



Catalyst 2960-XR Switch Layer 2 Command Reference, Cisco IOS Release 15.0(2)EX1

First Published: August 08, 2013

Americas Headquarters

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

Text Part Number: OL-29423-01

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

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

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

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

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

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

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

© 2013 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface

Preface vii

Document Conventions vii

Related Documentation ix

Obtaining Documentation and Submitting a Service Request ix

CHAPTER 1

Using the Command-Line Interface 1

Information About Using the Command-Line Interface 1

Command Modes 1

Using the Help System 3

Understanding Abbreviated Commands 4

No and default Forms of Commands 4

CLI Error Messages 4

Configuration Logging 5

How to Use the CLI to Configure Features 5

Configuring the Command History 5

Changing the Command History Buffer Size 6

Recalling Commands 6

Disabling the Command History Feature 7

Enabling and Disabling Editing Features 7

Editing Commands through Keystrokes 9

Editing Command Lines That Wrap 10

Searching and Filtering Output of show and more Commands 11

Accessing the CLI through a Console Connection or through Telnet 12

CHAPTER 2

Layer 2/3 Commands 13

channel-group 16

channel-protocol 19

clear lacp	21
clear pagp	22
clear spanning-tree counters	23
clear spanning-tree detected-protocols	24
debug etherchannel	25
debug lacp	27
debug pagp	28
debug platform etherchannel	30
debug platform pm	31
debug spanning-tree	34
debug platform udld	36
interface port-channel	37
lacp port-priority	39
lacp system-priority	41
link state group	43
link state track	44
pagp learn-method	45
pagp port-priority	47
pagp timer	49
port-channel load-balance	50
show etherchannel	51
show lacp	54
show link state group	59
show pagp	60
show platform backup interface	62
show platform etherchannel	63
show platform pm	64
show platform spanning-tree	66
show spanning-tree	67
show udld	70
spanning-tree backbonefast	73
spanning-tree bpdufilter	74
spanning-tree bpduguard	76
spanning-tree cost	77
spanning-tree etherchannel guard misconfig	79

spanning-tree extend system-id	80
spanning-tree guard	82
spanning-tree link-type	84
spanning-tree loopguard default	85
spanning-tree mode	86
spanning-tree mst configuration	88
spanning-tree mst cost	90
spanning-tree mst forward-time	91
spanning-tree mst hello-time	92
spanning-tree mst max-age	93
spanning-tree mst max-hops	94
spanning-tree mst port-priority	95
spanning-tree mst pre-standard	96
spanning-tree mst priority	97
spanning-tree mst root	98
spanning-tree pathcost method	100
spanning-tree port-priority	101
spanning-tree portfast (global configuration)	102
spanning-tree portfast (interface configuration)	104
spanning-tree transmit hold-count	106
spanning-tree uplinkfast	107
spanning-tree vlan	109
switchport access vlan	111
switchport mode	113
switchport nonegotiate	116
udld	118
udld port	120
udld reset	122



Preface

This preface contains the following topics:

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

Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^D or Ctrl-D means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands and keywords and user-entered text appear in bold font .
<i>Italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
Courier font	Terminal sessions and information the system displays appear in <i>courier font</i> .
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.

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

Reader Alert Conventions

This document uses the following conventions for reader alerts:



Note

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



Tip

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



Caution

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



Timesaver

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



Warning

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

Related Documentation

**Note**

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

- Catalyst 2960-XR Switch documentation, located at:
http://www.cisco.com/go/cat2960xr_docs
- Cisco SFP and SFP+ modules documentation, including compatibility matrixes, located at:
http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html
- Cisco Validated Designs documents, located at:
<http://www.cisco.com/go/designzone>

Obtaining Documentation and Submitting a Service Request

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

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

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



Using the Command-Line Interface

- [Information About Using the Command-Line Interface, page 1](#)
- [How to Use the CLI to Configure Features, page 5](#)

Information About Using the Command-Line Interface

Command Modes

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

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

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

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

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

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

Table 1: Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session using Telnet, SSH, or console.	Switch>	Enter logout or quit .	Use this mode to <ul style="list-style-type: none"> • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	While in user EXEC mode, enter the enable command.	Switch#	Enter disable to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the configure command.	Switch(config)#	To exit to privileged EXEC mode, enter exit or end , or press Ctrl-Z .	Use this mode to configure parameters that apply to the entire switch.
VLAN configuration	While in global configuration mode, enter the vlan <i>vlan-id</i> command.	Switch(config-vlan)#	To exit to global configuration mode, enter the exit command. To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the switch startup configuration file.
Interface configuration	While in global configuration mode, enter the interface command (with a specific interface).	Switch(config-if)#	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.

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

Using the Help System

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 4	? Example: Switch> ?	Lists all commands available for a particular command mode.
Step 5	<i>command</i> ? Example: Switch> show ?	Lists the associated keywords for a command.
Step 6	<i>command keyword</i> ? Example: Switch(config)# cdp holdtime ? <10-255> Length of time (in sec) that receiver must keep this packet	Lists the associated arguments for a keyword.

Understanding Abbreviated Commands

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

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

```
Switch# show conf
```

No and default Forms of Commands

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

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

CLI Error Messages

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

Table 2: Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: "show con"	You did not enter enough characters for your switch to recognize the command.	Reenter the command followed by a question mark (?) with a 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 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 the commands that are available in this command mode. The possible keywords that you can enter with the command appear.

Configuration Logging

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



Note Only CLI or HTTP changes are logged.

How to Use the CLI to Configure Features

Configuring the Command History

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

Changing the Command History Buffer Size

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	show history Example: Switch# <code>show history</code>	Lists the last several commands that you just entered in privileged EXEC mode. The number of commands that appear is controlled by the setting of the terminal history global configuration command and the history line configuration command.

Disabling the Command History Feature

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

SUMMARY STEPS

1. `terminal no history`

DETAILED STEPS

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

Enabling and Disabling Editing Features

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

SUMMARY STEPS

1. `terminal editing`
2. `terminal no editing`

DETAILED STEPS

	Command or Action	Purpose
Step 1	terminal editing Example: Switch# <code>terminal editing</code>	Reenables the enhanced editing mode for the current terminal session in the privileged EXEC mode.

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

Editing Commands through Keystrokes

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


Note

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

Table 3: Editing Commands

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

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

Editing Command Lines That Wrap

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

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



Note

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

The following example shows how to wrap a command line that extend 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: <code>Switch(config)# access-list 101 permit tcp</code>	Displays the global configuration command entry that extends beyond one line. When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign (\$) shows that the

	Command or Action	Purpose
	<pre>10.15.22.25 255.255.255.0 10.15.22.35 Switch(config)# \$ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25 Switch(config)# \$t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq Switch(config)# \$15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45</pre>	line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.
Step 2	<p>Ctrl-A</p> <p>Example:</p> <pre>Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.25\$</pre>	<p>Checks the complete syntax.</p> <p>The dollar sign (\$) appears at the end of the line to show that the line has been scrolled to the right.</p>
Step 3	Return key	<p>Execute the commands.</p> <p>The software assumes that you have a terminal screen that is 80 columns wide. If you have a different width, use the terminal width privileged EXEC command to set the width of your terminal.</p> <p>Use line wrapping with the command history feature to recall and modify previous complex command entries.</p>

Searching and Filtering Output of show and more Commands

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>{show more} command {begin include exclude} regular-expression</pre> <p>Example:</p> <pre>Switch# show interfaces include protocol Vlan1 is up, line protocol is up Vlan10 is up, line protocol is down GigabitEthernet1/0/1 is up, line protocol is down GigabitEthernet1/0/2 is up, line protocol is up</pre>	<p>Searches and filters the output.</p> <p>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.</p>

Accessing the CLI through a Console Connection or through Telnet

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

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

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

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

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



Layer 2/3 Commands

- [channel-group](#), page 16
- [channel-protocol](#), page 19
- [clear lacp](#), page 21
- [clear pagp](#), page 22
- [clear spanning-tree counters](#), page 23
- [clear spanning-tree detected-protocols](#), page 24
- [debug etherchannel](#), page 25
- [debug lacp](#), page 27
- [debug pagp](#), page 28
- [debug platform etherchannel](#), page 30
- [debug platform pm](#), page 31
- [debug spanning-tree](#), page 34
- [debug platform udd](#), page 36
- [interface port-channel](#), page 37
- [lacp port-priority](#), page 39
- [lacp system-priority](#), page 41
- [link state group](#), page 43
- [link state track](#), page 44
- [pagp learn-method](#), page 45
- [pagp port-priority](#), page 47
- [pagp timer](#), page 49
- [port-channel load-balance](#), page 50
- [show etherchannel](#), page 51
- [show lacp](#), page 54

- [show link state group](#) , page 59
- [show pagp](#), page 60
- [show platform backup interface](#), page 62
- [show platform etherchannel](#), page 63
- [show platform pm](#), page 64
- [show platform spanning-tree](#), page 66
- [show spanning-tree](#), page 67
- [show uddl](#), page 70
- [spanning-tree backbonefast](#), page 73
- [spanning-tree bpdudfilter](#), page 74
- [spanning-tree bpduguard](#), page 76
- [spanning-tree cost](#), page 77
- [spanning-tree etherchannel guard misconfig](#), page 79
- [spanning-tree extend system-id](#), page 80
- [spanning-tree guard](#), page 82
- [spanning-tree link-type](#), page 84
- [spanning-tree loopguard default](#), page 85
- [spanning-tree mode](#), page 86
- [spanning-tree mst configuration](#), page 88
- [spanning-tree mst cost](#), page 90
- [spanning-tree mst forward-time](#), page 91
- [spanning-tree mst hello-time](#), page 92
- [spanning-tree mst max-age](#), page 93
- [spanning-tree mst max-hops](#), page 94
- [spanning-tree mst port-priority](#), page 95
- [spanning-tree mst pre-standard](#), page 96
- [spanning-tree mst priority](#), page 97
- [spanning-tree mst root](#), page 98
- [spanning-tree pathcost method](#), page 100
- [spanning-tree port-priority](#), page 101
- [spanning-tree portfast \(global configuration\)](#), page 102
- [spanning-tree portfast \(interface configuration\)](#), page 104
- [spanning-tree transmit hold-count](#), page 106

- [spanning-tree uplinkfast](#), page 107
- [spanning-tree vlan](#), page 109
- [switchport access vlan](#), page 111
- [switchport mode](#), page 113
- [switchport nonegotiate](#), page 116
- [udld](#), page 118
- [udld port](#), page 120
- [udld reset](#), page 122

channel-group

To assign an Ethernet port to an EtherChannel group, or to enable an EtherChannel mode, or both, use the **channel-group** command in interface configuration mode. To remove an Ethernet port from an EtherChannel group, use the **no** form of this command.

channel-group *channel-group-number* **mode** {**active**| **auto** [**non-silent**]| **desirable** [**non-silent**]| **on**| **passive**}
no channel-group

Syntax Description

<i>channel-group-number</i>	Channel group number. The range is 1 to 48.
mode	Specifies the EtherChannel mode.
active	Unconditionally enables Link Aggregation Control Protocol (LACP).
auto	Enables the Port Aggregation Protocol (PAgP) only if a PAgP device is detected.
non-silent	(Optional) Configures the interface for nonsilent operation when connected to a partner that is PAgP-capable. Use in PAgP mode with the auto or desirable keyword when traffic is expected from the other device.
desirable	Unconditionally enables PAgP.
on	Enables the on mode.
passive	Enables LACP only if a LACP device is detected.

Command Default

No channel groups are assigned.
 No mode is configured.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The IP Lite feature set supports up to 48 EtherChannels.

For Layer 2 EtherChannels, the **channel-group** command automatically creates the port-channel interface when the channel group gets its first physical port. You do not have to use the **interface port-channel** command

in global configuration mode to manually create a port-channel interface. If you create the port-channel interface first, the *channel-group-number* can be the same as the *port-channel-number*, or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.

Although it is not necessary to disable the IP address that is assigned to a physical port that is part of a channel group, we strongly recommend that you do so.

You create Layer 3 port channels by using the **interface port-channel** command followed by the **no switchport** interface configuration command. Manually configure the port-channel logical interface before putting the interface into the channel group.

After you configure an EtherChannel, configuration changes that you make on the port-channel interface apply to all the physical ports assigned to the port-channel interface. Configuration changes applied to the physical port affect only the port where you apply the configuration. To change the parameters of all ports in an EtherChannel, apply configuration commands to the port-channel interface, for example, spanning-tree commands or commands to configure a Layer 2 EtherChannel as a trunk.

Active mode places a port into a negotiating state in which the port initiates negotiations with other ports by sending LACP packets. A channel is formed with another port group in either the active or passive mode.

Auto mode places a port into a passive negotiating state in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. A channel is formed only with another port group in desirable mode. When auto is enabled, silent operation is the default.

Desirable mode places a port into an active negotiating state in which the port starts negotiations with other ports by sending PAgP packets. An EtherChannel is formed with another port group that is in the desirable or auto mode. When desirable is enabled, silent operation is the default.

If you do not specify non-silent with the auto or desirable mode, silent is assumed. The silent mode is used when the switch is connected to a device that is not PAgP-capable and rarely, if ever, sends packets. An example of a silent partner is a file server or a packet analyzer that is not generating traffic. In this case, running PAgP on a physical port prevents that port from ever becoming operational. However, it allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission. Both ends of the link cannot be set to silent.

In on mode, a usable EtherChannel exists only when both connected port groups are in the on mode.

**Caution**

Use care when using the on mode. This is a manual configuration, and ports on both ends of the EtherChannel must have the same configuration. If the group is misconfigured, packet loss or spanning-tree loops can occur.

Passive mode places a port into a negotiating state in which the port responds to received LACP packets but does not initiate LACP packet negotiation. A channel is formed only with another port group in active mode.

Do not configure an EtherChannel in both the PAgP and LACP modes. EtherChannel groups running PAgP and LACP can coexist on the same switch or on different switches in the stack (but not in a cross-stack configuration). Individual EtherChannel groups can run either PAgP or LACP, but they cannot interoperate.

If you set the protocol by using the **channel-protocol** interface configuration command, the setting is not overridden by the **channel-group** interface configuration command.

Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an IEEE 802.1x port. If you try to enable IEEE 802.1x authentication on an EtherChannel port, an error message appears, and IEEE 802.1x authentication is not enabled.

Do not configure a secure port as part of an EtherChannel or configure an EtherChannel port as a secure port.

For a complete list of configuration guidelines, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

**Caution**

Do not enable Layer 3 addresses on the physical EtherChannel ports. Do not assign bridge groups on the physical EtherChannel ports because it creates loops.

