by default.

VTP pruning blocks unneeded flooded traffic to VLANs on trunk ports that are included in the pruning-eligible list. Only VLANs included in the pruning-eligible list can be pruned. By default, VLANs 2 through 1001 are pruning eligible controller trunk ports. If the VLANs are configured as pruning-ineligible, the flooding continues. VTP pruning is supported in all VTP versions.

VTP pruning is disabled in the switched network. Port 1 on Controller A and Port 2 on Controller D are assigned to the Red VLAN. If a broadcast is sent from the host connected to Controller A, Controller A floods

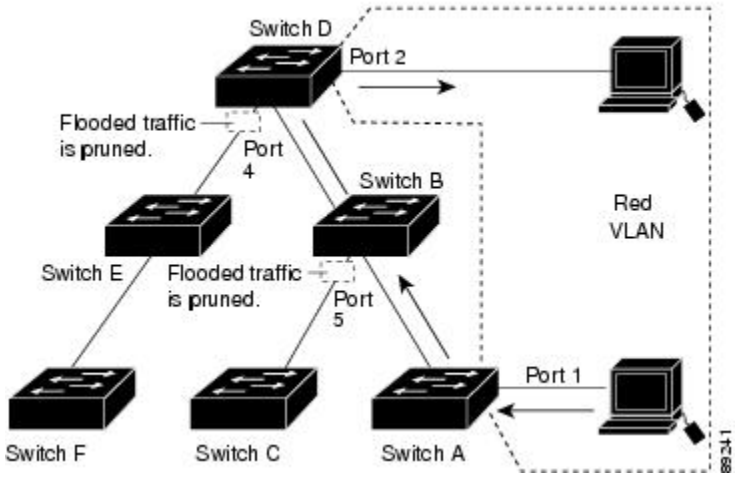
the broadcast and every controller in the network receives it, even though Controllers C, E, and F have no ports in the Red VLAN.

Figure 1: Flooding Traffic without VTP Pruning



VTP pruning is enabled in the switched network. The broadcast traffic from Controller A is not forwarded to Controllers C, E, and F because traffic for the Red VLAN has been pruned on the links shown (Port 5 on Controller B and Port 4 on Controller D).

Figure 2: Optimized Flooded Traffic VTP Pruning



With VTP versions 1 and 2, when you enable pruning on the VTP server, it is enabled for the entire VTP domain. In VTP version 3, you must manually enable pruning on each controller in the domain. Making VLANs pruning-eligible or pruning-ineligible affects pruning eligibility for those VLANs on that trunk only (not on all controllers in the VTP domain).

VTP pruning takes effect several seconds after you enable it. VTP pruning does not prune traffic from VLANs that are pruning-ineligible. VLAN 1 and VLANs 1002 to 1005 are always pruning-ineligible; traffic from these VLANs cannot be pruned. Extended-range VLANs (VLAN IDs higher than 1005) are also pruning-ineligible.

Related Topics

Enabling VTP Pruning , on page 36

VTP Configuration Guidelines

VTP Configuration Requirements

When you configure VTP, you must configure a trunk port so that the controller can send and receive VTP advertisements to and from other controllers in the domain.

VTP Settings

The VTP information is saved in the VTP VLAN database. When VTP mode is transparent, the VTP domain name and mode are also saved in the controller running configuration file, and you can save it in the controller startup configuration file by entering the **copy running-config startup-config** privileged EXEC command. You must use this command if you want to save VTP mode as transparent, even if the controller resets.

When you save VTP information in the controller startup configuration file and reboot the controller, the controller 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.

Related Topics

Configuring VTP on a Per-Port Basis , on page 38

Configuring a VTP Version 3 Primary Server , on page 34

Domain Names for Configuring VTP

When configuring VTP for the first time, you must always assign a domain name. You must configure all controllers in the VTP domain with the same domain name. Controllers in VTP transparent mode do not exchange VTP messages with other controllers, and you do not need to configure a VTP domain name for them.

Note If the NVRAM and DRAM storage is sufficient, all controllers in a VTP domain should be in VTP server mode.

Caution Do not configure a VTP domain if all controllers are operating in VTP client mode. If you configure the domain, it is impossible to make changes to the VLAN configuration of that domain. Make sure that you configure at least one controller in the VTP domain for VTP server mode.

Related Topics

Adding a VTP Client Controller to a VTP Domain , on page 39

Passwords for the VTP Domain

You can configure a password for the VTP domain, but it is not required. If you do configure a domain password, all domain controllers must share the same password and you must configure the password on each controller in the management domain. Controllers without a password or with the wrong password reject VTP advertisements.

If you configure a VTP password for a domain, a controller that is booted without a VTP configuration does not accept VTP advertisements until you configure it with the correct password. After the configuration, the controller accepts the next VTP advertisement that uses the same password and domain name in the advertisement.

If you are adding a new controller to an existing network with VTP capability, the new controller learns the domain name only after the applicable password has been configured on it.

Caution When you configure a VTP domain password, the management domain does not function properly if you do not assign a management domain password to each controller in the domain.

Related Topics

Configuring a VTP Version 3 Password , on page 32

Example: Configuring a Switch as the Primary Server, on page 42

VTP Version

Follow these guidelines when deciding which VTP version to implement:

- All controllers in a VTP domain must have the same domain name, but they do not need to run the same VTP version.
- A VTP version 2-capable controller can operate in the same VTP domain as a controller running VTP version 1 if version 2 is disabled on the version 2-capable controller (version 2 is disabled by default).
- If a controller running VTP version 1, but capable of running VTP version 2, receives VTP version 3 advertisements, it automatically moves to VTP version 2.
- If a controller running VTP version 3 is connected to a controller running VTP version 1, the VTP version 1 controller moves to VTP version 2, and the VTP version 3 controller sends scaled-down versions of the VTP packets so that the VTP version 2 controller can update its database.
- A controller running VTP version 3 cannot move to version 1 or 2 if it has extended VLANs.

- Do not enable VTP version 2 on a controller unless all of the controllers in the same VTP domain are version-2-capable. When you enable version 2 on a controller, all of the version-2-capable controllers in the domain enable version 2. If there is a version 1-only controller, it does not exchange VTP information with controllers that have version 2 enabled.
- Cisco recommends placing VTP version 1 and 2 controllers at the edge of the network because they do not forward VTP version 3 advertisements.
- If there are TrBRF and TrCRF Token Ring networks in your environment, you must enable VTP version 2 or version 3 for Token Ring VLAN switching to function properly. To run Token Ring and Token Ring-Net, disable VTP version 2.
- VTP version 1 and version 2 do not propagate configuration information for extended range VLANs (VLANs 1006 to 4094). You must configure these VLANs manually on each device. VTP version 3 supports extended-range VLANs and support for extended range VLAN database propagation.
- When a VTP version 3 device trunk port receives messages from a VTP version 2 device, it sends a scaled-down version of the VLAN database on that particular trunk in VTP version 2 format. A VTP version 3 device does not send VTP version 2-formatted packets on a trunk unless it first receives VTP version 2 packets on that trunk port.
- When a VTP version 3 device detects a VTP version 2 device on a trunk port, it continues to send VTP version 3 packets, in addition to VTP version 2 packets, to allow both kinds of neighbors to coexist on the same trunk.
- A VTP version 3 device does not accept configuration information from a VTP version 2 or version 1 device.
- Two VTP version 3 regions can only communicate in transparent mode over a VTP version 1 or version 2 region.
- Devices that are only VTP version 1 capable cannot interoperate with VTP version 3 devices.
- VTP version 1 and version 2 do not propagate configuration information for extended range VLANs (VLANs 1006 to 4094). You must manually configure these VLANs on each device.

Related Topics

Enabling the VTP Version , on page 35

How to Configure VTP

Configuring VTP Mode

You can configure VTP mode as one of these:

- VTP server mode—In VTP server mode, you can change the VLAN configuration and have it propagated throughout the network.
- VTP client mode—In VTP client mode, you cannot change its VLAN configuration. The client controller receives VTP updates from a VTP server in the VTP domain and then modifies its configuration accordingly.

- VTP transparent mode—In VTP transparent mode, VTP is disabled on the controller. The controller does not send VTP updates and does not act on VTP updates received from other controller. However, a VTP transparent controller running VTP version 2 does forward received VTP advertisements on its trunk links.
- VTP off mode—VTP off mode is the same as VTP transparent mode except that VTP advertisements are not forwarded.

When you configure a domain name, it cannot be removed; you can only reassign a controller to a different domain.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vtp domain** *domain-name*
4. **vtp mode** {**client** | **server** | **transparent** | **off**} {**vlan** | **mst** | **unknown**}
5. **vtp password** *password*
6. **end**
7. **show vtp status**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters the global configuration mode.
Step 3	**vtp domain** *domain-name* **Example:** `Controller(config)# vtp domain eng_group`	Configures the VTP administrative-domain name. The name can be 1 to 32 characters. All controllers operating in VTP server or client mode under the same administrative responsibility must be configured with the same domain name. This command is optional for modes other than server mode. VTP server mode requires a domain name. If the controller has a trunk connection to a VTP domain, the controller learns the domain name from the VTP server in the domain. You should configure the VTP domain before configuring other VTP parameters.

