



## **Layer 2/3 Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)**

**First Published:** October 10, 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-29948-01

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 v

Document Conventions v

Related Documentation vii

Obtaining Documentation and Submitting a Service Request vii

---

### CHAPTER 1

#### Using the Command-Line Interface 1

Information About Using the Command-Line Interface 1

Command Modes 1

Using the Help System 3

Understanding Abbreviated Commands 4

No and Default Forms of Commands 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 on a Switch Stack 12

Accessing the CLI Through a Console Connection or Through Telnet 12

---

### CHAPTER 2

#### Layer 2/3 Commands 13

channel-group 15

channel-protocol	18
clear lacp	20
clear pagp	21
clear spanning-tree counters	22
clear spanning-tree detected-protocols	23
debug etherchannel	25
debug lacp	27
debug pagp	28
debug platform pm	30
debug platform udld	32
debug spanning-tree	33
interface port-channel	35
lacp max-bundle	37
lacp port-priority	38
lacp system-priority	40
pagp learn-method	42
pagp port-priority	44
port-channel load-balance	46
port-channel load-balance extended	48
port-channel min-links	50
show etherchannel	52
show lacp	55
show pagp	60
show platform etherchannel	62
show platform pm	63
show udld	64
switchport	68
switchport access vlan	70
switchport mode	71
switchport nonegotiate	74
udld	76
udld port	78
udld reset	80



## Preface

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

## Document Conventions

This document uses the following conventions:

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

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

### Reader Alert Conventions

This document may use the following conventions for reader alerts:



#### Note

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



#### Tip

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



#### Caution

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



#### Timesaver

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



#### Warning

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

## Related Documentation

**Note**

---

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

---

- Cisco Catalyst 3650 Switch documentation, located at:  
[http://www.cisco.com/go/cat3650\\_docs](http://www.cisco.com/go/cat3650_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](http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html)
- Error Message Decoder, located at:  
<https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>

## Obtaining Documentation and Submitting a Service Request

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

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

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

## Using the Help System

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

### SUMMARY STEPS

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

### DETAILED STEPS

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

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

## Understanding Abbreviated Commands

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

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

```
Switch# show conf
```

## No and Default Forms of Commands

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

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

## CLI Error Messages

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

**Table 2: Common CLI Error Messages**

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

## Configuration Logging

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




---

**Note** Only CLI or HTTP changes are logged.

---

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

## Recalling Commands

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



### Note

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

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>Ctrl-P</b> or use the <b>up arrow</b> key	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
<b>Step 2</b>	<b>Ctrl-N</b> or use the <b>down arrow</b> key	Returns to more recent commands in the history buffer after recalling commands with <b>Ctrl-P</b> or the up arrow key. Repeat the key sequence to recall successively more recent commands.

	Command or Action	Purpose
<b>Step 3</b>	<b>show history</b>  <b>Example:</b> 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 <b>terminal history</b> global configuration command and the <b>history</b> line configuration command.

## Disabling the Command History Feature

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

### SUMMARY STEPS

1. `terminal no history`

### DETAILED STEPS

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

## Enabling and Disabling Editing Features

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

### SUMMARY STEPS

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

### DETAILED STEPS

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

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



## Editing Commands Through Keystrokes

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


**Note**

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

**Table 3: Editing Commands**

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

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

## Editing Command Lines That Wrap

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

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



### Note

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

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

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>access-list</b>  <b>Example:</b> Switch(config)# <b>access-list 101 permit tcp</b>	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><b>Ctrl-A</b></p> <p><b>Example:</b></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	<b>Return key</b>	<p>Execute the commands.</p> <p>The software assumes that you have a terminal screen that is 80 columns wide. If you have a different width, use the <b>terminal width</b> privileged EXEC command to set the width of your terminal.</p> <p>Use line wrapping with the command history feature to recall and modify previous complex command entries.</p>