Examples

This example shows how to configure an EtherChannel on a single switch in the stack. It assigns two static-access ports in VLAN 10 to channel 5 with the PAgP mode desirable:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable
Switch(config-if-range)# end
```

This example shows how to configure an EtherChannel on a single switch in the stack. It assigns two static-access ports in VLAN 10 to channel 5 with the LACP mode active:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

This example shows how to configure a cross-stack EtherChannel in a switch stack. It uses LACP passive mode and assigns two ports on stack member 2 and one port on stack member 3 as static-access ports in VLAN 10 to channel 5:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/4 -5
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode passive
Switch(config-if-range)# exit
Switch(config)# interface gigabitethernet3/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# channel-group 5 mode passive
Switch(config-if)# exit
```

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

Related Commands

Command	Description
channel-protocol	Restricts the protocol used on a port to manage channeling.
interface port-channel	Accesses or creates a port channel.
show etherchannel	Displays EtherChannel information for a channel.
show lacp	Displays LACP channel-group information.
show pagp	Displays Port Aggregation Protocol (PAgP) channel-group information.

channel-protocol

To restrict the protocol used on a port to manage channeling, use the **channel-protocol** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

channel-protocol {**lacp**|**pagp**}

no channel-protocol

Syntax Description

lacp	Configures an EtherChannel with the Link Aggregation Control Protocol (LACP).
pagp	Configures an EtherChannel with the Port Aggregation Protocol (PAgP).

Command Default

No protocol is assigned to the EtherChannel.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Use the **channel-protocol** command only to restrict a channel to LACP or PAgP. If you set the protocol by using the **channel-protocol** command, the setting is not overridden by the **channel-group** interface configuration command.

You must use the **channel-group** interface configuration command to configure the EtherChannel parameters. The **channel-group** command also can set the mode for the EtherChannel.

You cannot enable both the PAgP and LACP modes on an EtherChannel group.

PAgP and LACP are not compatible; both ends of a channel must use the same protocol.

You cannot configure PAgP on cross-stack configurations.

Examples

This example shows how to specify LACP as the protocol that manages the EtherChannel:

```
Switch(config-if)# channel-protocol lacp
```

You can verify your settings by entering the **show etherchannel** [*channel-group-number*] **protocol** privileged EXEC command.

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group, or enables an EtherChannel mode, or both.
show etherchannel	Displays EtherChannel information for a channel.

clear lacp

To clear Link Aggregation Control Protocol (LACP) channel-group counters, use the **clear lacp** command in privileged EXEC mode.

clear lacp [*channel-group-number*] **counters**

Syntax Description

<i>channel-group-number</i>	(Optional) Channel group number. The range is 1 to 48.
counters	Clears traffic counters.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

You can clear all counters by using the **clear lacp counters** command, or you can clear only the counters for the specified channel group by using the **clear lacp *channel-group-number* counters** command.

Examples

This example shows how to clear all channel-group information:

```
Switch# clear lacp counters
```

This example shows how to clear LACP traffic counters for group 4:

```
Switch# clear lacp 4 counters
```

You can verify that the information was deleted by entering the **show lacp counters** or the **show lacp *channel-group-number* counters** privileged EXEC command.

Related Commands

Command	Description
debug lacp	Enables debugging of LACP.
show lacp	Displays LACP channel-group information.

clear pagp

To clear the Port Aggregation Protocol (PAgP) channel-group information, use the **clear pagp** command in privileged EXEC mode.

clear pagp [*channel-group-number*] **counters**

Syntax Description

<i>channel-group-number</i>	(Optional) Channel group number. The range is 1 to 48.
counters	Clears traffic counters.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

You can clear all counters by using the **clear pagp counters** command, or you can clear only the counters for the specified channel group by using the **clear pagp channel-group-number counters** command.

Examples

This example shows how to clear all channel-group information:

```
Switch# clear pagp counters
```

This example shows how to clear PAgP traffic counters for group 10:

```
Switch# clear pagp 10 counters
```

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

Related Commands

Command	Description
debug pagp	Enables debugging of PAgP.
show pagp	Displays Port Aggregation Protocol (PAgP) channel-group information.

clear spanning-tree counters

To clear the spanning-tree counters, use the **clear spanning-tree counters** command in privileged EXEC mode.

clear spanning-tree counters [**interface** *interface-id*]

Syntax Description	<p>interface <i>interface-id</i></p> <p>(Optional) Clears all spanning-tree counters on the specified interface. Valid interfaces include physical ports, VLANs, and port channels.</p> <p>The VLAN range is 1 to 4094.</p> <p>The port-channel range is 1 to 48.</p>
---------------------------	--

Command Default None

Command Modes Privileged EXEC

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

Usage Guidelines If the *interface-id* value is not specified, spanning-tree counters are cleared for all interfaces.

Examples This example shows how to clear spanning-tree counters for all interfaces:

```
Switch# clear spanning-tree counters
```

clear spanning-tree detected-protocols

To restart the protocol migration process and force renegotiation with neighboring switches on the interface, use the **clear spanning-tree detected-protocols** command in privileged EXEC mode.

clear spanning-tree detected-protocols [**interface** *interface-id*]

Syntax Description

interface <i>interface-id</i>	(Optional) Restarts the protocol migration process on the specified interface. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 48.
--------------------------------------	---

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

A switch running the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol or the Multiple Spanning Tree Protocol (MSTP) supports a built-in protocol migration method that enables it to interoperate with legacy IEEE 802.1D switches. If a rapid-PVST+ or an MSTP switch receives a legacy IEEE 802.1D configuration bridge protocol data unit (BPDU) with the protocol version set to 0, the switch sends only IEEE 802.1D BPDUs on that port. A multiple spanning-tree (MST) switch can also detect that a port is at the boundary of a region when it receives a legacy BPDU, an MST BPDU (Version 3) associated with a different region, or a rapid spanning-tree (RST) BPDU (Version 2).

The switch does not automatically revert to the rapid-PVST+ or the MSTP mode if it no longer receives IEEE 802.1D BPDUs because it cannot learn whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. Use the **clear spanning-tree detected-protocols** command in this situation.

Examples

This example shows how to restart the protocol migration process on a port:

```
Switch# clear spanning-tree detected-protocols interface gigabitethernet2/0/1
```

debug etherchannel

To enable debugging of EtherChannels, use the **debug etherchannel** command in privileged EXEC mode. To disable debugging, use the **no** form of the command.

debug etherchannel[all| detail| error| event| idb]

no debug etherchannel[all| detail| error| event| idb]

Syntax Description

all	(Optional) Displays all EtherChannel debug messages.
detail	(Optional) Displays detailed EtherChannel debug messages.
error	(Optional) Displays EtherChannel error debug messages.
event	(Optional) Displays EtherChannel event messages.
idb	(Optional) Displays PAgP interface descriptor block debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The **undebug etherchannel** command is the same as the **no debug etherchannel** command.



Note

Although the **linecard** keyword is displayed in the command-line help, it is not supported.

When you enable debugging on a stack, it is enabled only on the stack master. To enable debugging on a stack member, start a session from the stack master by using the **session switch-number** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the stack member.

To enable debugging on a stack member without first starting a session on the stack master, use the **remote command switch-number LINE** command in privileged EXEC mode.

Examples

This example shows how to display all EtherChannel debug messages:

```
Switch# debug etherchannel all
```

This example shows how to display debug messages related to EtherChannel events:

```
Switch# debug etherchannel event
```

Related Commands

Command	Description
show etherchannel	Displays EtherChannel information for a channel.

debug lacp

To enable debugging of Link Aggregation Control Protocol (LACP) activity, use the **debug lacp** command in privileged EXEC mode. To disable LACP debugging, use the **no** form of this command.

debug lacp [**all** | **event** | **fsm** | **misc** | **packet**]

no debug lacp [**all** | **event** | **fsm** | **misc** | **packet**]

Syntax Description

all	(Optional) Displays all LACP debug messages.
event	(Optional) Displays LACP event debug messages.
fsm	(Optional) Displays messages about changes within the LACP finite state machine.
misc	(Optional) Displays miscellaneous LACP debug messages.
packet	(Optional) Displays the receiving and transmitting LACP control packets.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The **undebug etherchannel** command is the same as the **no debug etherchannel** command.

When you enable debugging on a stack, it is enabled only on the stack master. To enable debugging on a stack member, start a session from the stack master by using the **session switch-number** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the stack member.

To enable debugging on a stack member without first starting a session on the stack master, use the **remote command switch-number LINE** command in privileged EXEC mode.

Examples

This example shows how to display all LACP debug messages:

```
Switch# debug LACP all
```

This example shows how to display debug messages related to LACP events:

```
Switch# debug LACP event
```

debug pagp

To enable debugging of Port Aggregation Protocol (PAgP) activity, use the **debug pagp** command in privileged EXEC mode. To disable PAgP debugging, use the **no** form of this command.

debug pagp [**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**]

no debug pagp [**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**]

Syntax Description

all	(Optional) Displays all PAgP debug messages.
dual-active	(Optional) Displays dual-active detection messages.
event	(Optional) Displays PAgP event debug messages.
fsm	(Optional) Displays messages about changes within the PAgP finite state machine.
misc	(Optional) Displays miscellaneous PAgP debug messages.
packet	(Optional) Displays the receiving and transmitting PAgP control packets.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The **undebg pagp** command is the same as the **no debug pagp** command.

When you enable debugging on a stack, it is enabled only on the stack master. To enable debugging on a stack member, start a session from the stack master by using the **session switch-number** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the stack member.

To enable debugging on a stack member without first starting a session on the stack master, use the **remote command switch-number LINE** command in privileged EXEC mode.

Examples

This example shows how to display all PAgP debug messages:

```
Switch# debug pagp all
```

This example shows how to display debug messages related to PAgP events:

```
Switch# debug pagp event
```

debug platform etherchannel

To enable debugging of platform-dependent EtherChannel events, use the **debug platform etherchannel** command in EXEC mode. To disable debugging, use the **no** form of this command.

debug platform etherchannel {init| link-up| rpc| warnings}

no debug platform etherchannel {init| link-up| rpc| warnings}

Syntax Description

init	Displays EtherChannel module initialization debug messages.
link-up	Displays EtherChannel link-up and link-down related debug messages.
rpc	Displays EtherChannel remote procedure call (RPC) debug messages.
warnings	Displays EtherChannel warning debug messages.

Command Default

Debugging is disabled.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

The **undebug platform etherchannel** command is the same as the **no debug platform etherchannel** command. When you enable debugging on a stack, it is enabled only on the stack master. To enable debugging on a stack member, start a session from the stack master by using the **session switch-number** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the stack member. To enable debugging on a stack member without first starting a session on the stack master, use the **remote command switch-number LINE** command in privileged EXEC mode.

Examples

This example shows how to display debug messages related to Etherchannel initialization:

```
Switch# debug platform etherchannel init
```

debug platform pm

To enable debugging of the platform-dependent port manager software module, use the **debug platform pm** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug platform pm {all| atom| counters| errdisable| etherchnl| exceptions| gvi| hpm-events| idb-events| if-numbers| ios-events| link-status| platform| pm-events| pm-span| pm-vectors [detail]| rpc [general| oper-info| state| vectors| vp-events]]| soutput-vectors| stack-manager| sync| vlans}

no debug platform pm {all| counters| errdisable| etherchnl| exceptions| hpm-events| idb-events| if-numbers| ios-events| link-status| platform| pm-events| pm-span| pm-vectors [detail]| rpc [general| oper-info| state| vectors| vp-events]]| soutput-vectors| stack-manager| sync| vlans}

Syntax Description

all	Displays all port manager debug messages.
atom	Displays AToM related events.
counters	Displays counters for remote procedure call (RPC) debug messages.
errdisable	Displays error-disabled-related events debug messages.
etherchnl	Displays EtherChannel-related events debug messages.
exceptions	Displays system exception debug messages.
gvi	Displays IPe GVI-related messages.
hpm-events	Displays platform port manager event debug messages.
idb-events	Displays interface descriptor block (IDB)-related events debug messages.
if-numbers	Displays interface-number translation event debug messages.
ios-events	Displays Cisco IOS software events.
link-status	Displays interface link-detection event debug messages.
platform	Displays port manager function event debug messages.
pm-events	Displays port manager event debug messages.
pm-span	Displays port manager Switched Port Analyzer (SPAN) event debug messages.
pm-vectors	Displays port manager vector-related event debug messages.

detail	(Optional) Displays vector-function details.
rpc	Displays RPC-related messages.
general	(Optional) Displays general RPC-related messages.
oper-info	(Optional) Displays operational- and informational-related RPC messages.
state	(Optional) Displays administrative- and operational-related RPC messages.
vectors	(Optional) Displays vector-related RPC messages.
vp-events	(Optional) Displays virtual ports-related RPC messages.
soutput-vectors	Displays IDB output vector event debug messages.
stack-manager	Displays stack manager-related events debug messages. This keyword is supported only on stacking-capable switches.
sync	Displays operational synchronization and VLAN line-state event debug messages.
vlans	Displays VLAN creation and deletion event debug messages.

Command Default Debugging is disabled

Command Modes Privileged EXEC

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

Usage Guidelines

The **undebbug platform pm** command is the same as the **no debug platform pm** command.

When you enable debugging on a stack, it is enabled only on the stack master. To enable debugging on a stack member, start a session from the stack master by using the **session switch-number** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the stack member.

To enable debugging on a stack member without first starting a session on the stack master, use the **remote command switch-number LINE** command in privileged EXEC mode.

