



## **Cisco Nexus 3548 Switch NX-OS Interfaces Command Reference**

First Published: April 2011

Last Modified: May 2016

**Cisco Systems, Inc.**

[www.cisco.com](http://www.cisco.com)

Cisco has more than 200 offices worldwide.  
Addresses, phone numbers, and fax numbers  
are listed on the Cisco website at  
[www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Text Part Number: OL-27846-02

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

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

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

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

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

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: [www.cisco.com/go/trademarks](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. (1721R)

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 Nexus 3548 Switch NX-OS Interfaces Command Reference*  
© 2016 Cisco Systems, Inc. All rights reserved.



<b>Preface</b>	<b>1</b>
Audience	1
Document Conventions	1
Related Documentation	2
Documentation Feedback	3
Obtaining Documentation and Submitting a Service Request	1-3
	3
<b>New and Changed Information</b>	<b>1-9</b>
<b>Interfaces Commands</b>	<b>1-1</b>
address (NAT pool)	1-2
bandwidth (interface)	1-3
channel-group (Ethernet)	1-5
cdp enable	1-8
clear ip nat translation	1-9
copy running-config startup-config	1-11
delay (interface)	1-12
delay restore	1-13
description (interface)	1-14
dual-active exclude interface-vlan	1-15
encapsulation dot1Q	1-17
feature vpc	1-18
interface ethernet	1-19
interface ethernet (Layer 3)	1-20
interface loopback	1-22
interface port-channel	1-23
interface vlan	1-25
ip nat	1-26
ip nat inside source list	1-27
ip nat inside source static	1-29
ip nat outside source list	1-31

ip nat outside source static	1-33
ip nat pool	1-35
ip nat translation	1-37
lacp min-links	1-39
lacp port-priority	1-40
lacp rate fast	1-41
lacp system-priority	1-43
lldp (interface)	1-44
no switchport	1-45
peer-keepalive	1-47
port-channel load-balance ethernet	1-50
role	1-52
show interface brief	1-54
show interface capabilities	1-55
show interface debounce	1-57
show interface ethernet	1-58
show interface loopback	1-61
show interface port-channel	1-64
show interface mac-address	1-66
show interface status err-disabled	1-68
show interface switchport	1-69
show interface transceiver	1-70
show ip nat translation	1-72
show lacp	1-74
show module	1-76
show port-channel capacity	1-77
show port-channel compatibility-parameters	1-78
show port-channel database	1-79
show port-channel load-balance	1-80
show port-channel summary	1-82
show port-channel traffic	1-83
show port-channel usage	1-84
show resource	1-85
show running-config interface	1-86
show running-config nat	1-87

show tech-support port-channel	1-88
show version	1-90
show vpc brief	1-92
show vpc consistency-parameters	1-94
show vpc orphan-ports	1-96
show vpc peer-keepalive	1-97
show vpc role	1-99
show vpc statistics	1-101
shutdown	1-103
speed (Ethernet)	1-105
switchport host	1-107
switchport mode	1-108
switchport trunk allowed vlan	1-110
ttag	1-112
ttag-marker	1-113
ttag-marker-interval	1-115
udld (configuration mode)	1-116
udld (Ethernet)	1-118
vpc	1-120
vpc domain	1-122
vpc peer-link	1-124





# Preface

---

This preface describes the audience, organization, and conventions of the *Cisco Nexus 3548 Switch NX-OS Interfaces Command Reference*. It also provides information on how to obtain related documentation.

This preface includes the following sections:

- [Audience, page 1](#)
- [Document Conventions, page 1](#)
- [Related Documentation, page 2](#)
- [Documentation Feedback, page 3](#)
- [Obtain Documentation and Submit a Service Request, page 3](#)

## Audience

This publication is for experienced network administrators who configure and maintain Cisco Nexus Series switches.

## Document Conventions

Command descriptions use these conventions:

Convention	Description
boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
[ x   y   z ]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use these conventions:

<code>screen font</code>	Terminal sessions and information that the switch displays are in screen font.
<b>boldface screen font</b>	Information that you must enter is in boldface screen font.
<i>italic screen font</i>	Arguments for which you supply values are in italic screen font.
< >	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.

This document uses the following conventions:



#### Note

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



#### Caution

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

## Related Documentation

Documentation for the Cisco Nexus 3000 Series Switch is available at the following URL:

[http://www.cisco.com/en/US/products/ps11541/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html)

The documentation set is divided into the following categories:

### Release Notes

The release notes are available at the following URL:

[http://www.cisco.com/en/US/products/ps11541/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps11541/prod_release_notes_list.html)

### Installation and Upgrade Guides

The installation and upgrade guides are available at the following URL:

[http://www.cisco.com/en/US/products/ps11541/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps11541/prod_installation_guides_list.html)

### Command References

The command references are available at the following URL:

[http://www.cisco.com/en/US/products/ps11541/prod\\_command\\_reference\\_list.html](http://www.cisco.com/en/US/products/ps11541/prod_command_reference_list.html)

### Technical References

The technical references are available at the following URL:

[http://www.cisco.com/en/US/products/ps11541/prod\\_technical\\_reference\\_list.html](http://www.cisco.com/en/US/products/ps11541/prod_technical_reference_list.html)



### Configuration Guides

The configuration guides are available at the following URL:

[http://www.cisco.com/en/US/products/ps11541/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps11541/products_installation_and_configuration_guides_list.html)

### Error and System Messages

The system message reference guide is available at the following URL:

[http://www.cisco.com/en/US/products/ps11541/products\\_system\\_message\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps11541/products_system_message_guides_list.html)

## Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to [nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com). We appreciate your feedback.

## Obtain Documentation and Submit a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *[What's New in Cisco Product Documentation](#)*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#). The RSS feeds are a free service.





## New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Nexus 3548 Switch NX-OS Interfaces Command Reference*. The latest version of this document is available at the following Cisco website:

[http://www.cisco.com/en/US/products/ps11541/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html)

To check for additional information about this Cisco NX-OS Release, see the *Cisco Nexus 3000 Series Switch Release Notes* available at the following Cisco website:

[http://www.cisco.com/en/US/products/ps11541/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps11541/prod_release_notes_list.html)

**Table 1** summarizes the new and changed features for Cisco NX-OS Release 6.x and tells you where they are documented.

**Table 1** *New and Changed Information for Release 6.x*

Feature	Description	Changed in Release	Where Documented
ttag Marker	Added support for ttag marker.	6.0(2)A8(1)	<a href="#">ttag</a> <a href="#">ttag-marker</a> <a href="#">ttag-marker-interval</a>
Twice NAT	This feature was introduced.	6.0(2)A4(1)	<a href="#">ip nat inside source list</a> <a href="#">ip nat inside source static</a> <a href="#">ip nat outside source list</a> <a href="#">ip nat outside source static</a>
TCP State Enhancements	<b>syn-timeout</b> and <b>finrst-timeout</b> timers were introduced.	6.0(2)A4(1)	<a href="#">ip nat translation</a>