	Command or Action	Purpose
		Note
Step 4	**vtp mode** {**client** | **server** | **transparent** | **off**} {**vlan** | **mst** | **unknown**} **Example:** `Controller(config)# vtp mode server`	Configures the controller for VTP mode (client, server, transparent, or off). • **vlan—**The VLAN database is the default if none are configured. • **mst—**The multiple spanning tree (MST) database. • **unknown—**An unknown database type.
Step 5	**vtp password** *password* **Example:** `Controller(config)# vtp password mypassword`	(Optional) Sets the password for the VTP domain. The password can be 8 to 64 characters. If you configure a VTP password, the VTP domain does not function properly if you do not assign the same password to each controller in the domain.
Step 6	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 7	**show vtp status** **Example:** `Controller# show vtp status`	Verifies your entries in the *VTP Operating Mode* and the *VTP Domain Name* fields of the display.
Step 8	**copy running-config startup-config** **Example:** `Controller# copy running-config startup-config`	(Optional) Saves the configuration in the startup configuration file. Only VTP mode and domain name are saved in the controller running configuration and can be copied to the startup configuration file.

Related Topics

VTP Modes, on page 23

Configuring a VTP Version 3 Password

You can configure a VTP version 3 password on the controller.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vtp password** *password* [**hidden** | **secret**]
4. **end**
5. **show vtp password**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters the global configuration mode.
Step 3	**vtp password** *password* [**hidden**	**secret**] **Example:** `Controller(config)# vtp password mypassword hidden`	(Optional) Sets the password for the VTP domain. The password can be 8 to 64 characters. • (Optional) **hidden—**Saves the secret key generated from the password string in the nvram:vlan.dat file. If you configure a takeover by configuring a VTP primary server, you are prompted to reenter the password. • (Optional) **secret—**Directly configures the password. The secret password must contain 32 hexadecimal characters.
Step 4	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 5	**show vtp password** **Example:** `Controller# show vtp password`	Verifies your entries. The output appears like this: VTP password: 89914640C8D90868B6A0D8103847A733

	Command or Action	Purpose
Step 6	**copy running-config startup-config** **Example:** `Controller# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Passwords for the VTP Domain, on page 29
Example: Configuring a Switch as the Primary Server, on page 42

Configuring a VTP Version 3 Primary Server

When you configure a VTP server as a VTP primary server, the takeover operation starts.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**vtp primary** [**vlan**	**mst**] [**force**] **Example:** `Controller# vtp primary vlan force`	Changes the operational state of a controller from a secondary server (the default) to a primary server and advertises the configuration to the domain. If the controller password is configured as **hidden**, you are prompted to reenter the password. • (Optional) **vlan**—Selects the VLAN database as the takeover feature. This is the default. • (Optional) **mst**—Selects the multiple spanning tree (MST) database as the takeover feature. • (Optional) **force**—Overwrites the configuration of any conflicting servers. If you do not enter **force**, you are prompted for confirmation before the takeover.

Related Topics

VTP Settings, on page 28

Enabling the VTP Version

VTP version 2 and version 3 are disabled by default.

- When you enable VTP version 2 on a controller , every VTP version 2-capable controller in the VTP domain enables version 2. To enable VTP version 3, you must manually configure it on each controller .
- With VTP versions 1 and 2, you can configure the version only on controllers in VTP server or transparent mode. If a controller is running VTP version 3, you can change to version 2 when the controller is in client mode if no extended VLANs exist, and no hidden password was configured.

  Caution VTP version 1 and VTP version 2 are not interoperable on controllers in the same VTP domain. Do not enable VTP version 2 unless every controller in the VTP domain supports version 2.

- In TrCRF and TrBRF Token Ring environments, you must enable VTP version 2 or VTP version 3 for Token Ring VLAN switching to function properly. For Token Ring and Token Ring-Net media, disable VTP version 2.
- **Caution** In VTP version 3, both the primary and secondary servers can exist on an instance in the domain.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vtp version** {**1** | **2** | **3**}
4. **end**
5. **show vtp status**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters the global configuration mode.
Step 3	**vtp version** {**1** | **2** | **3**} **Example:** `Controller(config)# vtp version 2`	Enables the VTP version on the controller. The default is VTP version 1.
Step 4	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 5	**show vtp status** **Example:** `Controller# show vtp status`	Verifies that the configured VTP version is enabled.
Step 6	**copy running-config startup-config** **Example:** `Controller# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

VTP Version, on page 29
VTP Version 2, on page 25
VTP Version 3, on page 25

Enabling VTP Pruning

Before You Begin

VTP pruning is not designed to function in VTP transparent mode. If one or more controllers in the network are in VTP transparent mode, you should do one of these actions:

- Turn off VTP pruning in the entire network.

- Turn off VTP pruning by making all VLANs on the trunk of the controller upstream to the VTP transparent controller pruning ineligible.

To configure VTP pruning on an interface, use the **switchport trunk pruning vlan** interface configuration command. VTP pruning operates when an interface is trunking. You can set VLAN pruning-eligibility, whether or not VTP pruning is enabled for the VTP domain, whether or not any given VLAN exists, and whether or not the interface is currently trunking.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vtp pruning**
4. **end**
5. **show vtp status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters the global configuration mode.
Step 3	**vtp pruning** **Example:** `Controller(config)# vtp pruning`	Enables pruning in the VTP administrative domain. By default, pruning is disabled. You need to enable pruning on only one controller in VTP server mode.
Step 4	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 5	**show vtp status** **Example:** `Controller# show vtp status`	Verifies your entries in the *VTP Pruning Mode* field of the display.

Related Topics

VTP Pruning, on page 26

Configuring VTP on a Per-Port Basis

With VTP version 3, you can enable or disable VTP on a per-port basis. You can enable VTP only on ports that are in trunk mode. Incoming and outgoing VTP traffic are blocked, not forwarded.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **vtp**
5. **end**
6. **show running-config interface** *interface-id*
7. **show vtp status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Controller(config)# interface gigabitethernet1/0/1`	Identifies an interface, and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**vtp** **Example:** `Controller(config)# vtp`	Enables VTP on the specified port.
Step 5	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config interface** *interface-id* **Example:** `Controller# show running-config interface gigabitethernet1/0/1`	Verifies the change to the port.
Step 7	**show vtp status** **Example:** `Controller# show vtp status`	Verifies the configuration.

Related Topics

VTP Settings, on page 28

Adding a VTP Client Controller to a VTP Domain

Follow these steps to verify and reset the VTP configuration revision number on a controller *before* adding it to a VTP domain.

Before You Begin

Before adding a VTP client to a VTP domain, always verify that its VTP configuration revision number is *lower* than the configuration revision number of the other controllers in the VTP domain. Controllers in a VTP domain always use the VLAN configuration of the controller with the highest VTP configuration revision number. With VTP versions 1 and 2, adding a controller that has a revision number higher than the revision number in the VTP domain can erase all VLAN information from the VTP server and VTP domain. With VTP version 3, the VLAN information is not erased.

You can use the **vtp mode transparent** global configuration command to disable VTP on the controller and then to change its VLAN information without affecting the other controllers in the VTP domain.

SUMMARY STEPS

1. **enable**
2. **show vtp status**
3. **configure terminal**
4. **vtp domain** *domain-name*
5. **end**
6. **show vtp status**
7. **configure terminal**
8. **vtp domain** *domain-name*
9. **end**
10. **show vtp status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**show vtp status** **Example:** `Controller# show vtp status`	Checks the VTP configuration revision number. If the number is 0, add the controller to the VTP domain. If the number is greater than 0, follow these substeps: • Write down the domain name. • Write down the configuration revision number. • Continue with the next steps to reset the controller configuration revision number.
Step 3	**configure terminal** **Example:** `Controller# configure terminal`	Enters the global configuration mode.
Step 4	**vtp domain** *domain-name* **Example:** `Controller(config)# vtp domain domain123`	Changes the domain name from the original one displayed in Step 1 to a new name.

	Command or Action	Purpose
Step 5	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode. The VLAN information on the controller is updated and the configuration revision number is reset to 0.
Step 6	**show vtp status** **Example:** `Controller# show vtp status`	Verifies that the configuration revision number has been reset to 0.
Step 7	**configure terminal** **Example:** `Controller# configure terminal`	Enters global configuration mode.
Step 8	**vtp domain** *domain-name* **Example:** `Controller(config)# vtp domain domain012`	Enters the original domain name on the controller
Step 9	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode. The VLAN information on the controller is updated.
Step 10	**show vtp status** **Example:** `Controller# show vtp status`	(Optional) Verifies that the domain name is the same as in Step 1 and that the configuration revision number is 0.

Related Topics

VTP Domain, on page 23
Prerequisites for VTP, on page 21
Domain Names for Configuring VTP, on page 28

Monitoring VTP

This section describes commands used to display and monitor the VTP configuration.

You monitor VTP by displaying VTP configuration information: the domain name, the current VTP revision, and the number of VLANs. You can also display statistics about the advertisements sent and received by the controller.

Table 5: VTP Monitoring Commands

Command	Purpose
show vtp counters	Displays counters about VTP messages that have been sent and received.
show vtp devices [**conflict**]	Displays information about all VTP version 3 devices in the domain. Conflicts are VTP version 3 devices with conflicting primary servers. The **show vtp devices** command does not display information when the controller is in transparent or off mode.
show vtp interface [*interface-id*]	Displays VTP status and configuration for all interfaces or the specified interface.
show vtp password	Displays the VTP password. The form of the password displayed depends on whether or not the **hidden** keyword was entered and if encryption is enabled on the controller.
show vtp status	Displays the VTP controller configuration information.