Examples

This example shows how to display debug messages related to the creation and deletion of VLANs:

```
Switch# debug platform pm vlans
```

Related Commands

Command	Description
show platform pm	Displays platform-dependent port manager information.

debug spanning-tree

To enable debugging of spanning-tree activities, use the **debug spanning-tree** command in EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree {all | backbonefast | bpdu | bpdu-opt | config | csuf/csrt | etherchannel | events | exceptions | general | mstp | pvst+ | root | snmp | synchronization | switch | uplinkfast}

no debug spanning-tree {all | backbonefast | bpdu | bpdu-opt | config | csuf/csrt | etherchannel | events | exceptions | general | mstp | pvst+ | root | snmp | synchronization | switch | uplinkfast}

Syntax Description

all	Displays all spanning-tree debug messages.
backbonefast	Displays BackboneFast-event debug messages.
bpdu	Displays spanning-tree bridge protocol data unit (BPDU) debug messages.
bpdu-opt	Displays optimized BPDU handling debug messages.
config	Displays spanning-tree configuration change debug messages.
csuf/csrt	Displays cross-stack UplinkFast and cross-stack rapid transition activity debug messages.
etherchannel	Displays EtherChannel-support debug messages.
events	Displays spanning-tree topology event debug messages.
exceptions	Displays spanning-tree exception debug messages.
general	Displays general spanning-tree activity debug messages.
mstp	Debugs Multiple Spanning Tree Protocol (MSTP) events.
pvst+	Displays per-VLAN spanning-tree plus (PVST+) event debug messages.
root	Displays spanning-tree root-event debug messages.
snmp	Displays spanning-tree Simple Network Management Protocol (SNMP) handling debug messages.
switch	Displays switch shim command debug messages. This shim is the software module that is the interface between the generic Spanning Tree Protocol (STP) code and the platform-specific code of various switch platforms.

synchronization	Displays the spanning-tree synchronization event debug messages.
uplinkfast	Displays UplinkFast-event debug messages.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

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

Usage Guidelines The **undebg spanning-tree** command is the same as the **no debug spanning-tree** command.

When you enable debugging on a stack, it is enabled only on the stack master. To enable debugging on a stack member, start a session from the stack master by using the **session switch-number** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the stack member.

To enable debugging on a stack member without first starting a session on the stack master, use the **remote command switch-number LINE** command in privileged EXEC mode.

Examples This example shows how to display all spanning-tree debug messages:

```
Switch# debug spanning-tree all
```

debug platform udd

To enable debugging of the platform-dependent UniDirectional Link Detection (UDLD) software, use the **debug platform udd** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug platform udd [**all** | **error** | **switch** | **rpc** {**events** | **messages**}]

no platform udd [**all** | **error** | **rpc** {**events** | **messages**}]

Syntax Description

all	(Optional) Displays all UDLD debug messages.
error	(Optional) Displays error condition debug messages.
rpc { events messages }	(Optional) Displays UDLD remote procedure call (RPC) debug messages. The keywords have these meanings: <ul style="list-style-type: none"> • events—Displays UDLD RPC events. • messages—Displays UDLD RPC messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The **undebg platform udd** command is the same as the **no debug platform udd** command.

When you enable debugging on a stack, it is enabled only on the stack master. To enable debugging on a stack member, start a session from the stack master by using the **session** *switch-number* command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the stack member.

To enable debugging on a stack member without first starting a session on the stack master, use the **remote command** *switch-number* *LINE* command in privileged EXEC mode.

interface port-channel

To access or create a port channel, use the **interface port-channel** command in global configuration mode. Use the **no** form of this command to remove the port channel.

interface port-channel *port-channel-number*

no interface port-channel

Syntax Description

port-channel-number (Optional) Channel group number. The range is 1 to 48.

Command Default

No port channel logical interfaces are defined.

Command Modes

Global configuration

Command History

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

Usage Guidelines

For Layer 2 EtherChannels, you do not have to create a port-channel interface before assigning physical ports to a channel group. Instead, you can use the **channel-group** interface configuration command, which automatically creates the port-channel interface when the channel group obtains its first physical port. If you create the port-channel interface first, the *channel-group-number* can be the same as the *port-channel-number*, or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.

You create Layer 3 port channels by using the **interface port-channel** command followed by the **no switchport** interface configuration command. You should manually configure the port-channel logical interface before putting the interface into the channel group.

Only one port channel in a channel group is allowed.



Caution

When using a port-channel interface as a routed port, do not assign Layer 3 addresses on the physical ports that are assigned to the channel group.



Caution

Do not assign bridge groups on the physical ports in a channel group used as a Layer 3 port channel interface because it creates loops. You must also disable spanning tree.

Follow these guidelines when you use the **interface port-channel** command:

- If you want to use the Cisco Discovery Protocol (CDP), you must configure it on the physical port and not on the port channel interface.
- Do not configure a port that is an active member of an EtherChannel as an IEEE 802.1x port. If IEEE 802.1x is enabled on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.

For a complete list of configuration guidelines, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

Examples

This example shows how to create a port channel interface with a port channel number of 5:

```
Switch(config)# interface port-channel 5
```

You can verify your setting by entering the **show running-config** privileged EXEC or **show etherchannel channel-group-number detail** privileged EXEC command.

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group, or enables an EtherChannel mode, or both.
show etherchannel	Displays EtherChannel information for a channel.

lacp port-priority

To configure the port priority for the Link Aggregation Control Protocol (LACP), use the **lacp port-priority** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

lacp port-priority *priority*

no lacp port-priority

Syntax Description

<i>priority</i>	Port priority for LACP. The range is 1 to 65535.
-----------------	--

Command Default

The default is 32768.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The **lacp port-priority** interface configuration command determines which ports are bundled and which ports are put in hot-standby mode when there are more than eight ports in an LACP channel group.

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.

In port-priority comparisons, a numerically lower value has a higher priority: When there are more than eight ports in an LACP channel group, the eight ports with the numerically lowest values (highest priority values) for LACP port priority are bundled into the channel group, and the lower-priority ports are put in hot-standby mode. If two or more ports have the same LACP port priority (for example, they are configured with the default setting of 65535), then an internal value for the port number determines the priority.



Note

The LACP port priorities are only effective if the ports are on the switch that controls the LACP link. See the **lacp system-priority** global configuration command for determining which switch controls the link.

Use the **show lacp internal** privileged EXEC command to display LACP port priorities and internal port number values.

For information about configuring LACP on physical ports, see the configuration guide for this release.

Examples

This example shows how to configure the LACP port priority on a port:

```
Switch# interface gigabitethernet2/0/1
Switch(config-if)# lacp port-priority 1000
```

You can verify your settings by entering the **show lacp** [*channel-group-number*] **internal** privileged EXEC command.

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group, or enables an EtherChannel mode, or both.
lacp system-priority	Configures the LACP system priority.
show lacp	Displays LACP channel-group information.

lACP system-priority

To configure the system priority for the Link Aggregation Control Protocol (LACP), use the **lACP system-priority** command in global configuration mode on the switch. To return to the default setting, use the **no** form of this command.

lACP system-priority *priority*

no lACP system-priority

Syntax Description

<i>priority</i>	System priority for LACP. The range is 1 to 65535.
-----------------	--

Command Default

The default is 32768.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **lACP system-priority** command determines which switch in an LACP link controls port priorities.

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode. When there are more than eight ports in an LACP channel group, the switch on the controlling end of the link uses port priorities to determine which ports are bundled into the channel and which ports are put in hot-standby mode. Port priorities on the other switch (the noncontrolling end of the link) are ignored.

In priority comparisons, numerically lower values have a higher priority. Therefore, the system with the numerically lower value (higher priority value) for LACP system priority becomes the controlling system. If both switches have the same LACP system priority (for example, they are both configured with the default setting of 32768), the LACP system ID (the switch MAC address) determines which switch is in control.

The **lACP system-priority** command applies to all LACP EtherChannels on the switch.

Use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag in the output display).

Examples

This example shows how to set the LACP system priority:

```
Switch(config)# lACP system-priority 20000
```

You can verify your settings by entering the **show lACP sys-id** privileged EXEC command.

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group, or enables an EtherChannel mode, or both.
lacp port-priority	Configures the port priority for the Link Aggregation Control Protocol (LACP).
show lacp	Displays LACP channel-group information.

link state group

To configure an interface as a member of a link-state group, use the **link state group** command in interface configuration mode. Use the **no** form of this command to remove an interface from a link-state group.

```
link state group [number]{downstream|upstream}
```

```
no link state group [number]{downstream|upstream}
```

Syntax Description

<i>number</i>	(Optional) Specifies the number of the link-state group. The range is 1 to 2. The default group number is 1.
downstream	Configures the interface as a downstream interface in the group.
upstream	Configures the interface as an upstream interface in the group.

Command Default

No link-state group is configured.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Add upstream interfaces to the link-state group before adding downstream interfaces, otherwise, the downstream interfaces move into error-disable mode. These are the limitations:

- An interface can be an upstream interface or a downstream interface.
- An interface can belong to only one link-state group.
- Only two link-state groups can be configured on a switch.

Examples

This example shows how to configure the interfaces as upstream in group 2:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# link state group 2 upstream
Switch(config-if-range)# end
```

link state track

To enable a link-state group, use the **link state track** command in global configuration mode. Use the **no** form of this command to disable a link-state group.

link state track [*number*]

no link state track [*number*]

Syntax Description

<i>number</i>	(Optional) Specifies the number of the link-state group. The range is 1 to 2. The default is 1.
---------------	---

Command Default

Link-state tracking is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **link state group** command to create and configure the link-state group. You then can use this command to enable the link-state group.

Examples

This example shows how to enable link-state group 2:

```
Switch# configure terminal
Switch(config)# link state track 2
Switch(config)# end
```

pagp learn-method

To learn the source address of incoming packets received from an EtherChannel port, use the **pagp learn-method** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

pagp learn-method {aggregation-port| physical-port}

no pagp learn-method

Syntax Description

aggregation-port	Specifies address learning on the logical port channel. The switch sends packets to the source using any port in the EtherChannel. This setting is the default. With aggregation-port learning, it is not important on which physical port the packet arrives.
physical-port	Specifies address learning on the physical port within the EtherChannel. The switch sends packets to the source using the same port in the EtherChannel from which it learned the source address. The other end of the channel uses the same port in the channel for a particular destination MAC or IP address.

Command Default

The default is aggregation-port (logical port channel).

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The learn method must be configured the same at both ends of the link.

The switch supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the switch hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports.

When the link partner to the switch is a physical learner, we recommend that you configure the switch as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command. We also recommend that you set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. Use the **pagp learn-method** interface configuration command only in this situation.

Examples

This example shows how to set the learning method to learn the address on the physical port within the EtherChannel:

```
Switch(config-if)# pagp learn-method physical-port
```

This example shows how to set the learning method to learn the address on the port channel within the EtherChannel:

```
Switch(config-if)# pagp learn-method aggregation-port
```

You can verify your settings by entering the **show running-config** privileged EXEC command or the **show pagp channel-group-number internal** privileged EXEC command.

Related Commands

Command	Description
pagp port-priority	Selects a port over which all traffic through the EtherChannel is sent.
show pagp	Displays Port Aggregation Protocol (PAgP) channel-group information.

pagp port-priority

To select a port over which all Port Aggregation Protocol (PAgP) traffic through the EtherChannel is sent, use the **pagp port-priority** command in interface configuration mode. If all unused ports in the EtherChannel are in hot-standby mode, they can be placed into operation if the currently selected port and link fails. To return to the default setting, use the **no** form of this command.

pagp port-priority *priority*

no pagp port-priority

Syntax Description

<i>priority</i>	Priority number. The range is from 0 to 255.
-----------------	--

Command Default

The default is 128.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The physical port with the highest priority that is operational and has membership in the same EtherChannel is the one selected for PAgP transmission.

The switch supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the switch hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports, such as the Catalyst 1900 switch.

When the link partner to the switch is a physical learner, we recommend that you configure the switch as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command. We also recommend that you set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. Use the **pagp learn-method** interface configuration command only in this situation.

Examples

This example shows how to set the port priority to 200:

```
Switch(config-if)# pagp port-priority 200
```

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show pagp channel-group-number internal** privileged EXEC command.

Related Commands

Command	Description
pagp learn-method	Provides the ability to learn the source address of incoming packets.
port-channel load-balance	Sets the load-distribution method among the ports in the EtherChannel.
show pagp	Displays Port Aggregation Protocol (PAgP) channel-group information.

pagp timer

To set the PAgP timer expiration, use the **pagp timer** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

pagp timer *time*

no pagp timer

Syntax Description	<i>time</i>	Specifies the number of seconds after which PAgP informational packets are timed-out. The range is 45 to 90.
---------------------------	-------------	--

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

Command Modes	Interface configuration
----------------------	-------------------------

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

Usage Guidelines	This command is available for all interfaces configured as part of a PAgP port channel.
-------------------------	---

Examples This example shows how to set the PAgP timer expiration to 50 seconds:

```
Switch(config-if)# pagp timer 50
```

port-channel load-balance

To set the load-distribution method among the ports in the EtherChannel, use the **port-channel load-balance** command in global configuration mode. To reset the load-balancing function to the default setting, use the **no** form of this command.

```
port-channel load-balance {dst-ip|dst-mac|src-dst-ip|src-dst-mac|src-ip|src-mac}
no port-channel load-balance
```

Syntax Description

dst-ip	Specifies load distribution based on the destination host IP address.
dst-mac	Specifies load distribution based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel.
src-dst-ip	Specifies load distribution based on the source and destination host IP address.
src-dst-mac	Specifies load distribution based on the source and destination host MAC address.
src-ip	Specifies load distribution based on the source host IP address.
src-mac	Specifies load distribution based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.

Command Default

The default is **src-mac**.

Command Modes

Global configuration

Command History

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

Usage Guidelines

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show etherchannel load-balance** privileged EXEC command.

Examples

This example shows how to set the load-distribution method to **dst-mac**:

```
Switch(config)# port-channel load-balance dst-mac
```

show etherchannel

To display EtherChannel information for a channel, use the **show etherchannel** command in user EXEC mode.

```
show etherchannel [channel-group-number | {detail | port | port-channel | protocol | summary } ] | [detail | port | port-channel | protocol | summary]
```

Syntax Description

<i>channel-group-number</i>	(Optional) Channel group number. The range is 1 to 48.
detail	Displays detailed EtherChannel information.
port	Displays EtherChannel port information.
port-channel	Displays port-channel information.
protocol	Displays the protocol that is being used in the channel.
summary	Displays a one-line summary per channel group.
load-balance	(Optional) Displays the load-balance or frame-distribution scheme among ports in the port channel.

Command Default

None

Command Modes

User EXEC

Command History

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

Usage Guidelines

If you do not specify a channel group number, all channel groups are displayed.

In the output, the passive port list field is displayed only for Layer 3 port channels. This field means that the physical port, which is still not up, is configured to be in the channel group (and indirectly is in the only port channel in the channel group).

Examples

This is an example of output from the **show etherchannel *channel-group-number* detail** command:

```
Switch> show etherchannel 1 detail
Group state = L2
Ports: 2   Maxports = 16
Port-channels: 1 Max Port-channels = 16
```

show etherchannel

```

Protocol:          LACP
                  Ports in the group:
                  -----
Port: Gi1/0/1
-----
Port state        = Up Mstr In-Bndl
Channel group    = 1          Mode = Active          Gcchange = -
Port-channel     =           PolGC = -             Pseudo port-channel = Po1
Port index       =           0Load = 0x00          Protocol = LACP

Flags: S - Device is sending Slow LACPDU      F - Device is sending fast LACPDU
      A - Device is in active mode.           P - Device is in passive mode.