## Searching and Filtering Output of show and more Commands

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

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>{show   more} command   {begin   include   exclude} regular-expression</pre> <p><b>Example:</b></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 <b>  exclude output</b>, the lines that contain <b>output</b> are not displayed, but the lines that contain <b>OUTPUT</b> appear.</p>

## Accessing the CLI on a Switch Stack

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

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

**Note**

---

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

---

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

To debug the standby switch, use the **session standby ios** privileged EXEC command from the active switch to access the IOS console of the standby switch. To debug a specific stack member, use the **session switch stack-member-number** privileged EXEC command from the active switch to access the diagnostic shell of the stack member. For more information about these commands, see the switch command reference.

## 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 15
- [channel-protocol](#), page 18
- [clear lacp](#), page 20
- [clear pagp](#), page 21
- [clear spanning-tree counters](#), page 22
- [clear spanning-tree detected-protocols](#), page 23
- [debug etherchannel](#), page 25
- [debug lacp](#), page 27
- [debug pagp](#), page 28
- [debug platform pm](#), page 30
- [debug platform udd](#), page 32
- [debug spanning-tree](#), page 33
- [interface port-channel](#), page 35
- [lacp max-bundle](#), page 37
- [lacp port-priority](#), page 38
- [lacp system-priority](#), page 40
- [pagp learn-method](#), page 42
- [pagp port-priority](#), page 44
- [port-channel load-balance](#), page 46
- [port-channel load-balance extended](#), page 48
- [port-channel min-links](#), page 50
- [show etherchannel](#), page 52
- [show lacp](#), page 55
- [show pagp](#), page 60

- [show platform etherchannel](#), page 62
- [show platform pm](#), page 63
- [show uddl](#), page 64
- [switchport](#), page 68
- [switchport access vlan](#), page 70
- [switchport mode](#), page 71
- [switchport nonegotiate](#), page 74
- [uddl](#), page 76
- [uddl port](#), page 78
- [uddl reset](#), page 80

# 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 128.
<b>mode</b>	Specifies the EtherChannel mode.
<b>active</b>	Unconditionally enables Link Aggregation Control Protocol (LACP).
<b>auto</b>	Enables the Port Aggregation Protocol (PAgP) only if a PAgP device is detected.
<b>non-silent</b>	(Optional) Configures the interface for nonsilent operation when connected to a partner that is PAgP-capable. Use in PAgP mode with the <b>auto</b> or <b>desirable</b> keyword when traffic is expected from the other device.
<b>desirable</b>	Unconditionally enables PAgP.
<b>on</b>	Enables the on mode.
<b>passive</b>	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 XE 3.3SE	This command was introduced.

## Usage Guidelines

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
<a href="#">channel-protocol</a>	Restricts the protocol used on a port to manage channeling.
<a href="#">interface port-channel</a>	Accesses or creates a port channel.
<a href="#">show etherchannel</a>	Displays EtherChannel information for a channel.
<a href="#">show lacp</a>	Displays LACP channel-group information.
<a href="#">show pagp</a>	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

<b>lacp</b>	Configures an EtherChannel with the Link Aggregation Control Protocol (LACP).
<b>pagp</b>	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 XE 3.3SE	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**

<b>Command</b>	<b>Description</b>
<a href="#">channel-group</a>	Assigns an Ethernet port to an EtherChannel group, or enables an EtherChannel mode, or both.
<a href="#">show etherchannel</a>	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 128.
<b>counters</b>	Clears traffic counters.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.3SE	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
<a href="#">show lacp</a>	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 128.
<b>counters</b>	Clears traffic counters.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.3SE	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
<a href="#">debug pagp</a>	Enables debugging of PAgP.
<a href="#">show pagp</a>	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