Table 1 New and Changed Information for Release 6.x (continued)

Feature	Description	Changed in Release	Where Documented
Virtual Port Channel	This feature was introduced.	6.0(2)A3(1)	<a href="#">delay restore</a> <a href="#">dual-active exclude interface-vlan</a> <a href="#">feature vpc</a> <a href="#">peer-keepalive</a> <a href="#">role</a> <a href="#">show vpc brief</a> <a href="#">show vpc consistency-parameters</a> <a href="#">show vpc orphan-ports</a> <a href="#">show vpc peer-keepalive</a> <a href="#">show vpc role</a> <a href="#">show vpc statistics</a> <a href="#">vpc</a> <a href="#">vpc domain</a> <a href="#">vpc peer-link</a>
Dynamic NAT Pool	This feature was introduced.	6.0(2)A3(1)	<a href="#">address (NAT pool)</a> <a href="#">ip nat inside source list</a> <a href="#">ip nat outside source list</a> <a href="#">ip nat outside source static</a>
Switchport Trunks	Default behavior of switchport trunkallowed vlans command changed.	6.0(2)A1(1)	<a href="#">switchport trunk allowed vlan</a>
4x10G Interface Port	This feature was introduced.	6.0(2)A1(1)	<a href="#">speed (Ethernet)</a>
Dynamic NAT	This feature was introduced.	6.0(2)A1(1)	<a href="#">clear ip nat translation</a> <a href="#">ip nat</a> <a href="#">ip nat inside source list</a> <a href="#">ip nat translation</a>



# Interfaces Commands

---

This chapter describes the Cisco NX-OS interfaces commands available on the Cisco Nexus 3548 switches.



## Note

---

The internal CLI commands are not supported on the Cisco Nexus Series switches.

---

## address (NAT pool)

To define a range of IP addresses for a dynamic NAT pool, use the **address** command. To remove a defined range of IP addresses, use the **no** form of this command.

**address** *startip endip*

**no address** *startip endip*

<b>Syntax Description</b>	<i>startip</i>	Specifies the starting IP address for the range of addresses in the pool.
	<i>endip</i>	Specifies the ending IP address for the range of addresses in the pool.

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

<b>Command Modes</b>	NAT pool configuration mode
----------------------	-----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	6.0(2)A31)	This command was introduced.

<b>Usage Guidelines</b>	<p>You can create a NAT pool by either defining the range of IP addresses in a single <b>ip nat pool</b> command or by using the <b>ip nat pool</b> and <b>address</b> commands.</p>
-------------------------	--

Dynamic NAT allows the configuration of a pool of global addresses that can be used to dynamically allocate global address from the pool for every new translation. The addresses are returned to the pool after the session ages out or is closed. This allows for a more efficient use of addresses based on requirements.

Support for PAT includes the use of the global address pool. This further optimizes IP address utilization. PAT exhausts one IP address at a time with the use of port numbers. If no port is available from the appropriate group and more than one IP address is configured, PAT moves to the next IP address and tries to allocate the original source port again. This process continues until PAT runs out of available ports and IP addresses.

<b>Examples</b>	<p>This example shows how to create a NAT pool and define the range of global IP addresses using the <b>ip nat pool</b> and <b>address</b> commands:</p>
-----------------	--

```
switch# configure terminal
switch(config)# ip nat pool pool17 netmask 255.255.0.0
switch(config-ipnat-pool)# address 40.1.1.1 40.1.1.5
switch(config-ipnat-pool)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip nat pool</b>	Creates a dynamic NAT pool of global IP addresses.

# bandwidth (interface)

To set the inherited and received bandwidth values for an interface, use the **bandwidth** command. To restore the default values, use the **no** form of this command.

**bandwidth** {*kbps* | **inherit** [*kbps*]}

**no bandwidth** {*kbps* | **inherit** [*kbps*]}

Syntax Description	<i>kbps</i>	Informational bandwidth in kilobits per second. Valid values are from 1 to 10000000.
	<b>inherit</b>	(Optional) Specifies that the bandwidth be inherited from the parent interface.

Command Default	1000000 kbps
-----------------	--------------

Command Modes	Interface configuration mode Subinterface configuration mode
---------------	---

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

The **bandwidth** command sets an informational parameter to communicate only the current bandwidth to the higher-level protocols; you cannot adjust the actual bandwidth of an interface using this command.

The **bandwidth inherit** command controls how a subinterface inherits the bandwidth of its main interface.

The **no bandwidth inherit** command enables all subinterfaces to inherit the default bandwidth of the main interface, regardless of the configured bandwidth. If a bandwidth is not configured on a subinterface, and you use the **bandwidth inherit** command, all subinterfaces will inherit the current bandwidth of the main interface. If you configure a new bandwidth on the main interface, all subinterfaces will use this new value.

If you do not configure a bandwidth on the subinterface and you configure the bandwidth inherit command on the main interface, the subinterfaces will inherit the specified bandwidth.

In all cases, if an interface has an explicit bandwidth setting configured, then that interface will use that setting, regardless of whether the bandwidth inheritance setting is in effect.

This command does not require a license.

Examples	This example shows how to configure the bandwidth for a Layer 2 interface:
----------	--

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# bandwidth 1000
```

```
switch(config-if)#
```