Local information:

Port   Flags   State   LACP port   Admin   Oper   Port   Port
      SA     bndl   Priority    Key     Key   Number State
Gi1/0/1 SA     bndl   32768      0x1     0x1   0x101 0x3D
Gi1/0/2 A      bndl   32768      0x0     0x1   0x0   0x3D

Age of the port in the current state: 01d:20h:06m:04s

                  Port-channels in the group:
                  -----

Port-channel: Po1 (Primary Aggregator)

Age of the Port-channel = 01d:20h:20m:26s
Logical slot/port = 10/1          Number of ports = 2
HotStandBy port   = null
Port state        = Port-channel Ag-Inuse
Protocol          = LACP

Ports in the Port-channel:

Index  Load  Port      EC state      No of bits
-----+-----+-----+-----+-----
  0     00   Gi1/0/1   Active        0
  0     00   Gi1/0/2   Active        0

Time since last port bundled: 01d:20h:24m:44s Gi1/0/2

```

This is an example of output from the **show etherchannel channel-group-number summary** command:

```

Switch> show etherchannel 1 summary
Flags: D - down P - in port-channel
      I - stand-alone s - suspended
      H - Hot-standby (LACP only)
      R - Layer3 S - Layer2
      u - unsuitable for bundling
      U - in use f - failed to allocate aggregator
      d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

```

```

Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
  1     Po1(SU)     LACP      Gi1/0/1(P) Gi1/0/2(P)

```

This is an example of output from the **show etherchannel channel-group-number port-channel** command:

```

Switch> show etherchannel 1 port-channel
Port-channels in the group:
-----
Port-channel: Po1 (Primary Aggregator)
-----
Age of the Port-channel = 01d:20h:24m:50s
Logical slot/port = 10/1 Number of ports = 2
Logical slot/port = 10/1 Number of ports = 2
Port state = Port-channel Ag-Inuse
Protocol = LACP

Ports in the Port-channel:

```

```

Index  Load  Port  EC state  No of bits
-----+-----+-----+-----+-----
0      00   Gi1/0/1 Active      0
0      00   Gi1/0/2 Active      0

```

Time since last port bundled: 01d:20h:24m:44s Gi1/0/2

This is an example of output from **show etherchannel protocol** command:

```

Switch# show etherchannel protocol
Channel-group listing:
-----
Group: 1
-----
Protocol: LACP
Group: 2
-----
Protocol: PAgP

```

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group, or enables an EtherChannel mode, or both.
channel-protocol	Restricts the protocol used on a port to manage channeling.
interface port-channel	Accesses or creates a port channel.

show lacp

To display Link Aggregation Control Protocol (LACP) channel-group information, use the **show lacp** command in user EXEC mode.

show lacp [*channel-group-number*] {**counters**| **internal**| **neighbor**| **sys-id**}

Syntax Description

<i>channel-group-number</i>	(Optional) Channel group number. The range is 1 to 48.
counters	Displays traffic information.
internal	Displays internal information.
neighbor	Displays neighbor information.
sys-id	Displays the system identifier that is being used by LACP. The system identifier consists of the LACP system priority and the switch MAC address.

Command Default

None

Command Modes

User EXEC

Command History

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

Usage Guidelines

You can enter any **show lacp** command to display the active channel-group information. To display specific channel information, enter the **show lacp** command with a channel-group number.

If you do not specify a channel group, information for all channel groups appears.

You can enter the *channel-group-number* to specify a channel group for all keywords except **sys-id**.

Examples

This is an example of output from the **show lacp counters** user EXEC command. The table that follows describes the fields in the display.

```
Switch> show lacp counters
          LACPDU      Marker      Marker Response  LACPDU
Port      Sent  Recv      Sent  Recv      Sent  Recv      Pkts  Err
-----
Channel group:1
Gi2/0/1      19   10           0    0           0    0         0
Gi2/0/2      14    6           0    0           0    0         0
```

Table 4: show lacp counters Field Descriptions

Field	Description
LACPDUs Sent and Recv	The number of LACP packets sent and received by a port.
Marker Sent and Recv	The number of LACP marker packets sent and received by a port.
Marker Response Sent and Recv	The number of LACP marker response packets sent and received by a port.
LACPDUs Pkts and Err	The number of unknown and illegal packets received by LACP for a port.

This is an example of output from the **show lacp internal** command:

```
Switch> show lacp 1 internal
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode           P - Device is in Passive mode

Channel group 1
Port      Flags   State   LACP port  Admin   Oper   Port   Port
Gi2/0/1   SA      bndl    32768      0x3     0x3    0x4    0x3D
Gi2/0/2   SA      bndl    32768      0x3     0x3    0x5    0x3D
```

The following table describes the fields in the display:

Table 5: show lacp internal Field Descriptions

Field	Description
State	<p>State of the specific port. These are the allowed values:</p> <ul style="list-style-type: none"> • --—Port is in an unknown state. • bndl—Port is attached to an aggregator and bundled with other ports. • susp—Port is in a suspended state; it is not attached to any aggregator. • hot-sby—Port is in a hot-standby state. • indiv—Port is incapable of bundling with any other port. • indep—Port is in an independent state (not bundled but able to handle data traffic. In this case, LACP is not running on the partner port). • down—Port is down.
LACP Port Priority	Port priority setting. LACP uses the port priority to put ports in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.
Admin Key	Administrative key assigned to this port. LACP automatically generates an administrative key value as a hexadecimal number. The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by the port physical characteristics (for example, data rate and duplex capability) and configuration restrictions that you establish.
Oper Key	Runtime operational key that is being used by this port. LACP automatically generates this value as a hexadecimal number.
Port Number	Port number.

Field	Description
Port State	<p>State variables for the port, encoded as individual bits within a single octet with these meanings:</p> <ul style="list-style-type: none"> • bit0: LACP_Activity • bit1: LACP_Timeout • bit2: Aggregation • bit3: Synchronization • bit4: Collecting • bit5: Distributing • bit6: Defaulted • bit7: Expired <p>Note In the list above, bit7 is the MSB and bit0 is the LSB.</p>

This is an example of output from the **show lacp neighbor** command:

```
Switch> show lacp neighbor
Flags: S - Device is sending Slow LACPDUs  F - Device is sending Fast LACPDUs
      A - Device is in Active mode          P - Device is in Passive mode
```

Channel group 3 neighbors

Partner's information:

Port	Partner System ID	Partner Port Number	Age	Partner Flags
Gi2/0/1	32768,0007.eb49.5e80	0xC	19s	SP
	LACP Partner Port Priority	Partner Oper Key	Partner Port State	
	32768	0x3	0x3C	

Partner's information:

Port	Partner System ID	Partner Port Number	Age	Partner Flags
Gi2/0/2	32768,0007.eb49.5e80	0xD	15s	SP
	LACP Partner Port Priority	Partner Oper Key	Partner Port State	
	32768	0x3	0x3C	

This is an example of output from the **show lacp sys-id** command:

```
Switch> show lacp sys-id
32765,0002.4b29.3a00
```

The system identification is made up of the system priority and the system MAC address. The first two bytes are the system priority, and the last six bytes are the globally administered individual MAC address associated to the system.

Related Commands

Command	Description
clear lacp	Clears the LACP channel-group information.
debug lacp	Enables debugging of LACP.
lacp port-priority	Configures the port priority for the Link Aggregation Control Protocol (LACP).
lacp system-priority	Configures the LACP system priority.

show link state group

To display link-state group information, use the **show link state group** command in privileged EXEC mode.

show link state group [*number*][*detail*]

Syntax Description	
<i>number</i>	(Optional) Specifies the number of the link-state group number. The range is 1 to 2.
detail	(Optional) Displays detailed information about the link-state group.

Command Default None

Command Modes Privileged EXEC

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

Usage Guidelines

To display information about all link-state groups, enter this command without keywords. To display information about a specific link-state group enter the link-state group number.

The output for the **show link state group detail** displays information for only those link-state groups that have link-state tracking enabled or that have upstream or downstream interfaces configured. If the group does not have a configuration, the group is not shown as enabled or disabled.

Examples This example shows the output from the **show link state group number** command:

```
Switch# show link state group 1
Link State Group: 1      Status: Enabled. Down
```

This example shows the output from the **show link state group detail** command:

```
Switch# show link state group detail
(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Gil/0/15(Dwn) Gil/0/16(Dwn)
Downstream Interfaces : Gil/0/11(Dis) Gil/0/12(Dis) Gil/0/13(Dis) Gil/0/14(Dis)
Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Gil/0/15(Dwn) Gil/0/16(Dwn) Gil/0/17(Dwn)
Downstream Interfaces : Gil/0/11(Dis) Gil/0/12(Dis) Gil/0/13(Dis) Gil/0/14(Dis)
(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

show pagp

To display Port Aggregation Protocol (PAgP) channel-group information, use the **show pagp** command in EXEC mode.

show pagp [*channel-group-number*] {**counters**| **dual-active**| **internal**| **neighbor**}

Syntax Description

<i>channel-group-number</i>	(Optional) Channel group number. The range is 1 to 48.
counters	Displays traffic information.
dual-active	Displays the dual-active status.
internal	Displays internal information.
neighbor	Displays neighbor information.

Command Default

None

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

You can enter any **show pagp** command to display the active channel-group information. To display the nonactive information, enter the **show pagp** command with a channel-group number.

Examples

This is an example of output from the **show pagp 1 counters** command:

```
Switch> show pagp 1 counters
          Information          Flush
Port      Sent   Recv      Sent   Recv
-----
Channel group: 1
  Gi1/0/1   45    42         0     0
  Gi1/0/2   45    41         0     0
```

This is an example of output from the **show pagp dual-active** command:

```
Switch> show pagp dual-active
PAgP dual-active detection enabled: Yes
PAgP dual-active version: 1.1
```

```

Channel group 1
  Dual-Active   Partner
Port           Detect Capable Name      Partner   Partner
              Name      Port     Port     Version
Gi1/0/1       No          Switch   Gi3/0/3   N/A
Gi1/0/2       No          Switch   Gi3/0/4   N/A

```

<output truncated>

This is an example of output from the **show pagp 1 internal** command:

```

Switch> show pagp 1 internal
Flags: S - Device is sending Slow hello.  C - Device is in Consistent state.
       A - Device is in Auto mode.
Timers: H - Hello timer is running.       Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

```

```

Channel group 1
Port      Flags State  Timers  Hello  Partner  PAgP    Learning  Group
          Count Priority Method Ifindex
Gi1/0/1   SC   U6/S7  H       30s    1        128     Any       16
Gi1/0/2   SC   U6/S7  H       30s    1        128     Any       16

```

This is an example of output from the **show pagp 1 neighbor** command:

```

Switch> show pagp 1 neighbor

Flags: S - Device is sending Slow hello.  C - Device is in Consistent state.
       A - Device is in Auto mode.       P - Device learns on physical port.

Channel group 1 neighbors
Port      Partner
          Name      Device ID      Partner  Partner  Age  Flags  Group
          Name      Device ID      Port     Port     Age  Flags  Cap.
Gi1/0/1   switch-p2  0002.4b29.4600  Gi01//1  9s  SC    10001
Gi1/0/2   switch-p2  0002.4b29.4600  Gi1/0/2  24s SC    10001

```

Related Commands

Command	Description
clear pagp	Clears PAgP channel-group information.
debug pagp	Enables debugging of PAgP.

show platform backup interface

To display platform-dependent backup information used in a Flex Links configuration, use the **show platform backup interface** privileged EXEC command.

show platform backup interface [*interface-id* | **dummyQ**]

Syntax Description

<i>interface-id</i>	(Optional) Backup information for all interfaces or the specified interface. The interface can be a physical interface or a port channel.
dummyQ	(Optional) Displays dummy queue information.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use this command only when you are working directly with a technical support representative while troubleshooting a problem.

Do not use this command unless a technical support representative asks you to do so.

show platform etherchannel

To display platform-dependent EtherChannel information, use the **show platform etherchannel** command in privileged EXEC mode.

show platform etherchannel {**data-structures**|**flags**|**time-stamps**}

Syntax Description

data-structures	Displays EtherChannel data structures.
flags	Displays EtherChannel port flags.
time-stamps	Displays EtherChannel time stamps.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use this command only when you are working directly with a technical support representative while troubleshooting a problem.

Do not use this command unless a technical support representative asks you to do so.

show platform pm

To display platform-dependent port manager information, use the **show platform pm** command in privileged EXEC mode.

```
show platform pm {counters| group-masks| idbs {active-idbs| deleted-idbs}| if-numbers| link-status|
module-info| platform-block| port-info interface-id| stack-view| vlan {info| line-state}}
```

Syntax Description

counters	Displays module counters information.
group-masks	Displays EtherChannel group masks information.
idbs {active-idbs deleted-idbs}	Displays interface data block (IDB) information. The keywords have these meanings: <ul style="list-style-type: none"> • active-idbs—Displays active IDB information. • deleted-idbs—Displays deleted and leaked IDB information.
if-numbers	Displays interface numbers information.
link-status	Displays local port link status information.
module-info	Displays module status information.
platform-block	Displays platform port block information.
port-info <i>interface-id</i>	Displays port administrative and operation fields for the specified interface.
stack-view	Displays status information for the stack.

vlan {info | line-state}

Displays platform VLAN information. The keywords have these meanings:

- **info**—Displays information for active VLANs.
 - **line-state**—Displays line-state information.
-

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use this command only when you are working directly with your technical support representative while troubleshooting a problem.

Do not use this command unless your technical support representative asks you to do so.

Related Commands

Command	Description
debug platform pm	Enables debugging of the platform-dependent port manager software module.

show platform spanning-tree

To display platform-dependent spanning-tree information, use the **show platform spanning-tree** privileged EXEC command.

show platform spanning-tree synchronization [**detail** | **vlan** *vlan-id*]

Syntax Description

synchronization	Displays spanning-tree state synchronization information.
detail	(Optional) Displays detailed spanning-tree information.
vlan <i>vlan-id</i>	(Optional) Displays VLAN switch spanning-tree information for the specified VLAN. The range is 1 to 4094.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use this command only when you are working directly with your technical support representative while troubleshooting a problem.