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

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.3SE	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
```

## Related Commands

Command	Description
<a href="#">clear spanning-tree detected-protocols</a>	Restarts the protocol migration process on the interface.
<a href="#">debug spanning-tree</a>	Enables debugging of spanning-tree activities.

# 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

<b>interface</b> <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 128.
--------------------------------------	--

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.3SE	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
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">clear spanning-tree detected-protocols</a>	Restarts the protocol migration process on the interface.
<a href="#">debug spanning-tree</a>	Enables debugging of spanning-tree activities.



# 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

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

## Command Default

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.3SE	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 active switch. To enable debugging on the standby switch, start a session from the active switch by using the **session switch-number** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the standby switch.

To enable debugging on the standby switch without first starting a session on the active switch, 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
<a href="#">show etherchannel</a>	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

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

## Command Default

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.3SE	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 active switch. To enable debugging on the standby switch, start a session from the active switch by using the **session switch-number** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the standby switch.

To enable debugging on the standby switch without first starting a session on the active switch, 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

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

## Command Default

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

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

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

To enable debugging on the standby switch without first starting a session on the active switch, 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 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| counters| errdisable| fec| if-numbers| l2-control| link-status| platform| pm-spi| pm-vectors [detail]| ses| vlans}

**no debug platform pm** {all| counters| errdisable| fec| if-numbers| l2-control| link-status| platform| pm-spi| pm-vectors [detail]| ses| vlans}

### Syntax Description

<b>all</b>	Displays all port manager debug messages.
<b>counters</b>	Displays counters for remote procedure call (RPC) debug messages.
<b>errdisable</b>	Displays error-disabled-related events debug messages.
<b>fec</b>	Displays forwarding equivalence class (FEC) platform-related events debug messages.
<b>if-numbers</b>	Displays interface-number translation event debug messages.
<b>l2-control</b>	Displays Layer 2 control infra debug messages.
<b>link-status</b>	Displays interface link-detection event debug messages.
<b>platform</b>	Displays port manager function event debug messages.
<b>pm-spi</b>	Displays port manager stateful packet inspection (SPI) event debug messages.
<b>pm-vectors</b>	Displays port manager vector-related event debug messages.
<b>detail</b>	(Optional) Displays vector-function details.
<b>ses</b>	Displays service expansion shelf (SES) related event debug messages.
<b>vlans</b>	Displays VLAN creation and deletion event debug messages.

### Command Default

Debugging is disabled.

### Command Modes

Privileged EXEC

**Command History**

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

**Usage Guidelines**

The **undebug 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 active switch. To enable debugging on the standby switch, start a session from the active switch by using the **session switch-number** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the standby switch.

To enable debugging on the standby switch without first starting a session on the active switch, 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
```

## 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** [**error**| **event**] [**switch** *switch-number*]

**no debug platform udd** [**error**| **event**] [**switch** *switch-number*]

### Syntax Description

<b>error</b>	(Optional) Displays error condition debug messages.
<b>event</b>	(Optional) Displays UDLD-related platform event debug messages.
<b>switch</b> <i>switch-number</i>	(Optional) Displays UDLD debug messages for the specified stack member.

### Command Default

Debugging is disabled.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
Cisco IOS XE 3.3SE	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 switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the active switch by using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the stack member.



## 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 | etherchannel | events | exceptions | general | ha | mstp | pvst+ | root | snmp | synchronization | switch | uplinkfast}

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

### Syntax Description

<b>all</b>	Displays all spanning-tree debug messages.
<b>backbonefast</b>	Displays BackboneFast-event debug messages.
<b>bpdu</b>	Displays spanning-tree bridge protocol data unit (BPDU) debug messages.
<b>bpdu-opt</b>	Displays optimized BPDU handling debug messages.
<b>config</b>	Displays spanning-tree configuration change debug messages.
<b>etherchannel</b>	Displays EtherChannel-support debug messages.
<b>events</b>	Displays spanning-tree topology event debug messages.
<b>exceptions</b>	Displays spanning-tree exception debug messages.
<b>general</b>	Displays general spanning-tree activity debug messages.
<b>ha</b>	Displays high-availability spanning-tree debug messages.
<b>mstp</b>	Debugs Multiple Spanning Tree Protocol (MSTP) events.
<b>pvst+</b>	Displays per-VLAN spanning-tree plus (PVST+) event debug messages.
<b>root</b>	Displays spanning-tree root-event debug messages.
<b>snmp</b>	Displays spanning-tree Simple Network Management Protocol (SNMP) handling debug messages.
<b>switch</b>	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.