This example shows how to configure subinterfaces to inherit the bandwidth from the parent routed interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# bandwidth inherit 30000
switch(config-if)# interface ethernet 1/1.1
switch(config-subif)#
```

---

**Related Commands**

Command	Description
<b>show interface</b>	Displays the interface configuration information.

---



## channel-group (Ethernet)

To assign and configure a physical interface to an EtherChannel, use the **channel-group** command. To remove the channel group configuration from the interface, use the **no** form of this command.

**channel-group** *number* [**force**] [**mode** { **active** | **on** | **passive** }]

**no channel-group** [*number*]

Syntax Description	<i>number</i>	Number of channel group. The <i>number</i> range is from 1 to 4096. Cisco NX-OS creates the EtherChannel associated with this channel group if the EtherChannel does not already exist.
	<b>force</b>	(Optional) Specifies that the LAN port be forcefully added to the channel group.
	<b>mode</b>	(Optional) Specifies the EtherChannel mode of the interface.
	<b>active</b>	Specifies that when you enable the Link Aggregation Control Protocol (LACP), this command enables LACP on the specified interface. The interface is in an active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets.
	<b>on</b>	<p>This is the default channel mode. Specifies that all EtherChannels that are not running LACP remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the switch returns an error message.</p> <p>After you enable LACP globally, by using the <b>feature lacp</b> command, you enable LACP on each channel by configuring the channel mode as either active or passive. An interface in this mode does not initiate or respond to LACP packets. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the channel group.</p> <p>The default mode is <b>on</b>.</p>
	<b>passive</b>	Specifies that when you enable LACP, this command enables LACP only if an LACP device is detected. The interface is in a passive negotiation state, in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.

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

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

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

**Usage Guidelines**

Use this command to create a channel group that includes the interface that you are working on and to add or remove specific interfaces from the channel group. Use this command to move a port from one channel group to another. You enter the channel group that you want the port to move to; the switch automatically removes the specified port from its present channel group and adds it to the specified channel group.

Use the **force** keyword to force the addition of the interface into the specified channel group.

After you enable LACP globally, by using the **feature lacp** command, you enable LACP on each channel by configuring the channel mode as either **active** or **passive**. An EtherChannel in the **on** channel mode is a pure EtherChannel and can aggregate a maximum of eight ports. The EtherChannel does not run LACP.

You cannot change the mode for an existing EtherChannel or any of its interfaces if that EtherChannel is not running LACP; the channel mode remains as **on**. The system returns an error message if you attempt to change the mode.

Use the **no** form of this command to remove the physical interface from the EtherChannel. When you delete the last physical interface from an EtherChannel, the EtherChannel remains. To delete the EtherChannel completely, use the **no** form of the **interface port-channel** command.

The compatibility check includes the following operational attributes:

- Port mode
- Access VLAN
- Trunk native VLAN
- Tagged or untagged
- Allowed VLAN list
- Switched Port Analyzer (SPAN) (cannot be SPAN source or destination port)
- Storm control

Use the **show port-channel compatibility-parameters** command to see the full list of compatibility checks that Cisco NX-OS uses.

You can only add interfaces configured with the channel mode set to **on** for static EtherChannels, that is, without a configured aggregation protocol. You can only add interfaces configured with the channel mode as **active** or **passive** to EtherChannels that are running LACP.

You can configure these attributes on an individual member port. If you configure a member port with an incompatible attribute, Cisco NX-OS suspends that port in the EtherChannel.

When the interface joins an EtherChannel, some of its individual parameters are overridden with the values on the EtherChannel, as follows:

- MAC address
- Spanning Tree Protocol (STP)
- Service policy
- Quality of service (QoS)
- Access control lists (ACLs)

Interface parameters, such as the following, remain unaffected when the interface joins or leaves a EtherChannel:

- Description
- Cisco Discovery Protocol (CDP)

- LACP port priority
- Debounce
- Rate mode
- Shutdown
- SNMP trap

If interfaces are configured for the EtherChannel interface and a member port is removed from the EtherChannel, the configuration of the EtherChannel interface is not propagated to the member ports.

Any configuration changes that you make in any of the compatibility parameters to the EtherChannel interface are propagated to all interfaces within the same channel group as the EtherChannel (for example, configuration changes are also propagated to the physical interfaces that are not part of the EtherChannel but are part of the channel group).

This command does not require a license.

### Examples

This example shows how to add an interface to LACP channel group 5 in active mode:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# channel-group 5 mode active
switch(config-if)#
```

This example shows how to forcefully add an interface to the channel group 5:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# channel-group 5 force
switch(config-if)#
```

### Related Commands

Command	Description
<b>show interface port-channel</b>	Displays information about the traffic on the specified EtherChannel interface.
<b>show lacp</b>	Displays LACP information.
<b>show port-channel summary</b>	Displays information on the EtherChannels.

# cdp enable

To enable the Cisco Discovery Protocol (CDP) on an Ethernet interface, use the **cdp enable** command. To disable CDP on the interface, use the **no** form of this command.

**cdp enable**  
**no cdp enable**

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

**Command Default** None

**Command Modes** Interface configuration mode

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

**Examples** This example shows how to enable CDP on an Ethernet interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# cdp enable
switch(config-if)#
```

Related Commands	Command	Description
	show interface	Displays the interface configuration information.

# clear ip nat translation

To clear dynamic Network Address Translation (NAT) translations from the translation table, use the **clear ip nat translation** command in EXEC mode.

**clear ip nat translation** {**all** | **inside** *global-ip local-ip* [**outside** *local-ip global-ip*] | **outside** *local-ip global-ip*}

## Syntax Description

<b>all</b>	Clears all dynamic translations.
<b>inside</b>	Clears inside translations that contain the specified <i>global-ip</i> and <i>local-ip</i> addresses.
<i>global-ip</i>	Global IP address.
<i>local-ip</i>	Local IP address.
<b>outside</b>	Clears outside translations that contain the specified <i>local-ip</i> and <i>global-ip</i> addresses.

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
6.0(2)A1(1)	This command was introduced.

## Examples

This example shows how to clear entries from the translation table before they time out:

```
switch# show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
udp 1.1.1.2:65372      5.5.5.1:6118      1.1.1.1:161        1.1.1.1:161
udp 1.1.1.2:65390      5.5.5.1:6119      1.1.1.1:161        1.1.1.1:161
any 11.11.1.2          183.1.1.2         ---                ---
any 11.11.1.3          183.1.1.3         ---                ---
any 11.11.2.3          183.1.2.3         ---                ---
any 11.11.2.4          183.1.2.4         ---                ---

switch# clear ip nat translation inside 1.1.1.2 5.5.5.1 outside 1.1.1.1 1.1.1.1
.Done
switch# show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
any 11.11.1.2          183.1.1.2         ---                ---
any 11.11.1.3          183.1.1.3         ---                ---
any 11.11.2.3          183.1.2.3         ---                ---
any 11.11.2.4          183.1.2.4         ---                ---
switch#
```

Related Commands	Command	Description
	<b>ip nat</b>	Designates that traffic originating from or destined for the interface is subject to NAT.
	<b>ip nat inside source list</b>	Enables dynamic NAT of the inside source address by using an ACL.
	<b>show ip nat translations</b>	Displays active NAT translations.

# copy running-config startup-config

To save the running configuration to the startup configuration file so that all current configuration details are available after a reboot, use the **copy running-config startup-config** command.

## copy running-config startup-config

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

**Command Default** None

**Command Modes** EXEC mode

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

**Usage Guidelines** To view the changes to the configuration that you have made, use the **show startup-config** command.



Note

Once you enter the **copy running-config startup-config** command, the running and the startup copies of the configuration are identical.

**Examples** This example shows how to save the running configuration to the startup configuration:

```
switch# copy running-config startup-config
[#####] 100%
switch#
```

Related Commands	Command	Description
	<b>show running-config</b>	Displays the currently running configuration.
	<b>show startup-config</b>	Displays the startup configuration file.

# delay (interface)

To set a delay value for an interface, use the **delay** command. To restore the default delay value, use the **no** form of this command.

**delay** *tens-of-microseconds*

**no delay**

Syntax Description	<i>tens-of-microseconds</i>	Throughput delay in tens of microseconds. The range is from 1 to 16,777,215.
--------------------	-----------------------------	--

Command Default	10 microseconds
-----------------	-----------------

Command Modes	Interface configuration mode Subinterface configuration mode
---------------	---

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

**Examples** This example shows how to set a delay of 30,000 microseconds on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# delay 30000
switch(config-if)#
```

This example shows how to set a delay of 1000 microseconds on a subinterface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1.1
switch(config-subif)# delay 1000
switch(config-subif)#
```

Related Commands	Command	Description
	<b>interface ethernet (Layer 3)</b>	Configures an Ethernet routed interface.
	<b>show interface</b>	Displays the interface configuration information.