Do not use this command unless your technical support representative asks you to do so.

show spanning-tree

To display spanning-tree information for the specified spanning-tree instances, use the **show spanning-tree** command in privileged EXEC mode or user EXEC mode.

show spanning-tree [**active**| **backbonefast**| **blockedports**| **bridge**| **detail**| **inconsistentports**| **interface** *interface-type interface-number*| **mst**| **pathcost**| **root**| **summary** [**totals**]| **uplinkfast**| **vlan** *vlan-id*]

Syntax Description

active	(Optional) Displays spanning-tree information on active interfaces only.
backbonefast	(Optional) Displays spanning-tree BackboneFast status.
blockedports	(Optional) Displays blocked port information.
bridge	(Optional) Displays status and configuration of this switch.
detail	(Optional) Displays detailed information.
inconsistentports	(Optional) Displays information about inconsistent ports.
interface <i>interface-type interface-number</i>	(Optional) Specifies the type and number of the interface.
mst	(Optional) Specifies multiple spanning-tree.
pathcost	(Optional) Displays spanning-tree pathcost options.
root	(Optional) Displays root-switch status and configuration.
summary	(Optional) Specifies a summary of port states.
totals	(Optional) Displays the total lines of the spanning-tree state section.
uplinkfast	(Optional) Displays spanning-tree UplinkFast status.
vlan <i>vlan-id</i>	(Optional) Specifies the VLAN ID. The range is 1 to 4094.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

If you do not specify a *vlan-id* value when you use the **vlan** keyword, the command applies to spanning-tree instances for all VLANs.

Examples

This is an example of output from the **show spanning-tree active** command:

```
Switch# show spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID      Priority    32768
              Address     0001.42e2.cdd0
              Cost       3038
              Port       24 (GigabitEthernet2/0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID    Priority    49153 (priority 49152 sys-id-ext 1)
              Address     0003.fd63.9580
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300
  Uplinkfast   enabled

Interface      Role Sts Cost      Prio.Nbr Type
-----
Gi2/0/1        Root FWD 3019      128.24  P2p
Gi0/1          Root FWD 3019      128.24  P2p
<output truncated>
```

This is an example of output from the **show spanning-tree detail** command:

```
Switch# show spanning-tree detail
Bridge Identifier has priority 49152, sysid 1, address 0003.fd63.9580
Configured hello time 2, max age 20, forward delay 15
Current root has priority 32768, address 0001.42e2.cdd0
Root port is 1 (GigabitEthernet2/0/1), cost of root path is 3038
Topology change flag not set, detected flag not set
Number of topology changes 0 last change occurred 1d16h ago
Times: hold 1, topology change 35, notification 2
      hello 2, max age 20, forward delay 15
Timers: hello 0, topology change 0, notification 0, aging 300
Uplinkfast enabled

Port 1 (GigabitEthernet2/0/1) of VLAN0001 is forwarding
Port path cost 3019, Port priority 128, Port Identifier 128.24.
Designated root has priority 32768, address 0001.42e2.cdd0
Designated bridge has priority 32768, address 00d0.bbf5.c680
Designated port id is 128.25, designated path cost 19
Timers: message age 2, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDUs: sent 0, received 72364

<output truncated>
```

This is an example of output from the **show spanning-tree summary** command:

```
Switch# show spanning-tree interface mst configuration
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfiguration guard is enabled
Extended system ID is enabled
Portfast is disabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard is disabled by default
UplinkFast is enabled
```

```

BackboneFast          is enabled
Pathcost method used is short

Name                  Blocking Listening Learning Forwarding STP Active
-----
VLAN0001              1           0           0           11          12
VLAN0002              3           0           0           1           4
VLAN0004              3           0           0           1           4
VLAN0006              3           0           0           1           4
VLAN0031              3           0           0           1           4
VLAN0032              3           0           0           1           4
<output truncated>
-----
37 vlans              109         0           0           47          156
Station update rate set to 150 packets/sec.

UplinkFast statistics
-----
Number of transitions via uplinkFast (all VLANs)      : 0
Number of proxy multicast addresses transmitted (all VLANs) : 0

BackboneFast statistics
-----
Number of transition via backboneFast (all VLANs)    : 0
Number of inferior BPDUs received (all VLANs)       : 0
Number of RLQ request PDUs received (all VLANs)     : 0
Number of RLQ response PDUs received (all VLANs)    : 0
Number of RLQ request PDUs sent (all VLANs)         : 0
Number of RLQ response PDUs sent (all VLANs)        : 0

```

This is an example of output from the **show spanning-tree mst configuration** command:

```

Switch# show spanning-tree interface mst configuration
Name [region1]
Revision 1
Instance Vlans Mapped
-----
0        1-9,21-4094
1        10-20
-----

```

This is an example of output from the **show spanning-tree interface mst interface interface-id** command:

```

Switch# show spanning-tree interface mst configuration
GigabitEthernet2/0/1 of MST00 is root forwarding
Edge port: no (default) port guard : none (default)
Link type: point-to-point (auto) bpdu filter: disable (default)
Boundary : boundary (STP) bpdu guard : disable (default)
Bpdus sent 5, received 74

Instance role state cost prio vlans mapped
0        root FWD 200000 128 1,12,14-4094

```

This is an example of output from the **show spanning-tree interface mst instance-id** command:

```

Switch# show spanning-tree interface mst 0
GigabitEthernet2/0/1 of MST00 is root forwarding
Edge port: no (default) port guard : none (default)
Link type: point-to-point (auto) bpdu filter: disable (default)
Boundary : boundary (STP) bpdu guard : disable (default)
Bpdus sent 5, received 74

Instance role state cost prio vlans mapped
0        root FWD 200000 128 1,12,14-4094

```

show uddl

To display UniDirectional Link Detection (UDLD) administrative and operational status for all ports or the specified port, use the **show uddl** command in user EXEC mode.

show uddl [*interface_id*] **neighbors**

Syntax Description

<i>interface-id</i>	(Optional) ID of the interface and port number. Valid interfaces include physical ports, VLANs, and port channels.
neighbors	(Optional) Displays neighbor information only.

Command Default

None

Command Modes

User EXEC

Command History

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

Usage Guidelines

If you do not enter an interface ID, administrative and operational UDLD status for all interfaces appear.

Examples

This is an example of output from the **show uddl interface-id** command. For this display, UDLD is enabled on both ends of the link, and UDLD detects that the link is bidirectional. The table that follows describes the fields in this display.

```
Switch> show uddl gigabitethernet2/0/1
Interface gi2/0/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
Entry 1
Expiration time: 146
Device ID: 1
Current neighbor state: Bidirectional
Device name: Switch-A
Port ID: Gi2/0/1
Neighbor echo 1 device: Switch-B
Neighbor echo 1 port: Gi2/0/2
Message interval: 5
CDP Device name: Switch-A
```

Table 6: show uddld Field Descriptions

Field	Description
Interface	The interface on the local device configured for UDLD.
Port enable administrative configuration setting	How UDLD is configured on the port. If UDLD is enabled or disabled, the port enable configuration setting is the same as the operational enable state. Otherwise, the enable operational setting depends on the global enable setting.
Port enable operational state	Operational state that shows whether UDLD is actually running on this port.
Current bidirectional state	The bidirectional state of the link. An unknown state appears if the link is down or if it is connected to an UDLD-incapable device. A bidirectional state appears if the link is a normal two-way connection to a UDLD-capable device. All other values mean miswiring.
Current operational state	The current phase of the UDLD state machine. For a normal bidirectional link, the state machine is most often in the Advertisement phase.
Message interval	How often advertisement messages are sent from the local device. Measured in seconds.
Time out interval	The time period, in seconds, that UDLD waits for echoes from a neighbor device during the detection window.
Entry 1	Information from the first cache entry, which contains a copy of echo information received from the neighbor.
Expiration time	The amount of time in seconds remaining before this cache entry is aged out.
Device ID	The neighbor device identification.
Current neighbor state	The neighbor's current state. If both the local and neighbor devices are running UDLD normally, the neighbor state and local state should be bidirectional. If the link is down or the neighbor is not UDLD-capable, no cache entries appear.

Field	Description
Device name	The device name or the system serial number of the neighbor. The system serial number appears if the device name is not set or is set to the default (Switch).
Port ID	The neighbor port ID enabled for UDLD.
Neighbor echo 1 device	The device name of the neighbors' neighbor from which the echo originated.
Neighbor echo 1 port	The port number ID of the neighbor from which the echo originated.
Message interval	The rate, in seconds, at which the neighbor is sending advertisement messages.
CDP device name	The CDP device name or the system serial number. The system serial number appears if the device name is not set or is set to the default (Switch).

This is an example of output from the **show udd neighbors** command:

```
Switch# show udd neighbors
Port      Device Name      Device ID  Port-ID  OperState
-----
Gi2/0/1   Switch-A         1         Gi2/0/1  Bidirectional
Gi3/0/1   Switch-A         2         Gi3/0/1  Bidirectional
```

Related Commands

Command	Description
udd	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
udd port	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the udd global configuration command.
udd reset	Resets all interfaces shut down by UDLD and permits traffic to pass through again.

spanning-tree backbonefast

To enable BackboneFast to allow a blocked port on a switch to change immediately to a listening mode, use the **spanning-tree backbonefast** command in global configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree backbonefast
no spanning-tree backbonefast

Syntax Description This command has no arguments or keywords.

Command Default BackboneFast is disabled.

Command Modes Global configuration

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

Usage Guidelines Enable BackboneFast so that the switch detects indirect link failures and starts the spanning-tree reconfiguration sooner than it would under normal spanning-tree rules.

You can configure BackboneFast for rapid PVST+ or for multiple spanning-tree (MST) mode; however, the feature remains disabled until you change the spanning-tree mode to PVST+.

Use the **show spanning-tree** privileged EXEC command to verify your settings.

Examples The following example shows how to enable BackboneFast on the switch:

```
Switch(config)# spanning-tree backbonefast
```

Related Commands	Command	Description
	show spanning-tree	Displays spanning-tree information.

spanning-tree bpdudfilter

To enable bridge protocol data unit (BPDU) filtering on the interface, use the **spanning-tree bpdudfilter** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree bpdudfilter {enable| disable}

no spanning-tree bpdudfilter

Syntax Description

enable	Enables BPDU filtering on this interface.
disable	Disables BPDU filtering on this interface.

Command Default

The setting that is already configured when you enter the **spanning-tree portfast bpdudfilter default** command.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command has three states:

- **spanning-tree bpdudfilter enable** —Unconditionally enables BPDU filtering on the interface.
- **spanning-tree bpdudfilter disable** —Unconditionally disables BPDU filtering on the interface.
- **no spanning-tree bpdudfilter** —Enables BPDU filtering on the interface if the interface is in the operational PortFast state and if you configure the **spanning-tree portfast bpdudfilter default** command.



Caution

Be careful when you enter the **spanning-tree bpdudfilter enable** command. Enabling BPDU filtering on an interface is similar to disabling the spanning tree for this interface. If you do not use this command correctly, you might create bridging loops.

You can enable BPDU filtering when the switch is operating in the per-VLAN spanning-tree plus (PVST+) mode, the rapid-PVST mode, or the multiple spanning-tree (MST) mode.

You can globally enable BPDU filtering on all Port Fast-enabled interfaces with the **spanning-tree portfast bpdudfilter default** command.

The **spanning-tree bpdudfilter enable** command overrides the PortFast configuration.

Examples

This example shows how to enable BPDU filtering on this interface:

```
Switch(config-if) # spanning-tree bpdudfilter enable  
Switch(config-if) #
```

Related Commands

Command	Description
spanning-tree portfast (interface configuration)	Enables PortFast on the interface.

spanning-tree bpduguard

To enable bridge protocol data unit (BPDU) guard on the interface, use the **spanning-tree bpduguard** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree bpduguard {enable|disable}

no spanning-tree bpduguard

Syntax Description

enable	Enables BPDU guard on this interface.
disable	Disables BPDU guard on this interface.

Command Default

The setting that is already configured when you enter the **spanning-tree portfast bpduguard default** command.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Use the BPDU guard feature in a service-provider environment to prevent an access port from participating in the spanning tree. If the port still receives a BPDU, it is put in the error-disabled state as a protective measure. This command has three states:

- **spanning-tree bpduguard enable** —Unconditionally enables BPDU guard on the interface.
- **spanning-tree bpduguard disable** —Unconditionally disables BPDU guard on the interface.
- **no spanning-tree bpduguard** —Enables BPDU guard on the interface if the interface is in the operational PortFast state and if you configure the **spanning-tree portfast bpduguard default** command.

Examples

This example shows how to enable BPDU guard on an interface:

```
Switch(config-if)# spanning-tree bpduguard enable
Switch(config-if)#
```

Related Commands

Command	Description
spanning-tree portfast (interface configuration)	Enables PortFast on the interface.

spanning-tree cost

To set the path cost of the interface for Spanning Tree Protocol (STP) calculations, use the **spanning-tree cost** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

spanning-tree [**vlan** *vlan-id*] **cost** *cost*

no spanning-tree cost

Syntax Description

vlan <i>vlan-id</i>	(Optional) Specifies the VLAN range associated with the spanning-tree instance. The range of VLAN IDs is 1 to 4094.
<i>cost</i>	The path cost; valid values are from 1 to 200000000.

Command Default

The default path cost is computed from the bandwidth setting of the interface. Default path costs are:

- 1 Gb/s: 4
- 100 Mb/s: 19
- 10 Mb/s: 100

Command Modes

Interface configuration

Command History

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

Usage Guidelines

When you specify VLANs associated with a spanning tree instance, you can specify a single VLAN identified by a VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLAN IDs separated by a comma.

When you specify a value for the cost argument, higher values indicate higher costs. This range applies regardless of the protocol type specified.

Examples

This example shows how to set the path cost on an interface to a value of 250:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# spanning-tree cost 250
```

This example shows how to set the path cost to 300 for VLANS 10, 12 to 15, and 20:

```
Switch(config-if)# spanning-tree vlan 10,12-15,20 cost 300
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information.
spanning-tree port-priority	Sets the interface priority for spanning tree.
spanning-tree vlan	Configures STP on a per-VLAN basis.

spanning-tree etherchannel guard misconfig

To display an error message when the switch detects an EtherChannel misconfiguration, use the **spanning-tree etherchannel guard misconfig** command in global configuration mode. To disable the error message, use the **no** form of this command.

spanning-tree etherchannel guard misconfig

no spanning-tree etherchannel guard misconfig

Syntax Description This command has no arguments or keywords.

Command Default Error messages are displayed.