Configuration Examples for VTP

Example: Configuring a Switch as the Primary Server

This example shows how to configure a controller as the primary server for the VLAN database (the default) when a hidden or secret password was configured:

```
Controller# vtp primary vlan
Enter VTP password: mypassword
This switch is becoming Primary server for vlan feature in the VTP  domain

VTP Database Conf Switch ID      Primary Server Revision System Name
------------ ---- --------------- -------------- -------- --------------------
VLANDB       Yes  00d0.00b8.1400=00d0.00b8.1400 1        stp7

Do you want to continue (y/n) [n]? y
```

Related Topics

Configuring a VTP Version 3 Password , on page 32
Passwords for the VTP Domain, on page 29

Where to Go Next

After configuring VTP, you can configure the following:

- VLANs
- VLAN groups
- VLAN trunking

Additional References

Standards and RFCs

Standard/RFC	Title
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIBs

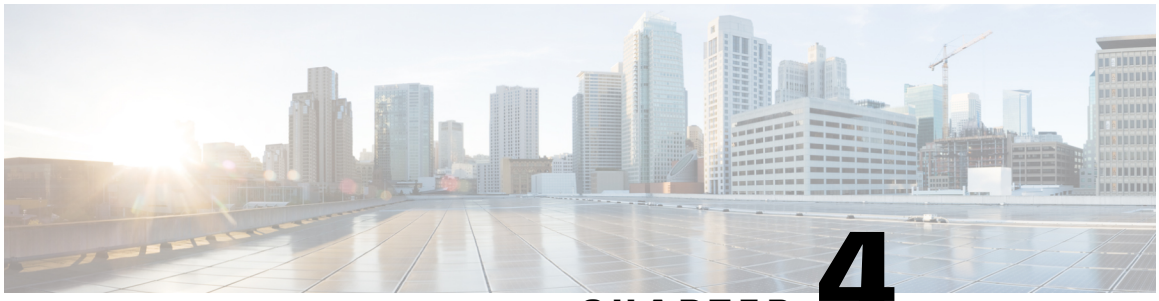
MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

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

Feature History and Information for VTP

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



CHAPTER 4

Configuring VLANs

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VLANs

The following are prerequisites and considerations for configuring VLANs:

- Before you create VLANs, you must decide whether to use VLAN Trunking Protocol (VTP) to maintain global VLAN configuration for your network.

- If you plan to configure many VLANs on the controller and to not enable routing, you can set the Switch Database Management (SDM) feature to the VLAN template, which configures system resources to support the maximum number of unicast MAC addresses.
- Controllers running the LAN Base feature set support only static routing on SVIs.
- A VLAN should be present in the controller to be able to add it to the VLAN group.

Restrictions for VLANs

The following are restrictions for VLANs:

- The controller supports per-VLAN spanning-tree plus (PVST+) or rapid PVST+ with a maximum of 128 spanning-tree instances. One spanning-tree instance is allowed per VLAN.
- The controller supports IEEE 802.1Q trunking methods for sending VLAN traffic over Ethernet ports.
- Configuring an interface VLAN router's MAC address is not supported. The interface VLAN already has an MAC address assigned by default.
- Private VLANs are not supported on the controller.
- You cannot have a switch stack containing a mix of Catalyst 3850 and Catalyst 3650 switches.

Information About VLANs

Logical Networks

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any controller port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or a controller supporting fallback bridging. Because a VLAN is considered a separate logical network, it contains its own bridge Management Information Base (MIB) information and can support its own implementation of spanning tree.

VLANs are often associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the controller is assigned manually on an interface-by-interface basis. When you assign controller interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership.

Traffic between VLANs must be routed.

The controller can route traffic between VLANs by using controller virtual interfaces (SVIs). An SVI must be explicitly configured and assigned an IP address to route traffic between VLANs.

Supported VLANs

The controller supports VLANs in VTP client, server, and transparent modes. VLANs are identified by a number from 1 to 4094. VLAN 1 is the default VLAN and is created during system initialization. VLAN IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs. All of the VLANs except 1002 to 1005 are available for user configuration.

There are 3 VTP versions: VTP version 1, version 2, and version 3. All VTP versions support both normal and extended range VLANs, but only with VTP version 3, does the controller propagate extended range VLAN configuration information. When extended range VLANs are created in VTP versions 1 and 2, their configuration information is not propagated. Even the local VTP database entries on the controller are not updated, but the extended range VLANs configuration information is created and stored in the running configuration file.

You can configure up to 4094 VLANs on the controller.

VLAN Port Membership Modes

You configure a port to belong to a VLAN by assigning a membership mode that specifies the kind of traffic the port carries and the number of VLANs to which it can belong.

When a port belongs to a VLAN, the controller learns and manages the addresses associated with the port on a per-VLAN basis.

Table 6: Port Membership Modes and Characteristics

Membership Mode	VLAN Membership Characteristics	VTP Characteristics
Static-access	A static-access port can belong to one VLAN and is manually assigned to that VLAN.	VTP is not required. If you do not want VTP to globally propagate information, set the VTP mode to transparent. To participate in VTP, there must be at least one trunk port on the controller connected to a trunk port of a second controller.
Trunk (IEEE 802.1Q) : • IEEE 802.1Q— Industry-standard trunking encapsulation.	A trunk port is a member of all VLANs by default, including extended-range VLANs, but membership can be limited by configuring the allowed-VLAN list. You can also modify the pruning-eligible list to block flooded traffic to VLANs on trunk ports that are included in the list.	VTP is recommended but not required. VTP maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP exchanges VLAN configuration messages with other controllers over trunk links.

Membership Mode	VLAN Membership Characteristics	VTP Characteristics
Dynamic access	A dynamic-access port can belong to one VLAN (VLAN ID 1 to 4094) and is dynamically assigned by a VLAN Member Policy Server (VMPS). You can have dynamic-access ports and trunk ports on the same controller, but you must connect the dynamic-access port to an end station or hub and not to another controller.	VTP is required. Configure the VMPS and the client with the same VTP domain name. To participate in VTP, at least one trunk port on the controller must be connected to a trunk port of a second controller .
Voice VLAN	A voice VLAN port is an access port attached to a Cisco IP Phone, configured to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone.	VTP is not required; it has no effect on a voice VLAN.

Related Topics

Assigning Static-Access Ports to a VLAN, on page 57
Monitoring VLANs, on page 61

VLAN Configuration Files

Configurations for VLAN IDs 1 to 1005 are written to the vlan.dat file (VLAN database), and you can display them by entering the **show vlan** privileged EXEC command. The vlan.dat file is stored in flash memory. If the VTP mode is transparent, they are also saved in the controller running configuration file.

You use the interface configuration mode to define the port membership mode and to add and remove ports from VLANs. The results of these commands are written to the running-configuration file, and you can display the file by entering the **show running-config** privileged EXEC command.

When you save VLAN and VTP information (including extended-range VLAN configuration information) in the startup configuration file and reboot the controller, the controller 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 does not match the VLAN database, the domain name and VTP mode and configuration for the VLAN IDs 1 to 1005 use the VLAN database information.
- In VTP versions 1 and 2, if VTP mode is server, the domain name and VLAN configuration for VLAN IDs 1 to 1005 use the VLAN database information. VTP version 3 also supports VLANs 1006 to 4094.

Normal-Range VLAN Configuration Guidelines

Normal-range VLANs are VLANs with IDs from 1 to 1005.

Follow these guidelines when creating and modifying normal-range VLANs in your network:

- Normal-range VLANs are identified with a number between 1 and 1001. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs.
- VLAN configurations for VLANs 1 to 1005 are always saved in the VLAN database. If the VTP mode is transparent, VTP and VLAN configurations are also saved in the controller running configuration file.
- If the controller is in VTP server or VTP transparent mode, you can add, modify or remove configurations for VLANs 2 to 1001 in the VLAN database. (VLAN IDs 1 and 1002 to 1005 are automatically created and cannot be removed.)
- Extended-range VLANs created in VTP transparent mode are not saved in the VLAN database and are not propagated. VTP version 3 supports extended range VLAN (VLANs 1006 to 4094) database propagation in VTP server mode.
- Before you can create a VLAN, the controller must be in VTP server mode or VTP transparent mode. If the controller is a VTP server, you must define a VTP domain or VTP will not function.
- The controller does not support Token Ring or FDDI media. The controller does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic, but it does propagate the VLAN configuration through VTP.
- The controller supports 128 spanning tree instances. If a controller has more active VLANs than supported spanning-tree instances, spanning tree can be enabled on 128 VLANs and is disabled on the remaining VLANs. If you have already used all available spanning-tree instances on a controller, adding another VLAN anywhere in the VTP domain creates a VLAN on that controller that is not running spanning-tree. If you have the default allowed list on the trunk ports of that controller (which is to allow all VLANs), the new VLAN is carried on all trunk ports. Depending on the topology of the network, this could create a loop in the new VLAN that would not be broken, particularly if there are several adjacent controllers that all have run out of spanning-tree instances. You can prevent this possibility by setting allowed lists on the trunk ports of controllers that have used up their allocation of spanning-tree instances.

  If the number of VLANs on the controller exceeds the number of supported spanning-tree instances, we recommend that you configure the IEEE 802.1s Multiple STP (MSTP) on your controller to map multiple VLANs to a single spanning-tree instance.

Related Topics

Creating or Modifying an Ethernet VLAN , on page 51

Monitoring VLANs, on page 61

Extended-Range VLAN Configuration Guidelines

Extended-range VLANs are VLANs with IDs from 1006 to 4094.