# delay restore

To delay the virtual port channel (vPC) from coming up on the restored vPC peer device after a reload when the peer adjacency is already established, use the **delay restore** command. To revert to the default delay value, use the **no** form of this command.

**delay restore** *time*

**no delay restore**

Syntax Description	<i>time</i>	Number of seconds to delay bringing up the restored vPC peer device. The range is from 1 to 3600.
--------------------	-------------	---

Command Default	30 seconds
-----------------	------------

Command Modes	vPC domain configuration mode
---------------	-------------------------------

Command History	Release	Modification
	6.0(2)A3(1)	This command was introduced.

Usage Guidelines	Use the <b>delay restore</b> command to avoid upstream traffic from the access device to the core from being dropped when you restore the vPC peer devices.  This command does not require a license.
------------------	---

Examples	This example shows how to configure the delay reload time for a vPC link:
----------	---

```
switch(config)# vpc domain 1
switch(config-vpc-domain)# delay restore 10
switch(config-vpc-domain)#
```

This example shows how to remove the reload time configuration for a vPC link:

```
switch(config)# vpc domain 1
switch(config-vpc-domain)# no delay restore
switch(config-vpc-domain)#
```

Related Commands	Command	Description
	<b>show vpc</b>	Displays the vPC configuration.

# description (interface)

To add a description to an interface configuration, use the **description** command. To remove the description, use the **no** form of this command.

**description** *description*

**no description**

<b>Syntax Description</b>	<i>description</i>	String description of the interface configuration. This string is limited to 80 characters.
---------------------------	--------------------	---

<b>Command Default</b>	No description is added.
------------------------	--------------------------

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

<b>Command History</b>	Release	Modification
	5.0(3)A1(1)	This command was introduced.

<b>Usage Guidelines</b>	<p>The <b>description</b> command is meant to provide a reminder in the configuration to describe what certain interfaces are used for. The description appears in the output of the following commands such as <b>show interface</b> and <b>show running-config</b>.</p> <p>This command does not require a license.</p>
-------------------------	---

<b>Examples</b>	This example shows how to add a description for an interface:
-----------------	---

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# description "10G Server Link"
switch(config-if)#
```

<b>Related Commands</b>	Command	Description
	<b>show interface ethernet</b>	Displays the interface configuration information.
	<b>show running-config</b>	Displays the contents of the currently running configuration file.

## dual-active exclude interface-vlan

To ensure that certain VLAN interfaces are not shut down on the virtual port-channel (vPC) secondary peer device when the vPC peer link fails for those VLANs carried on the vPC peer link but not on the vPC configuration itself, use the **dual-active exclude interface-vlan** command. To return to the default value, use the **no** form of this command.

**dual-active exclude interface-vlan** {*range*}

**no dual-active exclude interface-vlan**

<b>Syntax Description</b>	<i>range</i>	Range of VLAN interfaces that you want to exclude from shutting down. The allowed VLAN range is from 1 to 3967 and 4048 to 4093.
---------------------------	--------------	--

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

<b>Command Modes</b>	vPC domain configuration mode
----------------------	-------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	6.0(2)A3(1)	This command was introduced.

<b>Usage Guidelines</b>	The VLAN interfaces must have already been configured. This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to configure the device to keep the VLAN interfaces up on the vPC peer devices if the peer link fails:
-----------------	---

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# dual-active exclude interface-vlan 10
switch(config-vpc-domain)#
```

This example shows how to restore the default configuration on the vPC peer devices if the peer link fails:

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# no dual-active exclude interface-vlan
switch(config-vpc-domain)#
```

Related Commands	Command	Description
	<b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.
	<b>show vpc</b>	Displays vPC configuration information.

# encapsulation dot1Q

To enable IEEE 802.1Q encapsulation of traffic on a specified subinterface, use the **encapsulation dot1q** command. To disable encapsulation, use the **no** form of this command.

**encapsulation dot1Q** *vlan-id*

**no encapsulation dot1Q** *vlan-id*

<b>Syntax Description</b>	<i>vlan-id</i>	VLAN to set when the interface is in access mode; valid values are from 1 to 4093, except for the VLANs reserved for internal switch use.
---------------------------	----------------	---

<b>Command Default</b>	No encapsulation
------------------------	------------------

<b>Command Modes</b>	Subinterface configuration mode
----------------------	---------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

<b>Usage Guidelines</b>	IEEE 802.1Q encapsulation is configurable on Ethernet and EtherChannel interfaces. IEEE 802.1Q is a standard protocol for interconnecting multiple switches and routers and for defining VLAN topologies. Use the <b>encapsulation dot1q</b> command in subinterface range configuration mode to apply a VLAN ID to the subinterface.
-------------------------	---



## Note

This command is not applicable to loopback interfaces.

This command does not require a license but if you want to enable Layer 3 interfaces, you must install the LAN Base Services license.

<b>Examples</b>	This example shows how to enable dot1Q encapsulation on a subinterface for VLAN 30:
-----------------	---

```
switch# configure terminal
switch(config)# interface ethernet 1/5.1
switch(config-subif)# encapsulation dot1q 30
switch(config-subif)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show vlan dot1Q</b>	Displays dot1Q encapsulation information for a VLAN.

# feature vpc

To enable a virtual port channel (vPC), which allows links that are physically connected to two different Cisco Nexus 3000 Series devices to appear as a single port channel to a third device, use the **feature vpc** command. To disable vPC on the switch, use the **no** form of this command.

**feature vpc**

**no feature vpc**

---

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

---

<b>Command Default</b>	Disabled
------------------------	----------

---

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

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	6.0(2)A3(1)	This command was introduced.

---

---

<b>Usage Guidelines</b>	In a vPC configuration, the third device can be a Cisco Nexus 2000 Series Fabric Extender, switch, server, or any other networking device.
-------------------------	--

---

<b>Examples</b>	This example shows how to enable vPC on the switch:
-----------------	---

```
switch(config)# feature vpc
switch(config)#
```

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show vpc</b>	Displays the vPC configuration status.
	<b>show feature</b>	Displays whether or not vPC is enabled on the switch.

---

# interface ethernet

To enter interface configuration mode for an Ethernet IEEE 802.3 interface, use the **interface ethernet** command.

**interface ethernet** *slot/port*

<b>Syntax Description</b>	<i>slot</i>	Slot number. The range is from 1 to 255.
	<i>port</i>	Port number within a particular slot. The port number is from 1 to 128.

**Command Default** None

**Command Modes** Global configuration mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

**Examples** This example shows how to enter configuration mode for Ethernet interface 1/4:

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show interface ethernet</b>	Displays various parameters of an Ethernet IEEE 802.3 interface.
	<b>speed</b>	Sets the speed on the interface.
	<b>vtp (interface)</b>	Enables VLAN Trunking Protocol (VTP) on an interface.