Command Modes Global configuration

Command History

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

Usage Guidelines

When the switch detects an EtherChannel misconfiguration, this error message is displayed:

```
PM-4-ERR_DISABLE: Channel-misconfig error detected on [chars], putting [chars] in err-disable state.
```

To determine which local ports are involved in the misconfiguration, enter the **show interfaces status err-disabled** command. To check the EtherChannel configuration on the remote device, enter the **show etherchannel summary** command on the remote device.

After you correct the configuration, enter the **shutdown** and the **no shutdown** commands on the associated port-channel interface.

Examples

This example shows how to enable the EtherChannel-guard misconfiguration:

```
Switch(config)# spanning-tree etherchannel guard misconfig
```

Related Commands

Command	Description
show etherchannel	Displays EtherChannel information for a channel.

spanning-tree extend system-id

To enable extended system identification, use the **spanning-tree extend system-id** command in global configuration mode. To disable extended system identification, use the **no** form of this command.

spanning-tree extend system-id

no spanning-tree extend system-id

Syntax Description This command has no arguments or keywords.

Command Default The extended system ID is enabled.

Command Modes Global configuration

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

Usage Guidelines The spanning tree uses the extended system ID, the switch priority, and the allocated spanning-tree MAC address to make the bridge ID unique for each VLAN or multiple spanning-tree instance. Because a switch stack appears as a single switch to the rest of the network, all switches in the stack use the same bridge ID for a given spanning tree. If the stack master fails, the stack members recalculate their bridge IDs of all running spanning trees based on the new MAC address of the stack master.

Support for the extended system ID affects how you manually configure the root switch, the secondary root switch, and the switch priority of a VLAN.

If your network consists of switches that do not support the extended system ID and switches that do support it, it is unlikely that the switch with the extended system ID support will become the root switch. The extended system ID increases the switch priority value every time the VLAN number is greater than the priority of the connected switches.

Examples This example shows how to enable the extended-system ID:

```
Switch(config)# spanning-tree extend system-id
```

Related Commands	Command	Description
	spanning-tree mst root	Configures the MST root switch.
	spanning-tree vlan	Configures STP on a per-VLAN basis.

Command	Description
show spanning-tree	Displays spanning-tree information.

spanning-tree guard

To enable or disable root-guard mode or loop-guard mode on the VLANs associated with an interface, use the **spanning-tree guard** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree guard {loop| root| none}

no spanning-tree guard

Syntax Description

loop	Enables the loop-guard mode on the interface.
root	Enables root-guard mode on the interface.
none	Sets the guard mode to none.

Command Default

Root-guard mode is disabled.

Loop-guard mode is configured according to the **spanning-tree loopguard default** command in global configuration mode.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

You can enable root guard or loop guard when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

You cannot enable both root guard and loop guard at the same time.

Use the **spanning-tree guard loop** command to override the setting of the spanning-tree loop guard default setting.

When root guard is enabled, if spanning-tree calculations cause an interface to be selected as the root port, the interface transitions to the root-inconsistent (blocked) state to prevent the switch from becoming the root switch or from being in the path to the root. The root port provides the best path from the switch to the root switch.

When the **no spanning-tree guard** or the **no spanning-tree guard none** command is entered, root guard is disabled for all VLANs on the selected interface. If this interface is in the root-inconsistent (blocked) state, it automatically transitions to the listening state.

Do not enable root guard on interfaces that will be used by the UplinkFast feature. With UplinkFast, the backup interfaces (in the blocked state) replace the root port in the case of a failure. However, if root guard is also enabled, all the backup interfaces used by the UplinkFast feature are placed in the root-inconsistent state (blocked) and are prevented from reaching the forwarding state. The UplinkFast feature is not available when the switch is operating in the rapid-PVST+ or MST mode.

Examples

This example shows how to enable root guard on all the VLANs associated with the specified interface:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# spanning-tree guard root
```

Related Commands

Command	Description
spanning-tree loopguard default	Enables loop guard on all ports.

spanning-tree link-type

To configure a link type for a port, use the **spanning-tree link-type** command in the interface configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree link-type {point-to-point| shared}

no spanning-tree link-type

Syntax Description

point-to-point	Specifies that the interface is a point-to-point link.
shared	Specifies that the interface is a shared medium.

Command Default

Link type is automatically derived from the duplex setting unless you explicitly configure the link type.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Rapid Spanning Tree Protocol Plus (RSTP+) fast transition works only on point-to-point links between two bridges.

By default, the switch derives the link type of a port from the duplex mode. A full-duplex port is considered as a point-to-point link while a half-duplex configuration is assumed to be on a shared link.

If you designate a port as a shared link, RSTP+ fast transition is forbidden, regardless of the duplex setting.

Examples

This example shows how to configure the port as a shared link:

```
Switch(config-if)# spanning-tree link-type shared
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information.

spanning-tree loopguard default

To enable loop guard as a default on all ports of a given bridge, use the **spanning-tree loopguard default** command in global configuration mode. To disable loop guard, use the **no** form of this command.

spanning-tree loopguard default

no spanning-tree loopguard default

Syntax Description This command has no arguments or keywords.

Command Default Loop guard is disabled.

Command Modes Global configuration

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

Usage Guidelines Loop guard provides additional security in the bridge network. Loop guard prevents alternate or root ports from becoming the designated port due to a failure that could lead to a unidirectional link.

Loop guard operates only on ports that are considered point-to-point by the spanning tree.

The individual loop-guard port configuration overrides this command.

Examples This example shows how to enable loop guard:

```
Switch(config)# spanning-tree loopguard default
```

Related Commands	Command	Description
	spanning-tree guard	Enables root guard or loop guard.

spanning-tree mode

To switch between per-VLAN Spanning Tree+ (PVST+), Rapid-PVST+, and Multiple Spanning Tree (MST) modes, use the **spanning-tree mode** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mode {pvst| mst| rapid-pvst}

no spanning-tree mode

Syntax Description

pvst	Enables PVST+ mode.
mst	Enables MST mode.
rapid-pvst	Enables Rapid-PVST+ mode.

Command Default

The default mode is PVST+.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Only one mode can be active at a time.

All stack members run the same spanning-tree mode.



Caution

Be careful when using the **spanning-tree mode** command to switch between PVST+, Rapid-PVST+, and MST modes. When you enter the command, all spanning-tree instances are stopped for the previous mode and are restarted in the new mode. Using this command may cause disruption of user traffic.

Examples

This example shows how to enable MST mode:

```
Switch(config)# spanning-tree mode mst
```

This example shows how to return to the default mode (PVST+):

```
Switch(config)# no spanning-tree mode
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information.

spanning-tree mst configuration

To enter MST-configuration mode, use the **spanning-tree mst configuration** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst configuration

no spanning-tree mst configuration

Syntax Description

This command has no arguments or keywords.

Command Default

The default value for the Multiple Spanning Tree (MST) configuration is the default value for all its parameters:

- No VLANs are mapped to any MST instance (all VLANs are mapped to the Common and Internal Spanning Tree [CIST] instance).
- The region name is an empty string.
- The revision number is 0.

Command Modes

Global configuration

Command History

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

Usage Guidelines

You can use these commands for MST configuration:

- **abort** Exits the MST region configuration mode without applying configuration changes.
- **exit** Exits the MST region configuration mode and applies all configuration changes.
- **instance** *instance_id* **vlan** *vlan_id* Maps VLANs to an MST instance. The range for instance IDs is 1 to 4094. The range for VLANs is 1 to 4094. You can specify a single VLAN identified by a VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.
- **name** *name* Sets the configuration name. The *name* string is case sensitive and can be up to 32 characters long.
- **no** Negates the instance, name and revision commands or sets them to their defaults.
- **revision** *version* Sets the configuration revision number. The range is 0 to 65535.
- **show** [**current** | **pending**] Displays the current or pending MST region configuration.

In MST mode, a switch stack supports up to 65 MST instances. The number of VLANs that can be mapped to a particular MST instance is unlimited.

For two or more switches to be in the same MST region, they must have the same VLAN mapping, the same configuration name, and the same configuration revision number.

When you map VLANs to an MST instance, the mapping is incremental, and VLANs specified in the command are added to or removed from the VLANs that were previously mapped. To specify a range, use a hyphen; for example, **instance 1 vlan 1-63** maps VLANs 1 to 63 to MST instance 1. To specify a series, use a comma; for example, **instance 1 vlan 10, 20, 30** maps VLANs 10, 20, and 30 to MST instance 1.

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST by using the **no** form of this command.

Changing an MST-configuration mode parameter can cause connectivity loss. To reduce service disruptions, when you enter MST-configuration mode, make changes to a copy of the current MST configuration. When you have finished editing the configuration, you can apply all the changes at once by using the **exit** keyword, or you can exit the mode without committing any change to the configuration by using the **abort** keyword.

Examples

This example shows how to enter MST-configuration mode, map VLANs 10 to 20 to MST instance 1, name the region region1, set the configuration revision to 1 and display the pending configuration:

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instance  Vlans  Mapped
-----  -----
0          1-9,21-4094
1          10-20
-----
```

This example shows how to reset the MST configuration to the default settings:

```
Switch(config)# no spanning-tree mst configuration
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information.

spanning-tree mst cost

To set the path cost of the interface for multiple spanning tree (MST) calculations, use the **spanning-tree mst cost** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

spanning-tree mst *instance-id* **cost** *cost*

no spanning-tree mst *instance-id* **cost**

Syntax Description

<i>instance-id</i>	Range of spanning-tree instances. The range is 1 to 4094.
<i>cost</i>	Path cost. The range is 1 to 200000000.

Command Default

The default path cost is computed from the bandwidth setting of the interface. Default path costs are:

- 1 Gb/s: 20000
- 100 Mb/s: 200000
- 10 Mb/s: 2000000

Command Modes

Interface configuration

Command History

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

Usage Guidelines

When you specify a value for the cost argument, higher values indicate higher costs.

Examples

This example shows how to set the path cost for an interface associated with MST instances 2 and 4 to 50:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# spanning-tree mst 2,4 cost 250
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information.

spanning-tree mst forward-time

To set the forward-delay timer for MST instances, use the **spanning-tree mst forward-time** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst forward-time *seconds*

no spanning-tree mst forward-time

Syntax Description

<i>seconds</i>	Number of seconds to set the forward-delay timer for all the MST instances. The range is 4 to 30.
----------------	---

Command Default

The default is 15 seconds.

Command Modes

Global configuration

Command History

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

Examples

This example shows how to set the forward-delay timer for all MST instances:

```
Switch(config)# spanning-tree mst forward-time 20
```

Related Commands

Command	Description
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by the root switch.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Specifies the number of hops allowed before a BPDU is discarded.

spanning-tree mst hello-time

To set the hello-time delay timer, use the **spanning-tree mst hello-time** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst hello-time *seconds*

no spanning-tree mst hello-time

Syntax Description

<i>seconds</i>	Interval, in seconds, between hello BPDUs. The range is 1 to 10.
----------------	--

Command Default

The default is 2.

Command Modes

Global configuration

Command History

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

Usage Guidelines

If you do not specify the *hello-time* value, the value is calculated from the network diameter.

Exercise care when using this command. For most situations, we recommend that you use the **spanning-tree vlan *vlan-id* root primary** and the **spanning-tree vlan *vlan-id* root secondary** global configuration commands to modify the hello time.

Examples

This example shows how to set the hello-time delay timer to 3 seconds:

```
Switch(config)# spanning-tree mst hello-time 3
```

Related Commands

Command	Description
spanning-tree mst forward-time	Sets the forward-delay time for MST instances.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Specifies the number of hops allowed before a BPDU is discarded.

spanning-tree mst max-age

To set the interval between messages that the spanning tree receives from the root switch, use the **spanning-tree mst max-age** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst max-age *seconds*

no spanning-tree mst max-age

Syntax Description

<i>seconds</i>	Interval, in seconds, between messages the spanning tree receives from the root switch. The range is 6 to 40.
----------------	---

Command Default

The default is 20.

Command Modes

Global configuration

Command History

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

Examples

This example shows how to set the max-age timer to 40 seconds:

```
Switch(config)# spanning-tree mst max-age 40
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information.
spanning-tree mst forward-time	Sets the forward-delay time for MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by the root switch.
spanning-tree mst max-hops	Specifies the number of hops allowed before a BPDU is discarded.

spanning-tree mst max-hops

To specify the number of possible hops in the region before a bridge protocol data unit (BPDU) is discarded, use the **spanning-tree mst max-hops** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst max-hops *hop-count*

no spanning-tree mst max-hops

Syntax Description

<i>hop-count</i>	Number of possible hops in the region before a BPDU is discarded. The range is 1 to 255.
------------------	--

Command Default

The default is 20.

Command Modes

Global configuration

Command History

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

Examples

This example shows how to set the number of possible hops to 25:

```
Switch(config)# spanning-tree mst max-hops 25
```

Related Commands

Command	Description
spanning-tree mst forward-time	Sets the forward-delay time for MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by the root switch.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.

spanning-tree mst port-priority

To set the priority for an interface, use the **spanning-tree mst port-priority** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst *instance-id* **port-priority**

Syntax Description

<i>instance-id</i>	Range of spanning-tree instances. The range is 1 to 4094.
<i>priority</i>	Priority. The range is 0 to 240 in increments of 16.

Command Default

The default is 128.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

You can assign higher priority values (lower numerical values) to interfaces that you want selected first and lower priority values (higher numerical values) that you want selected last. If all interfaces have the same priority value, the multiple spanning tree (MST) puts the interface with the lowest interface number in the forwarding state and blocks other interfaces.

If the switch is a member of a switch stack, you must use the **spanning-tree mst** *instance_id* **cost** *cost* command to select an interface to put in the forwarding state.