Follow these guidelines when creating extended-range VLANs:

- VLAN IDs in the extended range are not saved in the VLAN database and are not recognized by VTP unless the controller is running VTP version 3.

- You cannot include extended-range VLANs in the pruning eligible range.
- For VTP version 1 or 2, you can set the VTP mode to transparent in global configuration mode. You should save this configuration to the startup configuration so that the controller boots up in VTP transparent mode. Otherwise, you lose the extended-range VLAN configuration if the controller resets. If you create extended-range VLANs in VTP version 3, you cannot convert to VTP version 1 or 2.

Related Topics

Creating an Extended-Range VLAN , on page 59
Monitoring VLANs, on page 61

Information About VLAN Groups

Whenever a client connects to a wireless network (WLAN), the client is placed in a VLAN that is associated with the WLAN. In a large venue such as an auditorium, a stadium, or a conference room where there are numerous wireless clients, having only a single WLAN to accommodate many clients might be a challenge.

The VLAN group feature uses a single WLAN that can support multiple VLANs. The clients can get assigned to one of the configured VLANs. This feature maps a WLAN to a single VLAN or multiple VLANs using the VLAN groups. When a wireless client associates to the WLAN, the VLAN is derived by an algorithm based on the MAC address of the wireless client. A VLAN is assigned to the client and the client gets the IP address from the assigned VLAN. This feature also extends the current AP group architecture and AAA override architecture, where the AP groups and AAA override can override a VLAN or a VLAN group to which the WLAN is mapped.

The system marks VLAN as "dirty" for 30 minutes when the clients are unable to receive IP address using DHCP. The system might not clear the "dirty" flag from the VLAN even after 30 minutes for a VLAN group. This is expected behavior because the timestamp of each interface has to be checked to see if it is greater than 30 minutes, due to which there is a lag of 5 minutes for the global timer to expire.

Related Topics

Creating VLAN Groups (CLI), on page 55

How to Configure VLANs

How to Configure Normal-Range VLANs

You can set these parameters when you create a new normal-range VLAN or modify an existing VLAN in the VLAN database:

- VLAN ID
- VLAN name
- VLAN type
  - Ethernet
  - Fiber Distributed Data Interface [FDDI]

- FDDI network entity title [NET]
- TrBRF or TrCRF
- Token Ring
- Token Ring-Net

- VLAN state (active or suspended)
- Maximum transmission unit (MTU) for the VLAN
- Security Association Identifier (SAID)
- Bridge identification number for TrBRF VLANs
- Ring number for FDDI and TrCRF VLANs
- Parent VLAN number for TrCRF VLANs
- Spanning Tree Protocol (STP) type for TrCRF VLANs
- VLAN number to use when translating from one VLAN type to another

You can cause inconsistency in the VLAN database if you attempt to manually delete the vlan.dat file. If you want to modify the VLAN configuration, follow the procedures in this section.

Creating or Modifying an Ethernet VLAN

Before You Begin

With VTP version 1 and 2, if the controller is in VTP transparent mode, you can assign VLAN IDs greater than 1006, but they are not added to the VLAN database.

The controller supports only Ethernet interfaces. Because FDDI and Token Ring VLANs are not locally supported, you only configure FDDI and Token Ring media-specific characteristics for VTP global advertisements to other controllers.

Although the controller does not support Token Ring connections, a remote device with Token Ring connections could be managed from one of the supported controllers. Controllers running VTP Version 2 advertise information about these Token Ring VLANs:

- Token Ring TrBRF VLANs
- Token Ring TrCRF VLANs

SUMMARY STEPS

1. **configure terminal**
2. **vlan** *vlan-id*
3. **name** *vlan-name*
4. **media** { **ethernet** | **fd-net** | **fddi** | **tokenring** | **trn-net** }
5. **remote-span**
6. **end**
7. **show vlan** {**name** *vlan-name* | **id** *vlan-id*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters the global configuration mode.
Step 2	**vlan** *vlan-id* **Example:** `Controller(config)# vlan 20`	Enters a VLAN ID, and enters VLAN configuration mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. **Note** The available VLAN ID range for this command is 1 to 4094. Additional **vlan** command options include: • **access-map—**Creates VLAN access-maps or enters the vlan access map command mode. • **configuration—**Enters the vlan feature configuration mode. • **dot1q—**Configures VLAN dot1q tag native parameters. • **filter—**Applies a VLAN filter map to a VLAN list. • **group—**Creates a VLAN group.
Step 3	**name** *vlan-name* **Example:** `Controller(config-vlan)# name test20`	(Optional) Enters a name for the VLAN. If no name is entered for the VLAN, the default is to append the *vlan-id* value with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4. The following additional VLAN configuration command options are available: • **are—**Sets the maximum number of All Router Explorer (ARE) hops for the VLAN. • **backupcrf—**Enables or disables the backup concentrator relay function (CRF) mode for the VLAN. • **bridge—**Sets the value of the bridge number for the FDDI net or Token Ring net type VLANs. • **exit—**Applies changes, bumps the revision number, and exits. • **media—**Sets the media type of the VLAN. • **no—**Negates the command or default. • **parent—**Sets the value of the ID for the parent VLAN for FDDI or Token Ring type VLANs. • **remote-span—**Configures a remote SPAN VLAN. • **ring—**Sets the ring number value for FDDI or Token Ring type VLANs. • **said—**Sets the IEEE 802.10 SAID value.

	Command or Action	Purpose
		• **shutdown—**Shuts down the VLAN switching. • **state—**Sets the operational VLAN state to active or suspended. • **ste—**Sets the maximum number of Spanning Tree Explorer (STE) hops for the VLAN. • **stp—**Sets the Spanning Tree characteristics of the VLAN.
Step 4	**media** { **ethernet** | **fd-net** | **fddi** | **tokenring** | **trn-net** } **Example:** `Controller(config-vlan)# media ethernet`	Configures the VLAN media type. Command options include: • **ethernet—**Sets the VLAN media type as Ethernet. • **fd-net—**Sets the VLAN media type as FDDI net. • **fddi—**Sets the VLAN media type as FDDI. • **tokenring—**Sets the VLAN media type as Token Ring. • **trn-net—**Sets the VLAN media type as Token Ring net.
Step 5	**remote-span** **Example:** `Controller(config-vlan)# remote-span`	(Optional) Configures the VLAN as the RSPAN VLAN for a remote SPAN session. For more information on remote SPAN, see the *Catalyst 3850 Network Management Configuration Guide*.
Step 6	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 7	**show vlan** {**name** *vlan-name* | **id** *vlan-id*} **Example:** `Controller# show vlan name test20 id 20`	Verifies your entries.

Related Topics

Normal-Range VLAN Configuration Guidelines, on page 49
Monitoring VLANs, on page 61

Deleting a VLAN

When you delete a VLAN from a controller that is in VTP server mode, the VLAN is removed from the VLAN database for all controllers in the VTP domain. When you delete a VLAN from a controller that is in VTP transparent mode, the VLAN is deleted only on that specific controller .

You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.

Caution When you delete a VLAN, any ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no vlan** *vlan-id*
4. **end**
5. **show vlan brief**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters the global configuration mode.
Step 3	**no vlan** *vlan-id* **Example:** `Controller(config)# no vlan 4`	Removes the VLAN by entering the VLAN ID.

	Command or Action	Purpose
Step 4	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 5	**show vlan brief** **Example:** `Controller# show vlan brief`	Verifies the VLAN removal.
Step 6	**copy running-config startup-config** **Example:** `Controller# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Monitoring VLANs, on page 61

Creating VLAN Groups (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **vlan group** *WORD* **vlan-list** *vlan-ID*
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global command mode.
Step 2	**vlan group** *WORD* **vlan-list** *vlan-ID* **Example:** `Controller(config)#vlan group vlangrp1 vlan-list 91-95`	Creates a VLAN group with the given group name (vlangrp1) and adds all the VLANs listed in the command. The VLAN list ranges from 1 to 4096 and the recommended number of VLANs in a group is 32.

	Command or Action	Purpose
Step 3	**end** **Example:** `Controller(config)#end`	Exits the global configuration mode and returns to privileged EXEC mode. Alternatively, press **CTRL-Z** to exit the global configuration mode.

Related Topics

Information About VLAN Groups, on page 50

Adding a VLAN Group to WLAN (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *WORD number*
3. **client vlan** *WORD*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global command mode.
Step 2	**wlan** *WORD number* **Example:** `Controller(config)#wlan wlanname 512`	Enables the WLAN to map a VLAN group using an identifier. The WLAN identifier values range from 1 to 512.
Step 3	**client vlan** *WORD* **Example:** `Controller(config-wlan)#client vlan vlangrp1`	Maps the VLAN group to the WLAN by entering the VLAN identifier, VLAN group, or the VLAN name.
Step 4	**end** **Example:** `Controller(config-wlan)#end`	Exits the global configuration mode and returns to privileged EXEC mode . Alternatively, press **CTRL-Z** to exit the global configuration mode.

Assigning Static-Access Ports to a VLAN

You can assign a static-access port to a VLAN without having VTP globally propagate VLAN configuration information by disabling VTP (VTP transparent mode).

If you are assigning a port on a cluster member controller to a VLAN, first use the **rcommand** privileged EXEC command to log in to the cluster member switch.