# interface ethernet (Layer 3)

To configure a Layer 3 Ethernet IEEE 802.3 routed interface, use the **interface ethernet** command.

**interface ethernet** *slot/port[.subintf-port-no]*

Syntax Description	<i>slot</i>	Slot number. The range is from 1 to 255.
	<i>port</i>	Port number within a particular slot. The port number is from 1 to 128.
	.	(Optional) Specifies the subinterface separator.
	<i>subintf-port-no</i>	(Optional) Port number for the subinterface. The range is from 1 to 48.

Command Default None

Command Modes Global configuration mode  
Interface configuration mode

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

**Usage Guidelines** You must use the **no switchport** command in the interface configuration mode to configure the interface as a Layer 3 routed interface. When you configure the interface as a Layer 3 interface, all Layer 2 specific configurations on this interface are deleted.

Use the **switchport** command to convert a Layer 3 interface into a Layer 2 interface. When you configure the interface as a Layer 2 interface, all Layer 3 specific configurations on this interface are deleted.

This command requires the LAN Base Services license.

**Examples** This example shows how to enter configuration mode for a Layer 3 Ethernet interface 1/5:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# ip address 10.1.1.1/24
switch(config-if)#
```

This example shows how to configure a Layer 3 subinterface for Ethernet interface 1/5 in the global configuration mode:

```
switch# configure terminal
switch(config)# interface ethernet 1/5.2
switch(config-if)# no switchport
switch(config-subif)# ip address 10.1.1.1/24
switch(config-subif)#
```



This example shows how to configure a Layer 3 subinterface in interface configuration mode:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# interface ethernet 1/5.1
switch(config-subif)# ip address 10.1.1.1/24
switch(config-subif)#
```

This example shows how to convert a Layer 3 interface to a Layer 2 interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# ip address 10.1.1.1/24
switch(config-if)# switchport
switch(config-if)#
```

#### Related Commands

Command	Description
<b>bandwidth</b>	Sets the bandwidth parameters for an interface.
<b>delay</b>	Configures the interface throughput delay value.
<b>encapsulation</b>	Sets the encapsulation type for an interface.
<b>ip address</b>	Sets a primary or secondary IP address for an interface.
<b>no switchport</b>	Configures an interface as a Layer 3 interface.
<b>service-polic</b>	Configures a service policy for an interface.
<b>show interface ethernet</b>	Displays various parameters of an Ethernet IEEE 802.3 interface.

# interface loopback

To create a loopback interface and enter interface configuration mode, use the **interface loopback** command. To remove a loopback interface, use the **no** form of this command.

```
interface loopback number

no interface loopback number
```

Syntax Description	number	Interface number; the range is from 0 to 1023.
--------------------	--------	--

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

Command Modes	Global configuration mode
---------------	---------------------------

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

Usage Guidelines

Use the **interface loopback** command to create or modify loopback interfaces.

From the loopback interface configuration mode, the following parameters are available:

- **description**—Provides a description of the purpose of the interface.
- **ip**—Configures IP features, such as the IP address for the interface, Address Resolution Protocol (ARP) attributes, load balancing, or Unicast Reverse Path Forwarding (RPF).
- **logging**—Configures logging of events.
- **shutdown**—Shuts down traffic on the interface.

This command does not require a license.

Examples

This example shows how to create a loopback interface:

```
switch# configure terminal
switch(config)# interface loopback 50
switch(config-if)# ip address 10.1.1.1/24
switch(config-if)#
```

Related Commands	Command	Description
	<b>show interface loopback</b>	Displays information about the traffic on the specified loopback interface.

# interface port-channel

To create an EtherChannel interface and enter interface configuration mode, use the **interface port-channel** command. To remove an EtherChannel interface, use the **no** form of this command.

**interface port-channel** *channel-number* [*.subintf-channel-no*]

**no interface port-channel** *channel-number* [*.subintf-channel-no*]

Syntax Description	<i>channel-number</i>	Channel number that is assigned to this EtherChannel logical interface. The range is from 1 to 4096.
	.	(Optional) Specifies the subinterface separator.
		<b>Note</b> Applies to Layer 3 interfaces.
	<i>subintf-channel-no</i>	(Optional) Port number of the EtherChannel subinterface. The range is from 1 to 4093.
		<b>Note</b> Applies to Layer 3 interfaces.

**Command Default** None

**Command Modes** Global configuration mode  
Interface configuration mode

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

**Usage Guidelines**

A port can belong to only one channel group.

When you use the **interface port-channel** command for Layer 2 interfaces, follow these guidelines:

- If you are using the Cisco Discovery Protocol (CDP), you must configure it only on the physical interface and not on the EtherChannel interface.
- The MAC address of the EtherChannel is the address of the first operational port added to the channel group. If this first-added port is removed from the channel, the MAC address comes from the next operational port added, if there is one.

You must use the **no switchport** command in the interface configuration mode to configure the EtherChannel interface as a Layer 3 interface. When you configure the interface as a Layer 3 interface, all Layer 2 specific configurations on this interface are deleted.

Use the **switchport** command to convert a Layer 3 EtherChannel interface into a Layer 2 interface. When you configure the interface as a Layer 2 interface, all Layer 3 specific configurations on this interface are deleted.

You can configure one or more subinterfaces on a port channel made from routed interfaces.

This command does not require a license.

**Examples**

This example shows how to create an EtherChannel group interface with channel-group number 50:

```
switch# configure terminal
switch(config)# interface port-channel 50
switch(config-if)#
```

This example shows how to create a Layer 3 EtherChannel group interface with channel-group number 10:

```
switch# configure terminal
switch(config)# interface port-channel 10
switch(config-if)# no switchport
switch(config-if)# ip address 192.0.2.1/24
switch(config-if)#
```

This example shows how to configure a Layer 3 EtherChannel subinterface with channel-group number 1 in interface configuration mode:

```
switch# configure terminal
switch(config)# interface port-channel 10
switch(config-if)# no switchport
switch(config-if)# interface port-channel 10.1
switch(config-subif)# ip address 192.0.2.2/24
switch(config-subif)#
```

This example shows how to configure a Layer 3 EtherChannel subinterface with channel-group number 20.1 in global configuration mode:

```
switch# configure terminal
switch(config)# interface port-channel 20.1
switch(config-subif)# ip address 192.0.2.3/24
switch(config-subif)#
```

**Related Commands**

Command	Description
<b>encapsulation</b>	(Layer 3 interfaces) Sets the encapsulation type for an interface.
<b>ip address</b>	(Layer 3 interfaces) Sets a primary or secondary IP address for an interface.
<b>no switchport</b>	(Layer 3 interfaces) Configures an interface as a Layer 3 interface.
<b>show interface</b>	Displays configuration information about interfaces.
<b>show lacp</b>	Displays LACP information.
<b>show port-channel summary</b>	Displays information on the EtherChannels.
<b>vtp (interface)</b>	Enables VLAN Trunking Protocol (VTP) on an interface.

# interface vlan

To create a VLAN interface and enter interface configuration mode, use the **interface vlan** command. To remove a VLAN interface, use the **no** form of this command.

**interface vlan** *vlan-id*

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

<b>Syntax Description</b>	<i>vlan-id</i>	VLAN to set when the interface is in access mode; valid values are from 1 to 4094, except for the VLANs reserved for the internal switch use.
---------------------------	----------------	---

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

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

<b>Usage Guidelines</b>	Before you use this command, enable the interface-vlan feature by using the <b>feature interface-vlan</b> command.
	Use the <b>interface vlan</b> command to create or modify VLAN interfaces.
	The VLAN interface is created the first time that you enter the <b>interface vlan</b> command for a particular VLAN. The <i>vlan-id</i> argument corresponds to the VLAN tag that is associated with the data frames on an IEEE 802.1Q-encapsulated trunk or the VLAN ID that is configured for an access port.
	This command does not require a license.

<b>Examples</b>	This example shows how to create a VLAN interface for VLAN 50:
-----------------	--

```
switch# configure terminal
switch(config)# interface vlan 50
switch(config-if)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>feature interface-vlan</b>	Enables the ability to create VLAN interfaces.
	<b>show interface vlan</b>	Displays information about the traffic on the specified VLAN interface.

# ip nat

To designate that traffic originating from or destined for an interface is subject to Network Address Translation (NAT), use the **ip nat** command in interface configuration mode. To disable the configuration, use the **no** form of this command.

**ip nat {inside | outside}**

**no ip nat {inside | outside}**

<b>Syntax Description</b>	<b>inside</b>	Connects the interface inside network (the network subject to NAT translation).
	<b>outside</b>	Connects the interface to the outside network.

**Command Default** Traffic leaving or arriving at an interface is not subject to NAT.

**Command Modes** Interface configuration (config-if)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

**Usage Guidelines** Only packets traversing between inside and outside interfaces can be translated. You must specify at least one inside interface and one outside interface for each border device where you intend to use NAT.

**Examples** The following example shows how to connect interfaces to the outside and inside networks:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# ip address 172.69.232.182 255.255.255.240
switch(config-if)# ip nat outside
switch(config-if)# exit
switch(config)# interface ethernet 1/4
switch(config-if)# ip address 192.168.1.94 255.255.255.0
switch(config-if)# ip nat inside
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clear ip nat translation</b>	Clears dynamic NAT translations from the translation table.
	<b>ip nat inside source list</b>	Enables dynamic NAT of the inside source address by using an ACL.
	<b>show ip nat translations</b>	Displays active NAT translations.

# ip nat inside source list

To enable dynamic Network Address Translation (NAT) of the inside source address by using an access control list (ACL), use the **ip nat inside source** command in global configuration mode. To disable the configuration, use the **no** form of this command.

```
ip nat inside source list access-list-name {interface type number | pool pool-name [overload]}
[group group-id] [dynamic]
```

```
no ip nat inside source list access-list-name {interface type number | pool pool-name [overload]}
[group group-id] [dynamic]
```

Syntax Description		
	<i>access-list-name</i>	Name of a standard or extended IP access list. Packets that are permitted by the access list are dynamically translated using the global address from the interfaces specified.
	<b>interface</b>	Specifies an interface for the global address.
	<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
	<i>number</i>	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
	<b>pool</b>	Specifies a pool of global addresses.
	<i>pool-name</i>	Specifies the name of the pool.
	<b>overload</b>	Enables the router to use one global address for many local addresses. When overloading is configured, the TCP or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address.
	<b>group</b>	Specifies the group to which a translation belongs.
	<i>group-id</i>	Specifies the ID of the group.
	<b>dynamic</b>	Specifies that the group is a dynamic twice NAT group.

<b>Command Default</b>	No NAT translation of inside source addresses occurs.
------------------------	---

<b>Command Modes</b>	Global configuration (config)
----------------------	-------------------------------

Command History	Release	Modification
	6.0(2)A4(1)	The <b>group</b> and <b>dynamic</b> keywords were introduced.
	6.0(2)A3(1)	The <b>pool</b> keyword was introduced.
	6.0(2)A1(1)	This command was introduced.

**Usage Guidelines**

Packets that enter a device through the inside interface and packets that are sourced from the device are checked against the access list for possible NAT candidates. The access list is used to specify the traffic that is to be translated.

Overload, also called Port Address Translation (PAT), is a form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address by using different ports. Your NAT configuration can have multiple dynamic NAT translations with different access control lists (ACLs); but each ACL must point to the same outgoing interface.

**Examples**

This example shows how to configure the dynamic NAT overload configuration:

```
switch# configure terminal
switch(config)# ip nat inside source list acl1 interface ethernet 1/1 overload
```

This example shows how to create a NAT inside source list with pool without overloading:

```
switch# configure terminal
switch(config)# ip nat inside source list list1 pool pool1
switch(config)#
```

This example shows how to create a NAT inside source list with pool with overloading:

```
switch# configure terminal
switch(config)# ip nat inside source list list2 pool pool2 overload
switch(config)#
```

This example shows how to configure dynamic twice NAT for an inside source address:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip nat outside source static 2.2.2.2 4.4.4.4 group 20 dynamic
switch(config)# ip nat inside source list acl_1 pool pool_1 overload group 20 dynamic
switch(config)# ip nat pool pool_1 3.3.3.3 3.3.3.10 prefix-length 24
switch(config)# interface Ethernet1/8
switch(config-if)# ip nat outside
switch(config-if)# exit
switch(config)# interface Ethernet1/15
switch(config-if)# ip nat inside
```

**Related Commands**

Command	Description
<b>clear ip nat translation</b>	Clears dynamic NAT translations from the translation table.
<b>ip access-list</b>	Defines an IP access list by a name.
<b>ip nat outside source list</b>	Enables dynamic NAT of the inside source address by using an ACL.
<b>show ip nat translations</b>	Displays active NAT translations.



# ip nat inside source static

To enable static Network Address Translation (NAT) of an inside global address to an inside local address or of inside local traffic to inside global traffic, use the **ip nat inside source static** command in global configuration mode. To disable the configuration, use the **no** form of this command.

**ip nat inside source static** *inside-local-ip-address* *inside-global-ip-address* [**tcp** | **udp**]  
*inside-local-ip-address* *local-port* *inside-global-ip-address* *global-port* [**group** *group-id*]  
**[dynamic]**

**no ip nat inside source static** *inside-local-ip-address* *inside-global-ip-address* [**tcp** | **udp**]  
*inside-local-ip-address* *local-port* *inside-global-ip-address* *global-port* [**group** *group-id*]  
**[dynamic]**

Syntax Description	<i>inside-local-ip-address</i>	Specifies the inside local IP address.
	<i>inside-global-ip-address</i>	Specifies the inside global IP address.
	<i>s</i>	
	<i>local-port</i>	Local UDP or TCP port. The port number can range between 1 and 65535.
	<i>global-port</i>	Global UDP or TCP port. The port number can range between 1 and 65535.
	<b>group</b>	Specifies the group to which a twice NAT translation belongs.
	<i>group-id</i>	Specifies the ID of the group.
	<b>dynamic</b>	Specifies that the group is a dynamic twice NAT group.

**Command Default** None

**Command Modes** Global configuration (config)

Command History	<b>Release</b>	<b>Modification</b>
	6.0(2)A4(1)	This command was introduced.

**Examples** This example shows how to configure dynamic twice NAT for an outside source address:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip nat inside source static 7.7.7.7 5.5.5.5 group 30 dynamic
switch(config)# ip nat outside source list acl_2 pool pool_2 overload group 30 dynamic
switch(config)# ip nat pool pool_2 4.4.4.4 4.4.4.10 prefix-length 24
switch(config)# interface Ethernet1/6
switch(config-if)# ip nat outside
switch(config-if)# exit
switch(config)# interface Ethernet1/11
switch(config-if)# ip nat inside
```