Examples

This example shows how to increase the likelihood that the interface associated with spanning-tree instances 20 and 22 is placed into the forwarding state if a loop occurs:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# spanning-tree mst 20,24 port-priority 0
```

Related Commands

Command	Description
spanning-tree mst cost	Configures the path cost for MST calculations.
spanning-tree mst priority	Sets the priority for the specified MST.

spanning-tree mst pre-standard

To configure a port to transmit only prestandard bridge protocol data units (BPDUs), use the **spanning-tree mst pre-standard** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst pre-standard

no spanning-tree mst pre-standard

Syntax Description This command has no arguments or keywords.

Command Default The default is to automatically detect prestandard neighbors.

Command Modes Interface configuration

Command History

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

Usage Guidelines

The port can accept both prestandard and standard BPDUs. If the neighbor types are mismatched, only the common and internal spanning tree (CIST) runs on this interface.



Note

If a switch port is connected to a switch running prestandard Cisco IOS software, you must use the **spanning-tree mst pre-standard** interface configuration command on the port. If you do not configure the port to send only prestandard BPDUs, the Multiple STP (MSTP) performance might diminish.

When the port is configured to automatically detect prestandard neighbors, the prestandard flag always appears in the **show spanning-tree mst** commands.

Examples

This example shows how to configure a port to transmit only prestandard BPDUs:

```
Switch(config-if) # spanning-tree mst pre-standard
```

Related Commands

Command	Description
spanning-tree bpdupfilter	Enables BPDU filtering on the interface.
spanning-tree bpduguard	Enables BPDU guard on the interface.
spanning-tree portfast (interface configuration)	Enables PortFast on the interface.

spanning-tree mst priority

To set the bridge priority for an instance, use the **spanning-tree mst priority** command in global configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree mst *instance* **priority** *priority*

no spanning-tree mst priority

Syntax Description

<i>instance</i>	Instance identification number. The range is 0 to 4094.
priority <i>priority</i>	Specifies the bridge priority. The range is 0 to 614440 in increments of 4096.

Command Default

The default is 32768.

Command Modes

Global configuration

Command History

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

Usage Guidelines

You can set the bridge priority in increments of 4096 only. Valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 40960, 45056, 49152, 53248, 57344 and 61440.

You can enter *instance* as a single instance or a range of instances, for example, 0-3,5,7-9.

Examples

This example shows how to set the spanning tree priority for MST instance 0 to 4096:

```
Switch(config)# spanning-tree mst 0 priority 4096
```

Related Commands

Command	Description
spanning-tree mst configuration	Enters MST configuration mode.
spanning-tree mst root	Configures the MST root switch.

spanning-tree mst root

To designate the primary and secondary root switch and set the timer value for an instance, use the **spanning-tree mst root** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst *instance* **root** {**primary**|**secondary**}

no spanning-tree mst *instance* **root**

Syntax Description

<i>instance</i>	Instance identification number. The range is 0 to 4094.
primary	Forces this switch to be the root switch.
secondary	Specifies this switch to act as the root switch, if the primary root fail.

Command Default

None

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use this command only on backbone switches. You can enter *instance-id* as a single instance or a range of instances, for example, 0-3,5,7-9.

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

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

Examples

This example shows how to configure the switch as the root switch for instance 10:

```
Switch(config)# spanning-tree mst 10 root primary
```

spanning-tree pathcost method

To set the default path-cost calculation method, use the **spanning-tree pathcost method** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree pathcost method {long| short}

no spanning-tree pathcost method

Syntax Description

long	Specifies the 32-bit based values for default port-path costs.
short	Specifies the 16-bit based values for default port-path costs.

Command Default

short

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **long** path-cost calculation method utilizes all 32 bits for path-cost calculation and yields values in the range of 1 through 200,000,000.

The **short** path-cost calculation method (16 bits) yields values in the range of 1 through 65535.

Examples

This example shows how to set the default path-cost calculation method to long:

```
Switch(config)#spanning-tree pathcost method long
```

This example shows how to set the default path-cost calculation method to short:

```
Switch(config)#spanning-tree pathcost method short
```

spanning-tree port-priority

To configure an interface priority when two bridges tie for position as the root bridge, use the **spanning-tree port-priority** command in interface configuration mode. To return to the default value, use the **no** form of this command.

spanning-tree [**vlan** *vlan-id*] **port-priority** *port-priority*

no spanning-tree [**vlan** *vlan-id*] **port-priority**

Syntax Description

vlan <i>vlan-id</i>	(Optional) Specifies the VLAN range associated with the spanning-tree instance. The range is 1 to 4094.
<i>port-priority</i>	The port priority in increments of sixteen. The range is 0 to 240. The default is 128.

Command Default

The port priority is 128.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The priority you set breaks the tie.

Examples

The following example shows how to increase the likelihood that a port will be put in the forwarding state if a loop occurs:

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# spanning-tree vlan 20 port-priority 0
```

spanning-tree portfast (global configuration)

To enable bridge protocol data unit (BPDU) filtering on PortFast-enabled interfaces, the BPDU guard feature on PortFast-enabled interfaces, or the PortFast feature on all nontrunking interfaces, use the **spanning-treeportfast** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree portfast {**bpdufilter default**| **bpduguard default**| **default**}

no portfast {**bpdufilter default**| **bpduguard default**| **default**}

Syntax Description

bpdufilter default	Enables BPDU filtering on PortFast-enabled interfaces and prevents the switch interface connect to end stations from sending or receiving BPDUs.
bpduguard default	Enables the BPDU guard feature on PortFast-enabled interfaces and places the interfaces that receive BPDUs in an error-disabled state.
default	Enables the PortFast feature on all nontrunking interfaces.

Command Default

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

You can enable these features when the switch is operating in the per-VLAN spanning-tree plus (PVST+) rapid-PVST+, or the multiple spanning-tree (MST) mode.

Use the **spanning-tree portfast bpdufilter default** global configuration command to globally enable BPDU filtering on interfaces that are PortFast-enabled (the interfaces are in a PortFast-operational state). The interfaces still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs. You should globally enable BPDU filtering on a switch so that hosts connected to switch interfaces do not receive BPDUs. If a BPDU is received on a PortFast-enabled interface, the interface loses its PortFast-operational status and BPDU filtering is disabled.

You can override the **spanning-tree portfast bpdufilter default** command by using the **spanning-tree portfast bpdufilter** interface command.

**Caution**

Be careful when using this command. Enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

Use the **spanning-tree portfast bpduguard default** global configuration command to globally enable BPDU guard on interfaces that are in a PortFast-operational state. In a valid configuration, PortFast-enabled interfaces do not receive BPDUs. Receiving a BPDU on a PortFast-enabled interface signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the interface in the error-disabled state. The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface back in service. Use the BPDU guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

You can override the **spanning-tree portfast bpduguard default** command by using the **spanning-tree portfast bpduguard** interface command.

Use the **spanning-tree portfast default** command to globally enable the PortFast feature on all nontrunking interfaces. Configure PortFast only on interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation. A PortFast-enabled interface moves directly to the spanning-tree forwarding state when linkup occurs; it does not wait for the standard forward-delay time.

You can override the **spanning-tree portfast default** global configuration command by using the **spanning-tree portfast** interface configuration command. You can use the **no spanning-tree portfast default** global configuration command to disable PortFast on all interfaces unless they are individually configured with the **spanning-tree portfast** interface configuration command.

Examples

This example shows how to globally enable BPDU filtering by default:

```
Switch(config)# spanning-tree portfast bpduguard default
```

This example shows how to globally enable the BPDU guard feature by default:

```
Switch(config)# spanning-tree portfast bpduguard default
```

This example shows how to globally enable the PortFast feature on all nontrunking interfaces:

```
Switch(config)# spanning-tree portfast default
```

spanning-tree portfast (interface configuration)

To enable PortFast mode where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire, use the **spanning-tree portfast** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree portfast [**disable**| **trunk**]

no spanning-tree portfast

Syntax Description

disable	(Optional) Disables PortFast on the interface.
trunk	(Optional) Enables PortFast edge mode on the interface.

Command Default

The settings that are configured by the **spanning-treeportfastdefault** command.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

You can enable this feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), Rapid PVST+, or the multiple spanning-tree (MST) mode.

This feature affects all VLANs on the interface.

Use this command only on interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the switch and network operation.

To enable PortFast on trunk ports, you must use the **spanning-tree portfast trunk** interface configuration command. The **spanning-tree portfast** command is not supported on trunk ports.

An interface with the PortFast feature enabled is moved directly to the spanning-tree forwarding state without the standard forward-time delay.

You can use the **spanning-tree portfast default** global configuration command to globally enable the PortFast feature on all nontrunking interfaces. Use the **spanning-tree portfast** interface configuration command to override the global setting.

If you configure the **spanning-tree portfast default** global configuration command, you can disable PortFast on an interface that is not a trunk interface by using the **spanning-tree portfast disable** interface configuration command.

Examples

This example shows how to enable the PortFast feature on a port:

```
Switch(config)# interface gigabitethernet1/0/2  
Switch(config-if) #spanning-tree portfast
```

Related Commands

Command	Description
spanning-tree bpdupfilter	Enables BPDU filtering on the interface.
spanning-tree bpduguard	Enables BPDU guard on the interface.
spanning-tree portfast (global configuration)	Enables bridge protocol data unit (BPDU) filtering on PortFast-enabled interfaces.

spanning-tree transmit hold-count

To specify the transmit hold count, use the **spanning-tree transmit hold-count** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree transmit hold-count *value*

no spanning-tree transmit hold-count

Syntax Description

<i>value</i>	Number of bridge protocol data units (BPDUs) sent every second. The range is 1 to 20.
--------------	---

Command Default

The default is 6.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command is supported on all spanning-tree modes.

The transmit hold count determines the number of BPDUs that can be sent before pausing for 1 second.



Note

Increasing the transmit-hold count value can have a significant impact on CPU utilization, especially in Rapid Per-VLAN Spanning Tree (PVST+) mode. Decreasing this value might result in slow convergence. We recommend that you used the default setting.

Examples

This example shows how to specify the transmit hold count 8:

```
Switch(config)# spanning-tree transmit hold-count 8
```

spanning-tree uplinkfast

To enable UplinkFast, use the **spanning-tree uplinkfast** command in global configuration mode. To disable UplinkFast, use the **no** form of this command.

spanning-tree uplinkfast [**max-update-rate** *packets-per-second*]

no spanning-tree uplinkfast [**max-update-rate**]

Syntax Description

max-update-rate <i>packets-per-second</i>	(Optional) Specifies the rate (number of packets per second) at which update packets are sent. The range is 0 to 320000. The default is 150.
---	---

Command Default

UplinkFast is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use this command only on access switches.

You can configure the UplinkFast feature for rapid PVST+ or for multiple spanning-tree (MST) mode, but the feature remains disabled (inactive) until you change the spanning-tree mode to PVST+.

When you enable UplinkFast, it is enabled for the entire switch; it cannot be enabled for individual VLANs.

When you enable or disable UplinkFast, cross-stack UplinkFast (CSUF) also is automatically enabled or disabled on all nonstack port interfaces. CSUF accelerates the choice of a new root port when a link or switch fails or when spanning tree reconfigures itself.

When UplinkFast is enabled, the switch priority of all VLANs is set to 49152. If you change the path cost to a value less than 3000 and you enable UplinkFast or UplinkFast is already enabled, the path cost of all interfaces and VLAN trunks is increased by 3000 (if you change the path cost to 3000 or above, the path cost is not altered). The changes to the switch priority and the path cost reduces the chance that a switch will become the root switch.

When UplinkFast is disabled, the switch priorities of all VLANs and path costs of all interfaces are set to default values if you did not modify them from their defaults.

When spanning tree detects that the root port has failed, UplinkFast immediately changes to an alternate root port, changing the new root port directly to forwarding state. During this time, a topology change notification is sent.

Do not enable the root guard on interfaces that will be used by the UplinkFast feature. With UplinkFast, the backup interfaces (in the blocked state) replace the root port in the case of a failure. However, if root guard is also enabled, all the backup interfaces used by the UplinkFast feature are placed in the root-inconsistent state (blocked) and prevented from reaching the forwarding state.

If you set the max-update-rate to 0, station-learning frames are not generated, so the spanning-tree topology converges more slowly after a loss of connectivity.

Examples

This example shows how to enable UplinkFast and set the maximum rate to 200 packets per second:

```
Switch(config)# spanning-tree uplinkfast max-update-rate 200
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information.
spanning-tree vlan	Configures STP on a per-VLAN basis.

spanning-tree vlan

To configure Spanning Tree Protocol (STP) on a per-virtual LAN (VLAN) basis, use the **spanning-tree vlan** command in global configuration mode. To return to the default settings, use the **no** form of this command.

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

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

Syntax Description

<i>vlan-id</i>	VLAN range associated with the spanning-tree instance. The range is 1 to 4094.
forward-time <i>seconds</i>	(Optional) Sets the STP forward delay time in second. The range is 4 to 30. The default is 15.
hello-time <i>seconds</i>	(Optional) Specifies the duration, in seconds, between the generation of configuration messages by the root switch. The range is 1 to 10. The default is 2.
max-age <i>seconds</i>	(Optional) Sets the maximum number of seconds the information in a bridge packet data unit (BPDU) is valid. The range is 6 to 40. The default is 20.
priority <i>priority</i>	(Optional) Sets the STP bridge priority. The range is 0 to 61440 in increments of 4096. The default for the primary root switch is 24576. The default for the secondary root switch is 28672.
root primary	(Optional) Forces this switch to be the root switch.
root secondary	(Optional) Specifies this switch to act as the root switch should the primary root fail.
diameter <i>net-diameter</i>	(Optional) Specifies the maximum number of switches between any two points of attachment of end stations. The range is 2 through 7.

Command Default

Spanning tree is enabled on all VLANs.

Command Modes

Global configuration

Command History

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

Usage Guidelines

If the switch does not hear BPDUs within the time specified by the **max-age seconds-** value, it recomputes the spanning-tree topology.

Use the **spanning-tree vlan *vlan-id* root** only on backbone switches.

The **spanning-tree vlan *vlan-id* root secondary** command alters this switch's priority from 32768 to 28672. If the root switch should fail, this switch becomes the next root switch.

**Caution**

We do not recommend disabling spanning tree, even in a topology that is free of physical loops. Spanning tree is a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.

Examples

The following example shows how to enable spanning tree on VLAN 200:

```
Switch(config)# spanning-tree vlan 200
```

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

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

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

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

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information.

switchport access vlan

To configure a port as a static-access or dynamic-access port, use the **switchport access vlan** command in interface configuration mode. To reset the access mode to the default VLAN mode, use the **no** form of this command.

switchport access vlan {*vlan-id*} **dynamic**}

no switchport access vlan

Syntax Description

vlan-id VLAN ID of the access mode VLAN. The range is 1 to 4094.

dynamic Specifies that the access mode VLAN is dependent on the VLAN Membership Policy Server (VMPS) protocol. The port is assigned to a VLAN based on the source MAC address of a host (or hosts) connected to the port. The switch sends every new MAC address received to the VMPS server to get the VLAN name to which the dynamic-access port should be assigned. If the port already has a VLAN assigned and the source has already been approved by the VMPS, the switch forwards the packet to the VLAN.

Command Default

The default access VLAN and trunk interface native VLAN is a default VLAN corresponding to the platform or interface hardware.

A dynamic-access port is initially a member of no VLAN and receives its assignment based on the packet it receives.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The port must be in access mode before the **switchport access vlan** command can take effect.

If the switchport mode is set to **access vlan** *vlan-id*, the port operates as a member of the specified VLAN. If set to **access vlan dynamic**, the port starts discovery of VLAN assignment based on the incoming packets it receives. An access port can be assigned to only one VLAN.

The **no switchport access** command resets the access mode VLAN to the appropriate default VLAN for the device.

You must configure the VMPS server before configuring a port as dynamic.

These restrictions apply to dynamic-access ports:

- The software implements the VLAN Query Protocol (VQP) client, which can query a VMPS, such as a Catalyst 6500 series switch. The switch cannot be a VMPS. You must configure the server before configuring a port configured as dynamic.
- Use dynamic-access ports only to connect end stations. Connecting them to switches or routers (that use bridging protocols) can cause a loss of connectivity.
- Configure the network so that STP does not put the dynamic-access port into an STP blocking state. The Port Fast feature is automatically enabled on dynamic-access ports.
- Dynamic-access ports can only be in one VLAN and do not use VLAN tagging.
- Dynamic-access ports cannot be configured as
 - Members of an EtherChannel port group (dynamic-access ports cannot be grouped with any other port, including other dynamic ports).
 - Source or destination ports in a static address entry.
 - Monitor ports.

You can verify your setting by entering the **show interfaces *vlan-id* switchport** privileged EXEC command and examining information in the Administrative Mode and Operational Mode rows.

Examples

This example shows how to change a switched port interface that is operating in access mode to operate in VLAN 2 instead of the default VLAN:

```
Switch(config-if)# switchport access vlan 2
```

Related Commands

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

switchport mode

To configure the VLAN membership mode of a port, use the **switchport mode** command in interface configuration mode. To reset the mode to the appropriate default for the device, use the **no** form of this command.