If you assign an interface to a VLAN that does not exist, the new VLAN is created.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **switchport mode access**
5. **switchport access vlan** *vlan-id*
6. **end**
7. **show running-config interface** *interface-id*
8. **show interfaces** *interface-id* **switchport**
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters global configuration mode
Step 3	**interface** *interface-id* **Example:** `Controller(config)# interface gigabitethernet2/0/1`	Enters the interface to be added to the VLAN.

	Command or Action	Purpose
Step 4	**switchport mode access** **Example:** `Controller(config-if)# switchport mode access`	Defines the VLAN membership mode for the port (Layer 2 access port).
Step 5	**switchport access vlan** *vlan-id* **Example:** `Controller(config-if)# switchport access vlan 2`	Assigns the port to a VLAN. Valid VLAN IDs are 1 to 4094.
Step 6	**end** **Example:** `Controller(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config interface** *interface-id* **Example:** `Controller# show running-config interface gigabitethernet2/0/1`	Verifies the VLAN membership mode of the interface.
Step 8	**show interfaces** *interface-id* **switchport** **Example:** `Controller# show interfaces gigabitethernet2/0/1 switchport`	Verifies your entries in the *Administrative Mode* and the *Access Mode VLAN* fields of the display.
Step 9	**copy running-config startup-config** **Example:** `Controller# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

VLAN Port Membership Modes, on page 47
Monitoring VLANs, on page 61

How to Configure Extended-Range VLANs

Extended-range VLANs enable service providers to extend their infrastructure to a greater number of customers. The extended-range VLAN IDs are allowed for any **switchport** commands that allow VLAN IDs.

With VTP version 1 or 2, extended-range VLAN configurations are not stored in the VLAN database, but because VTP mode is transparent, they are stored in the controller running configuration file, and you can save the configuration in the startup configuration file. Extended-range VLANs created in VTP version 3 are stored in the VLAN database.

You can change only the MTU size and the remote SPAN configuration state on extended-range VLANs; all other characteristics must remain at the default state.

Creating an Extended-Range VLAN

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vlan** *vlan-id*
4. **remote-span**
5. **exit**
6. **interface vlan**
7. **ip mtu** *mtu-size*
8. **end**
9. **show vlan id** *vlan-id*
10. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose

Step 3	**vlan** *vlan-id*
	
	Example:
	
	`Controller(config)# vlan 2000`
	`Controller(config-vlan)#`
		Enters an extended-range VLAN ID and enters VLAN configuration mode. The range is 1006 to 4094.

Step 4	**remote-span** **Example:** `Controller(config-vlan)# remote-span`	(Optional) Configures the VLAN as the RSPAN VLAN.

Step 5	**exit**
	
	Example:
	
	`Controller(config-vlan)# exit`
	`Controller(config)#`
		Returns to configuration mode.

Step 6	**interface vlan**
	
	Example:
	
	`Controller(config)# interface vlan 200`
	`Controller(config-if)#`
		Enters the interface configuration mode for the selected VLAN.

Step 7	**ip mtu** *mtu-size*
	
	Example:
	
	`Controller(config-if)# ip mtu 1024`
	`Controller(config-if)#`
		(Optional) Modifies the VLAN by changing the MTU size. You can configure the MTU size between 68 to 1500 bytes.
		
		Note Although all VLAN commands appear in the CLI help, only the **ip mtu** *mtu-size* and **remote-span** commands are supported for extended-range VLANs.

Step 8	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 9	**show vlan id** *vlan-id* **Example:** `Controller# show vlan id 2000`	Verifies that the VLAN has been created.
Step 10	**copy running-config startup-config** **Example:** `Controller# copy running-config`	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	`startup-config`	

Related Topics

Extended-Range VLAN Configuration Guidelines, on page 49
Monitoring VLANs, on page 61

Monitoring VLANs

Table 7: Privileged EXEC show Commands

Command	Purpose
show interfaces [**vlan** *vlan-id*]	Displays characteristics for all interfaces or for the specified VLAN configured on the controller .
show vlan [**access-map** *name* | **brief** | **dot1q** { **tag native** } | **filter** [**access-map** | **vlan**] | **group** [**group-name** *name*] | **id** *vlan-id* | **ifindex** | **mtu** | **name** *name* | **remote-span** | **summary**]	Displays parameters for all VLANs or the specified VLAN on the controller. The following command options are available: • **access-map—**Displays the VLAN access-maps. • **brief—**Displays VTP VLAN status in brief. • **dot1q—**Displays the dot1q parameters. • **filter—**Displays VLAN filter information. • **group—**Displays the VLAN group with its name and the connected VLANs that are available. • **id—**Displays VTP VLAN status by identification number. • **ifindex—**Displays SNMP ifIndex. • **mtu—**Displays VLAN MTU information. • **name—**Displays the VTP VLAN information by specified name. • **remote-span–**Displays the remote SPAN VLANs. • **summary—**Displays a summary of VLAN information.

Related Topics

Creating or Modifying an Ethernet VLAN , on page 51
Normal-Range VLAN Configuration Guidelines, on page 49
Deleting a VLAN , on page 54
Assigning Static-Access Ports to a VLAN, on page 57
VLAN Port Membership Modes, on page 47
Creating an Extended-Range VLAN , on page 59
Extended-Range VLAN Configuration Guidelines, on page 49

Where to Go Next

After configuring VLANs, you can configure the following:

- VLAN groups
- VLAN Trunking Protocol (VTP)
- VLAN trunks
- VLAN Membership Policy Server (VMPS)

Additional References

Standards and RFCs

Standard/RFC	Title
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIBs

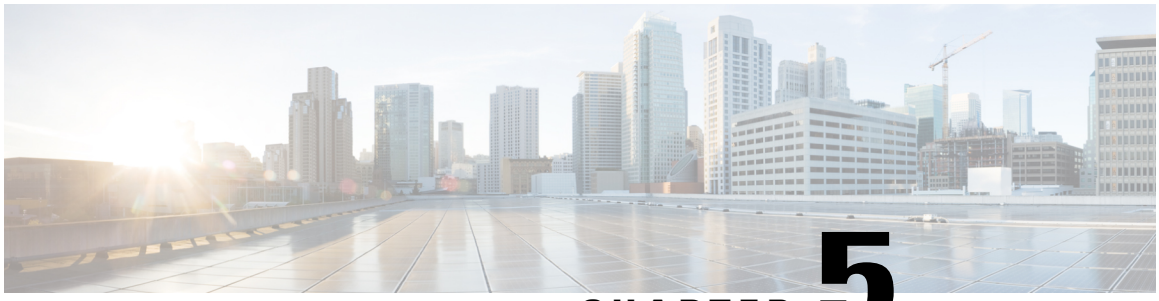
MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

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

Feature History and Information for VLANs

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced
Cisco IOS XE 3.3SE	VLAN GUI support.



CHAPTER 5

Configuring VLAN Group

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VLAN Groups

- A VLAN should be present in the controller to be able to add it to the VLAN group.
- For VLAN group to function properly, in addition to enabling DHCP snooping globally, you must ensure that DHCP snooping is enabled in all the VLANs.

Restrictions for VLAN Groups

The number of VLANs mapped to a VLAN group is not limited by Cisco IOS Software Release. But if the number of VLANs in a VLAN group exceed the recommended value of 32, the mobility behavior is unexpected and in the VLAN group, L2 multicast breaks for some VLANs. So it is the responsibility of the administrator to configure feasible number of VLANs in a VLAN group. When a VLAN is added to a VLAN group mapped to a WLAN which already has 32 VLANs, a warning is generated. But when a new VLAN group is mapped to a WLAN with more than 32 VLANs, an error is generated.

For expected behavior of the VLAN group, the VLANs mapped in the group must be present in the controller. The static IP client behavior is not supported.

Information About VLAN Groups

Whenever a client connects to a wireless network (WLAN), the client is placed in a VLAN that is associated with the WLAN. In a large venue such as an auditorium, a stadium, or a conference room where there are numerous wireless clients, having only a single WLAN to accommodate many clients might be a challenge.

The VLAN group feature uses a single WLAN that can support multiple VLANs. The clients can get assigned to one of the configured VLANs. This feature maps a WLAN to a single VLAN or multiple VLANs using the VLAN groups. When a wireless client associates to the WLAN, the VLAN is derived by an algorithm based on the MAC address of the wireless client. A VLAN is assigned to the client and the client gets the IP address from the assigned VLAN. This feature also extends the current AP group architecture and AAA override architecture, where the AP groups and AAA override can override a VLAN or a VLAN group to which the WLAN is mapped.

The system marks VLAN as "dirty" for 30 minutes when the clients are unable to receive IP address using DHCP. The system might not clear the "dirty" flag from the VLAN even after 30 minutes for a VLAN group. This is expected behavior because the timestamp of each interface has to be checked to see if it is greater than 30 minutes, due to which there is a lag of 5 minutes for the global timer to expire.

Related Topics

Creating VLAN Groups (CLI), on page 55

How to Configure VLAN Groups

Creating VLAN Groups (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **vlan group** *WORD* **vlan-list** *vlan-ID*
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global command mode.
Step 2	**vlan group** *WORD* **vlan-list** *vlan-ID* **Example:** `Controller(config)#vlan group vlangrp1 vlan-list 91-95`	Creates a VLAN group with the given group name (vlangrp1) and adds all the VLANs listed in the command. The VLAN list ranges from 1 to 4096 and the recommended number of VLANs in a group is 32.
Step 3	**end** **Example:** `Controller(config)#end`	Exits the global configuration mode and returns to privileged EXEC mode. Alternatively, press **CTRL-Z** to exit the global configuration mode.