Related Commands	Command	Description
	<b>clear ip nat translation</b>	Clears dynamic NAT translations from the translation table.
	<b>ip access-list</b>	Defines an IP access list by a name.
	<b>ip nat outside source list</b>	Enables dynamic NAT of the inside source address by using an ACL.
	<b>show ip nat translations</b>	Displays active NAT translations.

# ip nat outside source list

To enable dynamic Network Address Translation (NAT) of the outside source address by using an access control list (ACL), use the **ip nat outside source** command in global configuration mode. To disable the configuration, use the **no** form of this command.

```
ip nat outside source list access-list-name {interface type number | pool pool-name [overload]}
[group group-id] [add-route] [dynamic]
```

```
no ip nat outside source list access-list-name {interface type number | pool pool-name
[overload]} [group group-id] [add-route] [dynamic]
```

Syntax Description		
	<i>access-list-name</i>	Name of a standard or extended IP access list. Packets that are permitted by the access list are dynamically translated using the global address from the interfaces specified.
	<b>interface</b>	Specifies an interface for the global address.
	<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
	<i>number</i>	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
	<b>pool</b>	Specifies a pool of global addresses.
	<i>pool-name</i>	Specifies the name of the pool.
	<b>overload</b>	Enables the router to use one global address for many local addresses. When overloading is configured, the TCP or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address.
	<b>group</b>	Specifies the group to which a translation belongs.
	<i>group-id</i>	Specifies the ID of the group.
	<b>add-route</b>	Adds a static route for an outside local address.
	<b>dynamic</b>	Specifies that the group is a dynamic twice NAT group.

**Command Default** No NAT translation of outside source addresses occurs.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	6.0(2)A4(1)	The <b>group</b> and <b>dynamic</b> keywords were introduced.
	6.0(2)A3(1)	This command was introduced.

**Usage Guidelines**

Packets that enter a device through the outside interface and packets that are sourced from the device are checked against the access list for possible NAT candidates. The access list is used to specify the traffic that is to be translated.

**Examples**

This example shows how to create a NAT outside source list with pool without overloading:

```
switch# configure terminal
switch(config)# ip nat outside source list list3 pool pool3
switch(config)#
```

This example shows how to configure dynamic twice NAT for an outside source address:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip nat inside source static 7.7.7.7 5.5.5.5 group 30 dynamic
switch(config)# ip nat outside source list acl_2 pool pool_2 overload group 30 dynamic
switch(config)# ip nat pool pool_2 4.4.4.4 4.4.4.10 prefix-length 24
switch(config)# interface Ethernet1/6
switch(config-if)# ip nat outside
switch(config-if)# exit
switch(config)# interface Ethernet1/11
switch(config-if)# ip nat inside
```

**Related Commands**

Command	Description
<b>clear ip nat translation</b>	Clears dynamic NAT translations from the translation table.
<b>ip access-list</b>	Defines an IP access list by a name.
<b>ip nat inside source list</b>	Enables dynamic NAT of the inside source address by using an ACL.
<b>show ip nat translations</b>	Displays active NAT translations.

# ip nat outside source static

To enable static Network Address Translation (NAT) of an outside global address to an inside local address or of inside local traffic to inside global traffic, use the **ip nat outside source static** command in global configuration mode. To disable the configuration, use the **no** form of this command.

**ip nat outside source static** *outside-global-ip-address outside-local-ip-address* | [**tcp** | **udp**] *outside-global-ip-address outside-global-port outside-local-ip-address outside-local-port* [**group** *group-id*] [**add-route**] [**dynamic**]

**no ip nat outside source static** *outside-global-ip-address outside-local-ip-address* | [**tcp** | **udp**] *outside-global-ip-address outside-global-port outside-local-ip-address outside-local-port* [**group** *group-id*] [**add-route**] [**dynamic**]

Syntax Description	<i>outside-global-ip-address</i>	Specifies the outside global IP address.
	<i>ss</i>	
	<i>outside-local-ip-address</i>	Specifies the outside local IP address.
	<i>s</i>	
	<i>outside-local-port</i>	Outside local UDP or TCP port. The port number can range between 1 and 65535.
	<i>outside-global-port</i>	Outside global UDP or TCP port. The port number can range between 1 and 65535.
	<b>group</b>	Specifies the group to which a twice NAT translation belongs.
	<i>group-id</i>	Specifies the ID of the group.
	<b>add-route</b>	Adds a static route for an outside local address.
	<b>dynamic</b>	Specifies that the group is a dynamic twice NAT group.

**Command Default** None

**Command Modes** Global configuration (config)

Command History	Release	Modification
	6.0(2)A4(1)	This command was introduced.

**Examples** This example shows how to configure dynamic twice NAT for an inside source address:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip nat outside source static 2.2.2.2 4.4.4.4 group 20 dynamic
switch(config)# ip nat inside source list acl_1 pool pool_1 overload group 20 dynamic
switch(config)# ip nat pool pool_1 3.3.3.3 3.3.3.10 prefix-length 24
switch(config)# interface Ethernet1/8
switch(config-if)# ip nat outside
switch(config-if)# exit
```

```
switch(config)# interface Ethernet1/15
switch(config-if)# ip nat inside
```

**Related Commands**

Command	Description
<b>clear ip nat translation</b>	Clears dynamic NAT translations from the translation table.
<b>ip access-list</b>	Defines an IP access list by a name.
<b>ip nat outside source list</b>	Enables dynamic NAT of the inside source address by using an ACL.
<b>show ip nat translations</b>	Displays active NAT translations.

# ip nat pool

To create a dynamic Network Address Translation (NAT) pool, use the **ip nat pool** command in global configuration mode. To delete the pool, use the **no** form of this command.