<b>synchronization</b>	Displays the spanning-tree synchronization event debug messages.
<b>uplinkfast</b>	Displays UplinkFast-event debug messages.

**Command Default** Debugging is disabled.

**Command Modes** Privileged EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 3.3SE	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 active switch. To enable debugging on the standby switch, start a session from the active switch by using the **session switch-number** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the standby switch.

To enable debugging on the standby switch without first starting a session on the active switch, 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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">clear spanning-tree counters</a>	Clears spanning-tree counters.
	<a href="#">clear spanning-tree detected-protocols</a>	Restarts the protocol migration process on the interface.

# 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

<i>port-channel-number</i>	Channel group number. The range is 1 to 128.
----------------------------	--

## Command Default

No port channel logical interfaces are defined.

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE 3.3SE	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
<a href="#">channel-group</a>	Assigns an Ethernet port to an EtherChannel group, or enables an EtherChannel mode, or both.
<a href="#">show etherchannel</a>	Displays EtherChannel information for a channel.

# lACP max-bundle

To define the maximum number of active LACP ports allowed in a port channel, use the **lACP max-bundle** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

**lACP max-bundle** *max\_bundle\_number*

**no lACP max-bundle**

## Syntax Description

*max\_bundle\_number*

The maximum number of active LACP ports in the port channel. The range is 1 to 8. The default is 8.

## Command Default

None

## Command Modes

Interface configuration

## Command History

### Release

Cisco IOS XE 3.3SE

### Modification

This command was introduced.

## Usage Guidelines

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 hot-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.

The **lACP max-bundle** command must specify a number greater than the number specified by the **port-channel min-links** command.

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 specify a maximum of five active LACP ports in port channel 2:

```
Switch(config)# interface port-channel 2
Switch(config-if)# lACP max-bundle 5
```

## Related Commands

### Command

### Description

[port-channel min-links](#)

Specifies the minimum number of LACP ports that must be in the link-up state and bundled in the EtherChannel in order for the port channel to become active.

# 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 XE 3.3SE	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
<a href="#">channel-group</a>	Assigns an Ethernet port to an EtherChannel group, or enables an EtherChannel mode, or both.
<a href="#">lacp system-priority</a>	Configures the LACP system priority.
<a href="#">show lacp</a>	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 XE 3.3SE	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**

<b>Command</b>	<b>Description</b>
<a href="#">channel-group</a>	Assigns an Ethernet port to an EtherChannel group, or enables an EtherChannel mode, or both.
<a href="#">lacp port-priority</a>	Configures the port priority for the Link Aggregation Control Protocol (LACP).
<a href="#">show lacp</a>	Displays LACP channel-group information.

## 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

<b>aggregation-port</b>	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.
<b>physical-port</b>	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 XE 3.3SE	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
<a href="#">pagp port-priority</a>	Selects a port over which all traffic through the EtherChannel is sent.
<a href="#">show pagp</a>	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 XE 3.3SE	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**

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

## 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 mechanism to the default setting, use the **no** form of this command.