Related Topics

Information About VLAN Groups, on page 50

Removing VLAN Group (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **vlan group** *WORD* **vlan-list** *vlan-ID*
3. **no vlan group** *WORD* **vlan-list** *vlan-ID*
4. **end**

DETAILED STEPS

Step 1 **configure terminal**

Example:
`Controller# configure terminal`
Enters global command mode.

Step 2 **vlan group** *WORD* **vlan-list** *vlan-ID*

Example:
`Controller(config)#vlan group vlangrp1 vlan-list 91-95`

Creates a VLAN group with the given group name (vlangrp1) and adds all the VLANs listed in the command. The VLAN list ranges from 1 to 4096 and the recommended number of VLANs in a group is 32.

Step 3 **no vlan group** *WORD* **vlan-list** *vlan-ID*

Example:

```
Controller(config)#no vlan group vlangrp1 vlan-list 91-95
```

Removes the VLAN group with the given group name (vlangrp1).

Step 4 **end**

Example:

```
Controller(config)#end
```

Exits the global configuration mode and returns to privileged EXEC mode. Alternatively, press **CTRL-Z** to exit the global configuration mode.

Creating VLAN Groups (GUI)

To create a VLAN group using the controller web UI, you must:

Step 1 Choose **Configuration > Controller > System > VLAN** > **VLAN Group.**
The VLAN Group page appears. You must provide values for all parameters listed in the VLAN Group window.

Parameter	Description
VLAN Group Name	Group name for the VLANs.
VLAN List	The VLAN list to configure the mesh access point (MAP) access port.

Step 2 Click **Apply**.

Adding a VLAN Group to WLAN (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *WORD number*
3. **client vlan** *WORD*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global command mode.
Step 2	**wlan** *WORD number* **Example:** `Controller(config)#wlan wlanname 512`	Enables the WLAN to map a VLAN group using an identifier. The WLAN identifier values range from 1 to 512.
Step 3	**client vlan** *WORD* **Example:** `Controller(config-wlan)#client vlan vlangrp1`	Maps the VLAN group to the WLAN by entering the VLAN identifier, VLAN group, or the VLAN name.
Step 4	**end** **Example:** `Controller(config-wlan)#end`	Exits the global configuration mode and returns to privileged EXEC mode . Alternatively, press **CTRL-Z** to exit the global configuration mode.

Adding a VLAN Group to WLAN (GUI)

To add a VLAN group to WLAN using the controller web UI, you must follow the steps defined in this procedure.

Step 1 To add a VLAN group to a WLAN, choose **Configuration > Wireless > WLANs > WLAN Profile > General.** The general parameter page of the WLAN group appears.

Step 2 Select the VLAN group values listed in the **Interface/Interface Group** drop-down list to associate the selected WLAN profile to a VLAN group.

Step 3 Click **Apply.**

Removing VLAN Groups (GUI)

To remove a VLAN groups using the controller web UI, you must:

Step 1 Choose **Configuration > Controller > System > VLAN** > **VLAN Group.**

The VLAN Group page appears, listing the following details of the VLAN groups associated with the controller.

Parameter	Description
VLAN Group Name	Group name for the VLANs.
VLAN List	The VLAN list to configure the mesh access point (MAP) access port.

Step 2 Check the checkbox of the VLAN group you need to delete from the VLAN group names displayed in the VLAN group list .
You will receive a confirmation message confirming deletion of the selected VLAN group.

Step 3 Click **Ok**.

Viewing VLANs in VLAN Groups (CLI)

Commands	Description
`show vlan group`	Displays the list of VLAN groups with its name and the VLANs that are available.
`show vlan group group-name <group_name>`	Displays the specified VLAN group details.
`show wireless vlan group <group_name>`	Displays the specified wireless VLAN group details.

Viewing VLAN Groups (GUI)

To view a VLAN groups using the controller web UI, you must:

Step 1 Choose **Configuration > Controller > System > VLAN** > **VLAN Group.**
The VLAN Group page appears, listing the following details of the VLAN groups associated with the controller.

Parameter	Description
VLAN Group Name	Group name for the VLANs.
VLAN List	The VLAN list to configure the mesh access point (MAP) access port.

Step 2 Click **Apply**.

Where to Go Next

After configuring VLAN groups, you can configure the following:

- VLANs
- VLAN Trunking Protocol (VTP)
- VLAN trunks

Additional References

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	*VLAN Command Reference (Catalyst 3850 Switches) VLAN Command Reference (Cisco WLC 5700 Series)* *Layer 2/3 Command Reference (Catalyst 3850 Switches)Layer 2 Command Reference (Cisco WLC 5700 Series)*
VLAN access-maps	*Security Configuration Guide (Catalyst 3850 Switches)Security Configuration Guide (Cisco WLC 5700 Series)* *Security Command Reference (Catalyst 3850 Switches)Security Command Reference (Cisco WLC 5700 Series)*
VLAN and Mobility Agents	*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
Cisco Flexible NetFlow	*Cisco Flexible NetFlow Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)* *Flexible Netflow Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
IGMP Snooping	*IP Multicast Routing Command Reference (Catalyst 3850 Switches)Cisco 5760 Multicast Command Reference (Cisco WLC 5700 Series)* *IP Multicast Routing Configuration Guide (Catalyst 3850 Switches)Routing Configuration Guide (Cisco WLC 5700 Series)*

Related Topic	Document Title
IPv6	*IPv6 Configuration Guide (Catalyst 3850 Switches)IPv6 Configuration Guide (Cisco WLC 5700 Series)* *IPv6 Command Reference (Catalyst 3850 Switches)IPv6 Command Reference (Cisco WLC 5700 Series)*
SPAN	*Network Management Command Reference (Catalyst 3850 Switches)Network Management Command Reference (Cisco WLC 5700 Series)* *Network Management Configuration Guide (Catalyst 3850 Switches) Network Management Configuration Guide (Cisco WLC 5700 Series)*
Platform-independent configuration information	*Identity Based Networking Services Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Error Message Decoder

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

Standards and RFCs

Standard/RFC	Title
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIBs

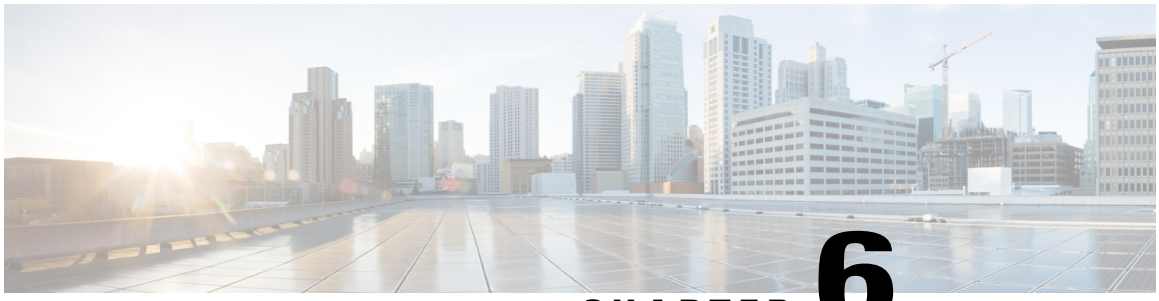
MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

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

Feature History and Information for VLAN Groups

Release	Modification
Cisco IOS XE 3.2E	This feature was introduced
Cisco IOS XE 3.3SE	VLAN GUI support.



CHAPTER 6

Configuring VLAN Trunks

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VLAN Trunks

The IEEE 802.1Q trunks impose these limitations on the trunking strategy for a network:

- In a network of Cisco controllers connected through IEEE 802.1Q trunks, the controllers maintain one spanning-tree instance for each VLAN allowed on the trunks. Non-Cisco devices might support one spanning-tree instance for all VLANs.

  When you connect a Cisco controller to a non-Cisco device through an IEEE 802.1Q trunk, the Cisco controller combines the spanning-tree instance of the VLAN of the trunk with the spanning-tree instance of the non-Cisco IEEE 802.1Q controller. However, spanning-tree information for each VLAN is

maintained by Cisco controllers separated by a cloud of non-Cisco IEEE 802.1Q controllers. The non-Cisco IEEE 802.1Q cloud separating the Cisco controllers is treated as a single trunk link between the controllers.

- Make sure the native VLAN for an IEEE 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.
- Disabling spanning tree on the native VLAN of an IEEE 802.1Q trunk without disabling spanning tree on every VLAN in the network can potentially cause spanning-tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an IEEE 802.1Q trunk or disable spanning tree on every VLAN in the network. Make sure your network is loop-free before disabling spanning tree.

Restrictions for VLAN Trunks

The following are restrictions for VLAN trunks:

- A trunk port cannot be a secure port.
- Trunk ports can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration. When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, the controller propagates the setting that you entered to all ports in the group:
  - Allowed-VLAN list.
  - STP port priority for each VLAN.
  - STP Port Fast setting.
  - Trunk status:

    If one port in a port group ceases to be a trunk, all ports cease to be trunks.
- We recommend that you configure no more than 24 trunk ports in Per VLAN Spanning Tree (PVST) mode and no more than 40 trunk ports in Multiple Spanning Tree (MST) mode.
- If you try to enable IEEE 802.1x on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, the port mode is not changed.
- A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable IEEE 802.1x on a dynamic port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to dynamic, the port mode is not changed.
- Dynamic Trunking Protocol (DTP) is not supported on tunnel ports.
- You cannot have a switch stack containing a mix of Catalyst 3850 and Catalyst 3650 switches.