```
switchport mode {access | dot1q-tunnel | dynamic {auto | desirable } | private-vlan | trunk}
no switchport mode {access | dot1q-tunnel | dynamic | trunk }
```

Syntax Description

access	Sets the port to access mode (either static-access or dynamic-access depending on the setting of the switchport access vlan interface configuration command). The port is set to access unconditionally and operates as a nontrunking, single VLAN interface that sends and receives nonencapsulated (non-tagged) frames. An access port can be assigned to only one VLAN.
dot1q-tunnel	Sets the port as an IEEE 802.1Q tunnel port.
dynamic auto	Sets the port trunking mode dynamic parameter to auto to specify that the interface convert the link to a trunk link. This is the default switchport mode.
dynamic desirable	Sets the port trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link.
private-vlan	See the switchport mode private-vlan command.
trunk	Sets the port to trunk unconditionally. The port is a trunking VLAN Layer 2 interface. The port sends and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two switches or between a switch and a router.

Command Default

The default mode is **dynamic auto**.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

A configuration that uses the **access** or **trunk** keywords takes effect only when you configure the port in the appropriate mode by using the **switchport mode** command. The static-access and trunk configuration are saved, but only one configuration is active at a time.

When you enter **access** mode, the interface changes to permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

When you enter **trunk** mode, the interface changes to permanent trunking mode and negotiates to convert the link into a trunk link even if the interface connecting to it does not agree to the change.

When you enter **dynamic auto** mode, the interface converts the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode.

When you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.

To autonegotiate trunking, the interfaces must be in the same VLAN Trunking Protocol (VTP) domain. Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a point-to-point protocol. However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations. To avoid this, you should configure interfaces connected to devices that do not support DTP to not forward DTP frames, which turns 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.

When you enter **dot1q-tunnel**, the port is set unconditionally as an IEEE 802.1Q tunnel port.

Access ports, trunk ports, and tunnel ports are mutually exclusive.

Any IEEE 802.1Q encapsulated IP packets received on a tunnel port can be filtered by MAC access control lists (ACLs), but not by IP ACLs. This is because the switch does not recognize the protocol inside the IEEE 802.1Q header. This restriction applies to router ACLs, port ACLs, and VLAN maps.

Configuring a port as an IEEE 802.1Q tunnel port has these limitations:

- IP routing and fallback bridging are not supported on tunnel ports.
- Tunnel ports do not support IP ACLs.
- If an IP ACL is applied to a trunk port in a VLAN that includes tunnel ports, or if a VLAN map is applied to a VLAN that includes tunnel ports, packets received from the tunnel port are treated as non-IP packets and are filtered with MAC access lists.
- Layer 3 quality of service (QoS) ACLs and other QoS features related to Layer 3 information are not supported on tunnel ports.

For more information about configuring IEEE 802.1Q tunnel ports, see the software configuration guide for this release.

The IEEE 802.1x feature interacts with switchport modes in these ways:

- 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.
- If you try to enable IEEE 802.1x on a port set to **dynamic auto** or **dynamic desirable**, 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 auto** or **dynamic desirable**, the port mode is not changed.

- If you try to enable IEEE 802.1x on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and IEEE 802.1x is not enabled. If you try to change an IEEE 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.

You can verify your settings by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command and examining information in the *Administrative Mode* and *Operational Mode* rows.

Examples

This example shows how to configure a port for access mode:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode access
```

This example shows how set the port to dynamic desirable mode:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode dynamic desirable
```

This example shows how to configure a port for trunk mode:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode trunk
```

This example shows how to configure a port as an IEEE 802.1Q tunnel port:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode dot1q-tunnel
```

Related Commands

Command	Description
switchport access vlan	Configures a port as a static-access or dynamic-access port.

switchport nonegotiate

To specify that Dynamic Trunking Protocol (DTP) negotiation packets are not sent on the Layer 2 interface, use the **switchport nonegotiate** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

switchport nonegotiate

no switchport nonegotiate

Syntax Description This command has no keywords or arguments.

Command Default The default is to use DTP negotiation to learn the trunking status.

Command Modes Interface configuration

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

Usage Guidelines The **no switchport nonegotiate** command removes nonegotiate status.

This command is valid only when the interface switchport mode is access or trunk (configured by using the **switchport mode access** or the **switchport mode trunk** interface configuration command). This command returns an error if you attempt to execute it in dynamic (auto or desirable) mode.

Internetworking devices that do not support DTP might forward DTP frames improperly and cause misconfigurations. To avoid this problem, turn off DTP by using the **switchport nonegotiate** command to configure the interfaces connected to devices that do not support DTP to not forward DTP frames.

When you enter the **switchport nonegotiate** command, DTP negotiation packets are not sent on the interface. The device does or does not trunk according to the **mode** parameter: **access** or **trunk**.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking on 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.

Examples This example shows how to cause a port to refrain from negotiating trunking mode and to act as a trunk or access port (depending on the mode set):

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport nonegotiate
```

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

Related Commands

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

udld

To enable aggressive or normal mode in the UniDirectional Link Detection (UDLD) and to set the configurable message timer time, use the **udld** command in global configuration mode. To disable aggressive or normal mode UDLD on all fiber-optic ports, use the **no** form of the command.

udld {**aggressive**|**enable**| **message time** *message-timer-interval*}

no udld {**aggressive**|**enable**| **message**}

Syntax Description

aggressive	Enables UDLD in aggressive mode on all fiber-optic interfaces.
enable	Enables UDLD in normal mode on all fiber-optic interfaces.
message time <i>message-timer-interval</i>	Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is 1 to 90 seconds. The default is 15 seconds.

Command Default

UDLD is disabled on all interfaces.
The message timer is set at 15 seconds.

Command Modes

Global configuration

Command History

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

Usage Guidelines

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links. For information about normal and aggressive modes, see the *Catalyst 2960-X Switch Layer 2 Configuration Guide* *Catalyst 2960-XR Switch Layer 2 Configuration Guide*.

If you change the message time between probe packets, you are making a trade-off between the detection speed and the CPU load. By decreasing the time, you can make the detection-response faster but increase the load on the CPU.

This command affects fiber-optic interfaces only. Use the **udld** interface configuration command to enable UDLD on other interface types.

You can use these commands to reset an interface shut down by UDLD:

- The **udld reset** privileged EXEC command to reset all interfaces shut down by UDLD.

- The **shutdown** and **no shutdown** interface configuration commands.
- The **no udld enable** global configuration command followed by the **udld {aggressive | enable}** global configuration command to reenable UDLD globally.
- The **no udld port** interface configuration command followed by the **udld port** or **udld port aggressive** interface configuration command to reenable UDLD on the specified interface.
- The **errdisable recovery cause udld** and **errdisable recovery interval *interval*** global configuration commands to automatically recover from the UDLD error-disabled state.

Examples

This example shows how to enable UDLD on all fiber-optic interfaces:

```
Switch(config)# udld enable
```

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

Related Commands

Command	Description
show udld	Displays UDLD administrative and operational status for all ports or the specified port.
udld port	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the udld global configuration command.
udld reset	Resets all interfaces shut down by UDLD and permits traffic to pass through again.

udld port

To enable UniDirectional Link Detection (UDLD) on an individual interface or to prevent a fiber-optic interface from being enabled by the **udld** global configuration command, use the **udld port** command in interface configuration mode. To return to the **udld** global configuration command setting or to disable UDLD if entered for a nonfiber-optic port, use the **no** form of this command.

udld port [aggressive]

no udld port [aggressive]

Syntax Description

aggressive	(Optional) Enables UDLD in aggressive mode on the specified interface.
-------------------	--

Command Default

On fiber-optic interfaces, UDLD is disabled and fiber-optic interfaces enable UDLD according to the state of the **udld enable** or **udld aggressive** global configuration command.

On nonfiber-optic interfaces, UDLD is disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch.

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links.

To enable UDLD in normal mode, use the **udld port** interface configuration command. To enable UDLD in aggressive mode, use the **udld port aggressive** interface configuration command.

Use the **no udld port** command on fiber-optic ports to return control of UDLD to the **udld enable** global configuration command or to disable UDLD on nonfiber-optic ports.

Use the **udld port aggressive** command on fiber-optic ports to override the setting of the **udld enable** or **udld aggressive** global configuration command. Use the **no** form on fiber-optic ports to remove this setting and to return control of UDLD enabling to the **udld** global configuration command or to disable UDLD on nonfiber-optic ports.

You can use these commands to reset an interface shut down by UDLD:

- The **udld reset** privileged EXEC command resets all interfaces shut down by UDLD.

- The **shutdown** and **no shutdown** interface configuration commands.
- The **no udld enable** global configuration command, followed by the **udld {aggressive | enable}** global configuration command reenables UDLD globally.
- The **no udld port** interface configuration command, followed by the **udld port** or **udld port aggressive** interface configuration command reenables UDLD on the specified interface.
- The **errdisable recovery cause udld** and **errdisable recovery interval *interval*** global configuration commands automatically recover from the UDLD error-disabled state.

Examples

This example shows how to enable UDLD on an port:

```
Switch(config)# interface gigabitethernet6/0/1
Switch(config-if)# udld port
```

This example shows how to disable UDLD on a fiber-optic interface despite the setting of the **udld** global configuration command:

```
Switch(config)# interface gigabitethernet6/0/1
Switch(config-if)# no udld port
```

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

Related Commands

Command	Description
show udld	Displays UDLD administrative and operational status for all ports or the specified port.
udld	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
udld reset	Resets all interfaces shut down by UDLD and permits traffic to pass through again.

udld reset

To reset all interfaces disabled by UniDirectional Link Detection (UDLD) and permit traffic to begin passing through them again (though other features, such as spanning tree, Port Aggregation Protocol (PAgP), and Dynamic Trunking Protocol (DTP) still have their normal effects, if enabled), use the **udld reset** command in privileged EXEC mode.

udld reset

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC

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

Usage Guidelines If the interface configuration is still enabled for UDLD, these ports begin to run UDLD again and are disabled for the same reason if the problem has not been corrected.

Examples This example shows how to reset all interfaces disabled by UDLD:

```
Switch# udld reset
1 ports shutdown by UDLD were reset.
```

Related Commands	Command	Description
	show udld	Displays UDLD administrative and operational status for all ports or the specified port.
	udld	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
	udld port	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the udld global configuration command.



INDEX

C

channel-group command [16](#)
channel-protocol command [19](#)
clear lacp command [21](#)
clear pagp command [22](#)
clear spanning-tree counters command [23](#)
clear spanning-tree detected-protocols command [24](#)

D

debug etherchannel command [25](#)
debug lacp command [27](#)
debug pagp command [28](#)
debug platform etherchannel command [30](#)
debug platform pm command [31](#)
debug platform uddl command [36](#)
debug spanning-tree command [34](#)

I

interface port-channel command [37](#)

L

lacp port-priority command [39](#)
lacp system-priority command [41](#)
link state group command [43](#)
link state track command [44](#)

P

pagp learn-method command [45](#)
pagp port-priority command [47](#)
pagp timer command [49](#)
port-channel load-balance command [50](#)

S

show etherchannel command [51](#)
show lacp command [54](#)
show link state group command [59](#)
show pagp command [60](#)
show platform backup interface command [62](#)
show platform etherchannel command [63](#)
show platform pm command [64](#)
show platform spanning-tree command [66](#)
show spanning-tree command [67](#)
show uddl command [70](#)
spanning-tree backbonefast command [73](#)
spanning-tree bpdufilter command [74](#)
spanning-tree bpduguard command [76](#)
spanning-tree cost command [77](#)
spanning-tree etherchannel guard misconfig command [79](#)
spanning-tree extend system-id command [80](#)
spanning-tree guard command [82](#)
spanning-tree link-type command [84](#)
spanning-tree loopguard default command [85](#)
spanning-tree mode command [86](#)
spanning-tree mst configuration command [88](#)
spanning-tree mst cost command [90](#)
spanning-tree mst forward-time [91](#)
spanning-tree mst hello-time command [92](#)
spanning-tree mst max-age command [93](#)
spanning-tree mst max-hops command [94](#)
spanning-tree mst port-priority command [95](#)
spanning-tree mst pre-standard command [96](#)
spanning-tree mst priority command [97](#)
spanning-tree mst root command [98](#)
spanning-tree pathcost method command [100](#)
spanning-tree port-priority command [101](#)
spanning-tree portfast command (global configuration) [102](#)
spanning-tree portfast command (interface configuration) [104](#)
spanning-tree transmit hold-count command [106](#)
spanning-tree uplinkfast command [107](#)
spanning-tree vlan command [109](#)
switchport access vlan command [111](#)
switchport mode command [113](#)
switchport nonegotiate command [116](#)

U

udld command [118](#)

udld port command [120](#)

udld reset command [122](#)