**port-channel load-balance** {**dst-ip**|**dst-mac**|**dst-mixed-ip-port**|**dst-port**|**extended**|**src-dst-ip**|**src-dst-mac**|**src-dst-mixed-ip-port**|**src-dst-port**|**src-ip**|**src-mac**|**src-mixed-ip-port**|**src-port**}

**no port-channel load-balance**

### Syntax Description

<b>dst-ip</b>	Specifies load distribution based on the destination host IP address.
<b>dst-mac</b>	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.
<b>dst-mixed-ip-port</b>	Specifies load distribution based on the destination IPv4 or IPv6 address and the TCP/UDP (Layer 4) port number.
<b>dst-port</b>	Specifies load distribution based on the destination TCP/UDP (Layer 4) port number for both IPv4 and IPv6.
<b>extended</b>	Sets extended load balance methods among the ports in the EtherChannel. See the <b>port-channel load-balance extended</b> command.
<b>src-dst-ip</b>	Specifies load distribution based on the source and destination host IP address.
<b>src-dst-mac</b>	Specifies load distribution based on the source and destination host MAC address.
<b>src-dst-mixed-ip-port</b>	Specifies load distribution based on the source and destination host IP address and TCP/UDP (layer 4) port number.
<b>src-dst-port</b>	Specifies load distribution based on the source and destination TCP/UDP (Layer 4) port number.
<b>src-ip</b>	Specifies load distribution based on the source host IP address.
<b>src-mac</b>	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.
<b>src-mixed-ip-port</b>	Specifies load distribution based on the source host IP address and TCP/UDP (Layer 4) port number.
<b>src-port</b>	Specifies load distribution based on the TCP/UDP (Layer 4) port number.

**Command Default** The default is **src-mac**.

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 3.3SE	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
```

## port-channel load-balance extended

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

**port-channel load-balance extended**[*dst-ip*| *dst-mac*| *dst-port*| *ipv6-label*| *l3-proto*| *src-ip*| *src-mac*| *src-port*]

**no port-channel load-balance extended**

### Syntax Description

<b>dst-ip</b>	(Optional) Specifies load distribution based on the destination host IP address.
<b>dst-mac</b>	(Optional) 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.
<b>dst-port</b>	(Optional) Specifies load distribution based on the destination TCP/UDP (Layer 4) port number for both IPv4 and IPv6.
<b>ipv6-label</b>	(Optional) Specifies load distribution based on the source MAC address and IPv6 flow label.
<b>l3-proto</b>	(Optional) Specifies load distribution based on the source MAC address and Layer 3 protocols.
<b>src-ip</b>	(Optional) Specifies load distribution based on the source host IP address.
<b>src-mac</b>	(Optional) 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.
<b>src-port</b>	(Optional) Specifies load distribution based on the TCP/UDP (Layer 4) port number.

### Command Default

The default is **src-mac**.

### Command Modes

Global configuration

### Command History

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



### Usage Guidelines

For information about when to use these forwarding methods, see the *Layer 2/3 Configuration Guide (Catalyst 3650 Switches)* for this release.

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 extended load-distribution method:

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

## port-channel min-links

To define the minimum number of LACP ports that must be bundled in the link-up state and bundled in the EtherChannel in order that a port channel becomes active, use the **port-channel min-links** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

**port-channel min-links** *min\_links\_number*

**no port-channel min-links**

<b>Syntax Description</b>	<i>min_links_number</i>	The minimum number of active LACP ports in the port channel. The range is 2 to 8. The default is 1.
---------------------------	-------------------------	---

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

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 3.3SE	This command was introduced.

**Usage Guidelines**

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 hot-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.

The **port-channel min-links** command must specify a number a less than the number specified by the **lacp max-bundle** command.

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 specify a minimum of three active LACP ports before port channel 2 becomes active:

```
Switch(config)# interface port-channel 2
Switch(config-if)# port-channel min-links 3
```

**Related Commands**

Command	Description
<a href="#">lacp max-bundle</a>	Specifies the maximum number of LACP ports allowed in a port channel.

# 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** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**]

## Syntax Description

<i>channel-group-number</i>	(Optional) Channel group number. The range is 1 to 128.
<b>detail</b>	(Optional) Displays detailed EtherChannel information.
<b>load-balance</b>	(Optional) Displays the load-balance or frame-distribution scheme among ports in the port channel.
<b>port</b>	(Optional) Displays EtherChannel port information.
<b>port-channel</b>	(Optional) Displays port-channel information.
<b>protocol</b>	(Optional) Displays the protocol that is being used in the channel.
<b>summary</b>	(Optional) Displays a one-line summary per channel group.

## Command Default

None

## Command Modes

User EXEC

## Command History

Release	Modification
Cisco IOS XE 3.3SE	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
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 = Pol
Port index    =          OLoad = 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
          |      |      |      |      |      |      |
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
<a href="#">channel-group</a>	Assigns an Ethernet port to an EtherChannel group, or enables an EtherChannel mode, or both.
<a href="#">channel-protocol</a>	Restricts the protocol used on a port to manage channeling.
<a href="#">interface port-channel</a>	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 128.
<b>counters</b>	Displays traffic information.
<b>internal</b>	Displays internal information.
<b>neighbor</b>	Displays neighbor information.
<b>sys-id</b>	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 XE 3.3SE	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's      Marker      Marker Response      LACPDU's
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
LACPDU's 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.
LACPDU's 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 LACPDU's
       F - Device is requesting Fast LACPDU's
       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"> <li>• <b>--</b>—Port is in an unknown state.</li> <li>• <b>bndl</b>—Port is attached to an aggregator and bundled with other ports.</li> <li>• <b>susp</b>—Port is in a suspended state; it is not attached to any aggregator.</li> <li>• <b>hot-sby</b>—Port is in a hot-standby state.</li> <li>• <b>indiv</b>—Port is incapable of bundling with any other port.</li> <li>• <b>indep</b>—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).</li> <li>• <b>down</b>—Port is down.</li> </ul>
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"> <li>• bit0: LACP_Activity</li> <li>• bit1: LACP_Timeout</li> <li>• bit2: Aggregation</li> <li>• bit3: Synchronization</li> <li>• bit4: Collecting</li> <li>• bit5: Distributing</li> <li>• bit6: Defaulted</li> <li>• bit7: Expired</li> </ul> <p><b>Note</b> 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**

<b>Command</b>	<b>Description</b>
<a href="#">clear lacp</a>	Clears the LACP channel-group information.
<a href="#">lacp port-priority</a>	Configures the port priority for the Link Aggregation Control Protocol (LACP).
<a href="#">lacp system-priority</a>	Configures the LACP system priority.

# 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 128.
<b>counters</b>	Displays traffic information.
<b>dual-active</b>	Displays the dual-active status.
<b>internal</b>	Displays internal information.
<b>neighbor</b>	Displays neighbor information.

## Command Default

None

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.3SE	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      Partner      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
<a href="#">clear pagp</a>	Clears PAgP channel-group information.

# show platform etherchannel

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

**show platform etherchannel** *channel-group-number* {**group-mask** | **load-balance mac** *src-mac dst-mac* [**ip** *src-ip dst-ip* [**port** *src-port dst-port*]]} [**switch** *switch-number*]

## Syntax Description

<i>channel-group-number</i>	Channel group number. The range is 1 to 128.
<b>group-mask</b>	Displays EtherChannel group mask.
<b>load-balance</b>	Tests EtherChannel load-balance hash algorithm.
<b>mac</b> <i>src-mac dst-mac</i>	Specifies the source and destination MAC addresses.
<b>ip</b> <i>src-ip dst-ip</i>	(Optional) Specifies the source and destination IP addresses.
<b>port</b> <i>src-port dst-port</i>	(Optional) Specifies the source and destination layer port numbers.
<b>switch</b> <i>switch-number</i>	(Optional) Specifies the stack member.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.3SE	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 {etherchannel channel-group-number group-mask| interface-numbers| port-data
interface-id| port-state| spi-info| spi-req-q}
```