Information About VLAN Trunks

Trunking Overview

A trunk is a point-to-point link between one or more Ethernet controller interfaces and another networking device such as a router or a controller. Ethernet trunks carry the traffic of multiple VLANs over a single link, and you can extend the VLANs across an entire network.

The following trunking encapsulations are available on all Ethernet interfaces:

- IEEE 802.1Q— Industry-standard trunking encapsulation.

Trunking Modes

Ethernet trunk interfaces support different trunking modes. You can set an interface as trunking or nontrunking or to negotiate trunking with the neighboring interface. To autonegotiate trunking, the interfaces must be in the same VTP domain.

Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a Point-to-Point Protocol (PPP). However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations.

Related Topics

Configuring a Trunk Port , on page 80
Layer 2 Interface Modes, on page 77

Layer 2 Interface Modes

Table 8: Layer 2 Interface Modes

Mode	Function
switchport mode access	Puts the interface (access port) into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface regardless of whether or not the neighboring interface is a trunk interface.
switchport mode dynamic auto	Makes the interface able to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to **trunk** or **desirable** mode. The default switchport mode for all Ethernet interfaces is **dynamic auto**.

Mode	Function
switchport mode dynamic desirable	Makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.
switchport mode trunk	Puts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link. The interface becomes a trunk interface even if the neighboring interface is not a trunk interface.
switchport nonegotiate	Prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is **access** or **trunk**. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.

Related Topics

Configuring a Trunk Port , on page 80
Trunking Modes, on page 77

Allowed VLANs on a Trunk

By default, a trunk port sends traffic to and receives traffic from all VLANs. All VLAN IDs, 1 to 4094, are allowed on each trunk. However, you can remove VLANs from the allowed list, preventing traffic from those VLANs from passing over the trunk.

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), DTP, and VTP in VLAN 1.

If a trunk port with VLAN 1 disabled is converted to a nontrunk port, it is added to the access VLAN. If the access VLAN is set to 1, the port will be added to VLAN 1, regardless of the **switchport trunk allowed** setting. The same is true for any VLAN that has been disabled on the port.

A trunk port can become a member of a VLAN if the VLAN is enabled, if VTP knows of the VLAN, and if the VLAN is in the allowed list for the port. When VTP detects a newly enabled VLAN and the VLAN is in the allowed list for a trunk port, the trunk port automatically becomes a member of the enabled VLAN. When VTP detects a new VLAN and the VLAN is not in the allowed list for a trunk port, the trunk port does not become a member of the new VLAN.

Related Topics

Defining the Allowed VLANs on a Trunk , on page 83

Load Sharing on Trunk Ports

Load sharing divides the bandwidth supplied by parallel trunks connecting controllers. To avoid loops, STP normally blocks all but one parallel link between controllers. Using load sharing, you divide the traffic between the links according to which VLAN the traffic belongs.

You configure load sharing on trunk ports by using STP port priorities or STP path costs. For load sharing using STP port priorities, both load-sharing links must be connected to the same controller. For load sharing using STP path costs, each load-sharing link can be connected to the same controller or to two different controllers.

Network Load Sharing Using STP Priorities

When two ports on the same controller form a loop, the controller uses the STP port priority to decide which port is enabled and which port is in a blocking state. You can set the priorities on a parallel trunk port so that the port carries all the traffic for a given VLAN. The trunk port with the higher priority (lower values) for a VLAN is forwarding traffic for that VLAN. The trunk port with the lower priority (higher values) for the same VLAN remains in a blocking state for that VLAN. One trunk port sends or receives all traffic for the VLAN.

Related Topics

Configuring Load Sharing Using STP Port Priorities , on page 88

Network Load Sharing Using STP Path Cost

You can configure parallel trunks to share VLAN traffic by setting different path costs on a trunk and associating the path costs with different sets of VLANs, blocking different ports for different VLANs. The VLANs keep the traffic separate and maintain redundancy in the event of a lost link.

Related Topics

Configuring Load Sharing Using STP Path Cost , on page 92

Feature Interactions

Trunking interacts with other features in these ways:

- A trunk port cannot be a secure port.
- Trunk ports can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration. When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, the controller propagates the setting that you entered to all ports in the group:
  - Allowed-VLAN list.
  - STP port priority for each VLAN.
  - STP Port Fast setting.
  - Trunk status:

If one port in a port group ceases to be a trunk, all ports cease to be trunks.

- We recommend that you configure no more than 24 trunk ports in Per VLAN Spanning Tree (PVST) mode and no more than 40 trunk ports in Multiple Spanning Tree (MST) mode.
- If you try to enable IEEE 802.1x on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, the port mode is not changed.
- A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable IEEE 802.1x on a dynamic port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to dynamic, the port mode is not changed.

How to Configure VLAN Trunks

To avoid trunking misconfigurations, configure interfaces connected to devices that do not support DTP to not forward DTP frames, that is, to turn off DTP.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

Configuring an Ethernet Interface as a Trunk Port

Configuring a Trunk Port

Because trunk ports send and receive VTP advertisements, to use VTP you must ensure that at least one trunk port is configured on the controller and that this trunk port is connected to the trunk port of a second controller. Otherwise, the controller cannot receive any VTP advertisements.

Before You Begin

By default, an interface is in Layer 2 mode. The default mode for Layer 2 interfaces is **switchport mode dynamic auto**. If the neighboring interface supports trunking and is configured to allow trunking, the link is a Layer 2 trunk or, if the interface is in Layer 3 mode, it becomes a Layer 2 trunk when you enter the **switchport** interface configuration command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk**}
5. **switchport access vlan** *vlan-id*
6. **switchport trunk native vlan** *vlan-id*
7. **end**
8. **show interfaces** *interface-id* **switchport**
9. **show interfaces** *interface-id* **trunk**
10. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Controller(config)# interface gigabitethernet1/0/2`	Specifies the port to be configured for trunking, and enters interface configuration mode.
Step 4	**switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk**} **Example:** `Controller(config-if)# switchport mode dynamic desirable`	Configures the interface as a Layer 2 trunk (required only if the interface is a Layer 2 access port or tunnel port or to specify the trunking mode). • **dynamic auto—**Sets the interface to a trunk link if the neighboring interface is set to trunk or desirable mode. This is the default. • **dynamic desirable—**Sets the interface to a trunk link if the neighboring interface is set to trunk, desirable, or auto mode.

	Command or Action	Purpose
		• **trunk—**Sets the interface in permanent trunking mode and negotiate to convert the link to a trunk link even if the neighboring interface is not a trunk interface.
Step 5	**switchport access vlan** *vlan-id* **Example:** `Controller(config-if)# switchport access vlan 200`	(Optional) Specifies the default VLAN, which is used if the interface stops trunking.
Step 6	**switchport trunk native vlan** *vlan-id* **Example:** `Controller(config-if)# switchport trunk native vlan 200`	Specifies the native VLAN for IEEE 802.1Q trunks.
Step 7	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 8	**show interfaces** *interface-id* **switchport** **Example:** `Controller# show interfaces gigabitethernet1/0/2 switchport`	Displays the switch port configuration of the interface in the *Administrative Mode* and the *Administrative Trunking Encapsulation* fields of the display.
Step 9	**show interfaces** *interface-id* **trunk** **Example:** `Controller# show interfaces gigabitethernet1/0/2 trunk`	Displays the trunk configuration of the interface.
Step 10	**copy running-config startup-config** **Example:** `Controller# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Trunking Modes, on page 77

Layer 2 Interface Modes, on page 77

Defining the Allowed VLANs on a Trunk

VLAN 1 is the default VLAN on all trunk ports in all Cisco controllers, and it has previously been a requirement that VLAN 1 always be enabled on every trunk link. You can use the VLAN 1 minimization feature to disable VLAN 1 on any individual VLAN trunk link so that no user traffic (including spanning-tree advertisements) is sent or received on VLAN 1.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **switchport mode trunk**
5. **switchport trunk allowed vlan** { *word* | **add** | **all** | **except** | **none** | **remove**} *vlan-list*
6. **end**
7. **show interfaces** *interface-id* **switchport**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Controller(config)# interface gigabitethernet1/0/1`	Specifies the port to be configured, and enters interface configuration mode.
Step 4	**switchport mode trunk** **Example:** `Controller(config-if)# switchport mode trunk`	Configures the interface as a VLAN trunk port.

	Command or Action	Purpose
Step 5	**switchport trunk allowed vlan** { *word* | **add** | **all** | **except** | **none** | **remove**} *vlan-list* **Example:** `Controller(config-if)# switchport trunk allowed vlan remove 2`	(Optional) Configures the list of VLANs allowed on the trunk. The *vlan-list* parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated VLAN parameters or in hyphen-specified ranges. All VLANs are allowed by default.
Step 6	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 7	**show interfaces** *interface-id* **switchport** **Example:** `Controller# show interfaces gigabitethernet1/0/1 switchport`	Verifies your entries in the *Trunking VLANs Enabled* field of the display.
Step 8	**copy running-config startup-config** **Example:** `Controller# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Allowed VLANs on a Trunk, on page 78

Changing the Pruning-Eligible List

The pruning-eligible list applies only to trunk ports. Each trunk port has its own eligibility list. VTP pruning must be enabled for this procedure to take effect.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**} *vlan-list* [,*vlan* [,*vlan* [,,,]]
5. **end**
6. **show interfaces** *interface-id* **switchport**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Controller(config)# interface gigabitethernet2/0/1`	Selects the trunk port for which VLANs should be pruned, and enters interface configuration mode.
Step 4	**switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**} *vlan-list* [,*vlan* [,*vlan* [,,,]]	Configures the list of VLANs allowed to be pruned from the trunk. For explanations about using the **add**, **except**, **none**, and **remove** keywords, see the command reference for this release. Separate non-consecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Valid IDs are 2 to 1001. Extended-range VLANs (VLAN IDs 1006 to 4094) cannot be pruned. VLANs that are pruning-ineligible receive flooded traffic. The default list of VLANs allowed to be pruned contains VLANs 2 to 1001.