## Syntax Description

<b>etherchannel</b> <i>channel-group-number</i> <b>group-mask</b>	Displays the EtherChannel group-mask table for the specified channel group. The range is 1 to 128.
<b>interface-numbers</b>	Displays interface numbers information.
<b>port-data</b> <i>interface-id</i>	Displays port data information for the specified interface.
<b>port-state</b>	Displays port state information.
<b>spi-info</b>	Displays stateful packet inspection (SPI) information.
<b>spi-req-q</b>	Displays stateful packet inspection (SPI) maximum wait time for acknowledgment.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.3SE	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 udd

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

**show udd** [**Auto-Template** | **Capwap** | **GigabitEthernet** | **GroupVI** | **InternalInterface** | **Loopback** | **Null** | **Port-channel** | **TenGigabitEthernet** | **Tunnel** | **Vlan**] *interface\_number*

**show udd neighbors**

## Syntax Description

<b>Auto-Template</b>	(Optional) Displays UDLD operational status of the auto-template interface. The range is from 1 to 999.
<b>Capwap</b>	(Optional) Displays UDLD operational status of the CAPWAP interface. The range is from 0 to 2147483647.
<b>GigabitEthernet</b>	(Optional) Displays UDLD operational status of the GigabitEthernet interface. The range is from 0 to 9.
<b>GroupVI</b>	(Optional) Displays UDLD operational status of the group virtual interface. The range is from 1 to 255.
<b>InternalInterface</b>	(Optional) Displays UDLD operational status of the internal interface. The range is from 0 to 9.
<b>Loopback</b>	(Optional) Displays UDLD operational status of the loopback interface. The range is from 0 to 2147483647.
<b>Null</b>	(Optional) Displays UDLD operational status of the null interface.
<b>Port-channel</b>	(Optional) Displays UDLD operational status of the Ethernet channel interfaces. The range is from 1 to 128.
<b>TenGigabitEthernet</b>	(Optional) Displays UDLD operational status of the Ten Gigabit Ethernet interface. The range is from 0 to 9.
<b>Tunnel</b>	(Optional) Displays UDLD operational status of the tunnel interface. The range is from 0 to 2147483647.
<b>Vlan</b>	(Optional) Displays UDLD operational status of the VLAN interface. The range is from 1 to 4095.
<i>interface-id</i>	(Optional) ID of the interface and port number. Valid interfaces include physical ports, VLANs, and port channels.
<b>neighbors</b>	(Optional) Displays neighbor information only.



**Command Default** None

**Command Modes** User EXEC

Command History	Release	Modification
	Cisco IOS XE 3.3SE	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 udld 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 udld 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 udld 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.

Field	Description
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.
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.

Field	Description
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 uddl neighbors** command:

```
Switch# show uddl 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
<a href="#">uddl</a>	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
<a href="#">uddl port</a>	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the <b>uddl</b> global configuration command.
<a href="#">uddl reset</a>	Resets all interfaces shut down by UDLD and permits traffic to pass through again.

# switchport

To put an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration, use the **switchport** command in interface configuration mode. To put an interface in Layer 3 mode, use the **no** form of this command.

**switchport**

**no switchport**

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

**Command Default** By default, all interfaces are in Layer 2 mode.

**Command Modes** Interface configuration

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

**Usage Guidelines** Use the **no switchport** command (without parameters) to set the interface to the routed-interface status and to erase all Layer 2 configurations. You must use this command before assigning an IP address to a routed port.



**Note** This command is not supported on switches running the LAN Base feature set.

Entering the **no switchport** command shuts the port down and then reenables it, which might generate messages on the device to which the port is connected.

When you put an interface that is in Layer 2 mode into Layer 3 mode (or the reverse), the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration.



**Note** If an interface is configured as a Layer 3 interface, you must first enter the **switchport** command to configure the interface as a Layer 2 port. Then you can enter the **switchport access vlan** and **switchport mode** commands.

The **switchport** command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2-switched interfaces.

You can verify the port status of an interface by entering the **show running-config** privileged EXEC command.

## Examples

This example shows how to cause an interface to cease operating as a Layer 2 port and become a Cisco-routed port:

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

This example shows how to cause the port interface to cease operating as a Cisco-routed port and convert to a Layer 2 switched interface:

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

# switchport access vlan

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

**switchport access vlan** *vlan-id*

**no switchport access vlan**

## Syntax Description

<i>vlan-id</i>	VLAN ID of the access mode VLAN; the range is 1 to 4094.
----------------	--

## Command Default

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

## Command Modes

Interface configuration

## Command History

Release	Modification
Cisco IOS XE 3.3SE	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. 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.

## 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
<a href="#">switchport mode</a>	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| dynamic | {auto| desirable}| trunk}
```

```
noswitchport mode {access| dynamic | {auto| desirable}| trunk}
```