	Command or Action	Purpose
Step 5	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 6	**show interfaces** *interface-id* **switchport** **Example:** `Controller# show interfaces gigabitethernet2/0/1 switchport`	Verifies your entries in the *Pruning VLANs Enabled* field of the display.
Step 7	**copy running-config startup-config** **Example:** `Controller# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring the Native VLAN for Untagged Traffic

A trunk port configured with IEEE 802.1Q tagging can receive both tagged and untagged traffic. By default, the controller forwards untagged traffic in the native VLAN configured for the port. The native VLAN is VLAN 1 by default.

The native VLAN can be assigned any VLAN ID.

If a packet has a VLAN ID that is the same as the outgoing port native VLAN ID, the packet is sent untagged; otherwise, the controller sends the packet with a tag.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **switchport trunk native vlan** *vlan-id*
5. **end**
6. **show interfaces** *interface-id* **switchport**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Controller(config)# interface gigabitethernet1/0/2`	Defines the interface that is configured as the IEEE 802.1Q trunk, and enters interface configuration mode.
Step 4	**switchport trunk native vlan** *vlan-id* **Example:** `Controller(config-if)# switchport trunk native vlan 12`	Configures the VLAN that is sending and receiving untagged traffic on the trunk port. For *vlan-id*, the range is 1 to 4094.
Step 5	**end** **Example:** `Controller(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show interfaces** *interface-id* **switchport** **Example:** `Controller# show interfaces gigabitethernet1/0/2 switchport`	Verifies your entries in the *Trunking Native Mode VLAN* field.
Step 7	**copy running-config startup-config** **Example:** `Controller# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Trunk Ports for Load Sharing

Configuring Load Sharing Using STP Port Priorities

These steps describe how to configure a network with load sharing using STP port priorities.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vtp domain** *domain-name*
4. **vtp mode server**
5. **end**
6. **show vtp status**
7. **show vlan**
8. **configure terminal**
9. **interface** *interface-id*
10. **switchport mode trunk**
11. **end**
12. **show interfaces** *interface-id* **switchport**
13. Repeat the above steps on Controller A for a second port in the controller.
14. Repeat the above steps on Controller B to configure the trunk ports that connect to the trunk ports configured on Controller A.
15. **show vlan**
16. **configure terminal**
17. **interface** *interface-id*
18. **spanning-tree vlan** *vlan-range* **port-priority** *priority-value*
19. **exit**
20. **interface** *interface-id*
21. **spanning-tree vlan** *vlan-range* **port-priority** *priority-value*
22. **end**
23. **show running-config**
24. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters global configuration mode on Controller A.
Step 3	**vtp domain** *domain-name* **Example:** `Controller(config)# vtp domain workdomain`	Configures a VTP administrative domain. The domain name can be 1 to 32 characters.
Step 4	**vtp mode server** **Example:** `Controller(config)# vtp mode server`	Configures Controller A as the VTP server.
Step 5	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 6	**show vtp status** **Example:** `Controller# show vtp status`	Verifies the VTP configuration on both Controller A and Controller B. In the display, check the *VTP Operating Mode* and the *VTP Domain Name* fields.
Step 7	**show vlan** **Example:** `Controller# show vlan`	Verifies that the VLANs exist in the database on Controller A.
Step 8	**configure terminal** **Example:** `Controller# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 9	**interface** *interface-id* **Example:** `Controller(config)# interface gigabitethernet1/0/1`	Defines the interface to be configured as a trunk, and enters interface configuration mode.
Step 10	**switchport mode trunk** **Example:** `Controller(config-if)# switchport mode trunk`	Configures the port as a trunk port.
Step 11	**end** **Example:** `Controller(config-if)# end`	Returns to privileged EXEC mode.
Step 12	**show interfaces** *interface-id* **switchport** **Example:** `Controller# show interfaces gigabitethernet1/0/1 switchport`	Verifies the VLAN configuration.
Step 13	Repeat the above steps on Controller A for a second port in the controller.	
Step 14	Repeat the above steps on Controller B to configure the trunk ports that connect to the trunk ports configured on Controller A.	
Step 15	**show vlan** **Example:** `Controller# show vlan`	When the trunk links come up, VTP passes the VTP and VLAN information to Controller B. This command verifies that Controller B has learned the VLAN configuration.
Step 16	**configure terminal** **Example:** `Controller# configure terminal`	Enters global configuration mode on Controller A.
Step 17	**interface** *interface-id* **Example:** `Controller(config)# interface gigabitethernet1/0/1`	Defines the interface to set the STP port priority, and enters interface configuration mode.

	Command or Action	Purpose
Step 18	**spanning-tree vlan** *vlan-range* **port-priority** *priority-value* **Example:** `Controller(config-if)# spanning-tree vlan 8-10 port-priority 16`	Assigns the port priority for the VLAN range specified. Enter a port priority value from 0 to 240. Port priority values increment by 16.
Step 19	**exit** **Example:** `Controller(config-if)# exit`	Returns to global configuration mode.
Step 20	**interface** *interface-id* **Example:** `Controller(config)# interface gigabitethernet1/0/2`	Defines the interface to set the STP port priority, and enters interface configuration mode.
Step 21	**spanning-tree vlan** *vlan-range* **port-priority** *priority-value* **Example:** `Controller(config-if)# spanning-tree vlan 3-6 port-priority 16`	Assigns the port priority for the VLAN range specified. Enter a port priority value from 0 to 240. Port priority values increment by 16.
Step 22	**end** **Example:** `Controller(config-if)# end`	Returns to privileged EXEC mode.
Step 23	**show running-config** **Example:** `Controller# show running-config`	Verifies your entries.
Step 24	**copy running-config startup-config** **Example:** `Controller# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Network Load Sharing Using STP Priorities, on page 79

Configuring Load Sharing Using STP Path Cost

These steps describe how to configure a network with load sharing using STP path costs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **switchport mode trunk**
5. **exit**
6. Repeat Steps 2 through 4 on a second interface in Controller A .
7. **end**
8. **show running-config**
9. **show vlan**
10. **configure terminal**
11. **interface** *interface-id*
12. **spanning-tree vlan** *vlan-range* **cost** *cost-value*
13. **end**
14. Repeat Steps 9 through 13 on the other configured trunk interface on Controller A, and set the spanning-tree path cost to 30 for VLANs 8, 9, and 10.
15. **exit**
16. **show running-config**
17. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters global configuration mode on Controller A.

	Command or Action	Purpose
Step 3	**interface** *interface-id* **Example:** `Controller(config)# interface gigabitethernet1/0/1`	Defines the interface to be configured as a trunk, and enters interface configuration mode.
Step 4	**switchport mode trunk** **Example:** `Controller(config-if)# switchport mode trunk`	Configures the port as a trunk port.
Step 5	**exit** **Example:** `Controller(config-if)# exit`	Returns to global configuration mode.
Step 6	Repeat Steps 2 through 4 on a second interface in Controller A .	
Step 7	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 8	**show running-config** **Example:** `Controller# show running-config`	Verifies your entries. In the display, make sure that the interfaces are configured as trunk ports.
Step 9	**show vlan** **Example:** `Controller# show vlan`	When the trunk links come up, Controller A receives the VTP information from the other controllers. This command verifies that Controller A has learned the VLAN configuration.
Step 10	**configure terminal** **Example:** `Controller# configure terminal`	Enters global configuration mode.
Step 11	**interface** *interface-id* **Example:** `Controller(config)# interface`	Defines the interface on which to set the STP cost, and enters interface configuration mode.

	Command or Action	Purpose
	gigabitethernet1/0/1	
Step 12	**spanning-tree vlan** *vlan-range* **cost** *cost-value* **Example:** `Controller(config-if)# spanning-tree vlan 2-4 cost 30`	Sets the spanning-tree path cost to 30 for VLANs 2 through 4.
Step 13	**end** **Example:** `Controller(config-if)# end`	Returns to global configuration mode.
Step 14	Repeat Steps 9 through 13 on the other configured trunk interface on Controller A, and set the spanning-tree path cost to 30 for VLANs 8, 9, and 10.	
Step 15	**exit** **Example:** `Controller(config)# exit`	Returns to privileged EXEC mode.
Step 16	**show running-config** **Example:** `Controller# show running-config`	Verifies your entries. In the display, verify that the path costs are set correctly for both trunk interfaces.
Step 17	**copy running-config startup-config** **Example:** `Controller# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Network Load Sharing Using STP Path Cost, on page 79

Where to Go Next

After configuring VLAN trunks, you can configure the following:

- VLANs

- VLAN groups

Additional References

Related Documents

Related Topic	Document Title
CLI commands	*VLAN Command Reference (Catalyst 3850 Switches)* *VLAN Command Reference (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIBs

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

Technical Assistance

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

Feature History and Information for VLAN Trunks

Release	Modification

INDEX

S

T

V