## Syntax Description

<b>access</b>	Sets the port to access mode (either static-access or dynamic-access depending on the setting of the <b>switchport access vlan</b> 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.
<b>dynamic auto</b>	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.
<b>dynamic desirable</b>	Sets the port trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link.
<b>trunk</b>	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 XE 3.3SE	This command was introduced.

## Usage Guidelines

### Note

Although visible in the CLI, the **dot1q-tunnel** keyword is not supported.

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 problem, 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.

Access ports and trunk ports are mutually exclusive.

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
```



**Related Commands**

Command	Description
<a href="#">switchport access vlan</a>	Configures a port as a static-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 arguments or keywords.

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

**Command Modes** Interface configuration

Command History	Release	Modification
	Cisco IOS XE 3.3SE	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
<a href="#">switchport mode</a>	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

<b>aggressive</b>	Enables UDLD in aggressive mode on all fiber-optic interfaces.
<b>enable</b>	Enables UDLD in normal mode on all fiber-optic interfaces.
<b>message time</b> <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 XE 3.3SE	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*, and *Layer 2/3 Configuration Guide (Catalyst 3650 Switches)*.

If you change the message time between probe packets, you are making a compromise 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
<a href="#">show udld</a>	Displays UDLD administrative and operational status for all ports or the specified port.
<a href="#">udld port</a>	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the <b>udld</b> global configuration command.
<a href="#">udld reset</a>	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

<b>aggressive</b>	(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 XE 3.3SE	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 a 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
<a href="#">show udld</a>	Displays UDLD administrative and operational status for all ports or the specified port.
<a href="#">udld</a>	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
<a href="#">udld reset</a>	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 arguments or keywords.

**Command Default** None

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.3SE	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
	<a href="#">show udld</a>	Displays UDLD administrative and operational status for all ports or the specified port.
	<a href="#">udld</a>	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
	<a href="#">udld port</a>	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the <b>udld</b> global configuration command.





## INDEX

### C

channel-group command [15](#)  
channel-protocol command [18](#)  
clear lacp command [20](#)  
clear pagp command [21](#)  
clear spanning-tree counters command [22](#)  
clear spanning-tree detected-protocols command [23](#)

### D

debug etherchannel command [25](#)  
debug lacp command [27](#)  
debug pagp command [28](#)  
debug platform pm command [30](#)  
debug platform udd command [32](#)  
debug spanning-tree command [33](#)

### I

interface port-channel command [35](#)

### L

lacp max-bundle command [37](#)  
lacp port-priority command [38](#)  
lacp system-priority command [40](#)

### P

pagp learn-method command [42](#)  
pagp port-priority command [44](#)  
port-channel load-balance command [46](#)  
port-channel load-balance extended command [48](#)  
port-channel min-links command [50](#)

### S

show etherchannel command [52](#)  
show lacp command [55](#)  
show pagp command [60](#)  
show platform etherchannel command [62](#)  
show platform pm command [63](#)  
show udd command [64](#)  
switchport access vlan command [70](#)  
switchport command [68](#)  
switchport mode command [71](#)  
switchport nonegotiate command [74](#)

### U

udd command [76](#)  
udd port command [78](#)  
udd reset command [80](#)