**ip nat pool** *pool-name* [*startip endip*] {**prefix** *prefix-length* | **netmask** *network-mask*}

**no ip nat pool** *pool-name*

Syntax Description		
<i>pool-name</i>		Specifies the name of the address pool.
<i>startip</i>		(Optional) Specifies the starting IP address for the range of addresses in the pool.
<i>endip</i>		(Optional) Specifies the ending IP address for the range of addresses in the pool.
<b>prefix</b>		Specifies that the prefix length will be used for filtering IP addresses.
<i>prefix-length</i>		Specifies the prefix length.
<b>netmask</b>		Specifies that a network mask will be used for filtering IP addresses.
<i>network-mask</i>		Specifies the network mask.

**Command Default** None.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	6.0(2)A3(1)	This command was introduced.

**Usage Guidelines** Dynamic NAT allows the configuration of a pool of global addresses that can be used to dynamically allocate global address from the pool for every new translation. The addresses are returned to the pool after the session ages out or is closed. This allows for a more efficient use of addresses based on requirements.

Support for PAT includes the use of the global address pool. This further optimizes IP address utilization. PAT exhausts one IP address at a time with the use of port numbers. If no port is available from the appropriate group and more than one IP address is configured, PAT moves to the next IP address and tries to allocate the original source port again. This process continues until PAT runs out of available ports and IP addresses.

You can create a NAT pool by either defining the range of IP addresses in a single **ip nat pool** command or by using the **ip nat pool** and **address** commands.

**Examples** This example shows how to create a NAT pool with a prefix length:

```
switch# configure terminal
```

```
switch(config)# ip nat pool pool1 30.1.1.1 30.1.1.2 prefix-length 24
switch(config)#
```

This example shows how to create a NAT pool with a network mask:

```
switch# configure terminal
switch(config)# ip nat pool pool5 20.1.1.1 20.1.1.5 netmask 255.0.255.0
switch(config)#
```

This example shows how to create a NAT pool and define the range of global IP addresses using multiple commands:

```
switch# configure terminal
switch(config)# ip nat pool pool7 netmask 255.255.0.0
switch(config-ipnat-pool)# address 40.1.1.1 40.1.1.5
switch(config-ipnat-pool)#
```

This example shows how to delete a NAT pool:

```
switch# configure terminal
switch(config)# no ip nat pool pool4
switch(config)#
```

#### Related Commands

Command	Description
<b>address</b>	Defines a range of IP addresses for a pool.
<b>ip nat inside source list</b>	Enables dynamic NAT of the inside source address by using an ACL.
<b>show ip nat translations</b>	Displays active NAT translations.



# ip nat translation

To change the Network Address Translation (NAT) timeout, use the **ip nat translation** command in global configuration mode. To disable the timeout, use the **no** form of this command.

```
ip nat translation {finrst-timeout {seconds | never} | max-entries number-of-entries |  
  sampling-timeout seconds | syn-timeout {seconds | never} | tcp-timeout seconds | timeout |  
  udp-timeout seconds}
```

```
no ip nat translation {finrst-timeout {seconds | never} | max-entries number-of-entries |  
  sampling-timeout seconds | syn-timeout {seconds | never} | tcp-timeout seconds | timeout |  
  seconds | udp-timeout seconds}
```

Syntax Description		
<b>finrst-timeout</b> <i>seconds</i>	Specifies the timeout value for the flow entries when a connection is terminated by receiving finish (FIN) or reset (RST) packets.  The timeout value ranges from 1 second to 172800 seconds. The default value is 60 seconds.	
<b>finrst-timeout never</b>	Specifies that the FIN or RST timer will not be run.	
<b>max-entries</b> <i>number-of-entries</i>	Limits the maximum number of dynamic translations that are created.  <b>Note</b> Appropriate TCAM space needs to be allocated.  The maximum number of allowed dynamic NAT entries range from 1 to 1023.	
<b>sampling-timeout</b> <i>seconds</i>	Specifies the timeout value after which dynamic translations are checked for activity. The default is 43,200 seconds (12 hours).  The timeout value can range from 900 seconds to 172800 seconds.	
<b>syn-timeout</b> <i>seconds</i>	Specifies the timeout value for TCP data packets that send the SYN request, but do not receive a SYN-ACK reply.  The timeout value ranges from 1 second to 172800 seconds. The default value is 60 seconds.	
<b>syn-timeout never</b>	Specifies that the SYN timer will not be run.	
<b>tcp-timeout</b> <i>seconds</i>	Specifies that the timeout value applies to the TCP port. The default is 86,400 seconds (24 hours).  The timeout value can range from 60 seconds to 172800 seconds in addition to the sampling-timeout.	
<b>timeout</b> <i>seconds</i>	Specifies the timeout value for dynamic NAT translations.  The timeout value can range from 60 seconds to 172800 seconds in addition to the sampling-timeout.	
<b>udp-timeout</b> <i>seconds</i>	Specifies that the timeout value applies to the UDP port. The default is 300 seconds (5 minutes).  The timeout value can range from 60 seconds to 172800 seconds in addition to the sampling-timeout.	

**Command Default** NAT translation timeouts are enabled by default.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	6.0(2)A4(1)	The <b>finrst-timeout</b> and <b>syn-timeout</b> command options were introduced.
	6.0(2)A1(1)	This command was introduced.

**Usage Guidelines** Timeout of a dynamic translation involves both the sampling-timeout value and the TCP or UDP timeout value. The sampling-timeout specifies the time after which the device checks for dynamic translation activity. During the checking, the device inspects the packets that are hitting this translation. The checking happens for the TCP or UDP timeout period. If there are no packets for the TCP or UDP timeout period, the translation is cleared. If activity is detected on the translation, then the checking is stopped immediately and a sampling-timeout period begins.

After waiting for this new sampling-timeout period, the device checks for dynamic translation activity again. During an activity check the Ternary Content-Addressable Memory (TCAM) sends a copy of the packet that matches the dynamic NAT translation to the CPU. If the Control Plane Policing (CoPP) is configured at a low threshold, the TCP or UDP packets might not reach the CPU, and the CPU considers this as inactivity of the NAT translation.

**Examples** The following example shows how to configure the timeout value for TCP data packets that send the SYN request, but do not receive a SYN-ACK reply:

```
switch# configure terminal
switch(config)# ip nat translation syn-timeout 20
```

The following example shows how to configure a device to cause UDP port translation entries to time out after 10 minutes (600 seconds):

```
switch# configure terminal
switch(config)# ip nat translation udp-timeout 600
```

Related Commands	Command	Description
	<b>clear ip nat translation</b>	Clears dynamic NAT translations from the translation table.
	<b>ip nat inside source list</b>	Enables dynamic NAT of the inside source address by using an ACL.
	<b>show ip nat translations</b>	Displays active NAT translations.

# lacp min-links

Command	Description
<b>reload</b>	Reloads the Cisco Nexus switch software.
<b>show running-config</b>	Displays the information for the running configuration.

To configure port channel min-links and enter the interface configuration mode, use the **lacp min-links** command. To remove the port channel min-links configuration, use the **no** form of this command.

**lacp min-links** *number*

**no lacp min-links**

<b>Syntax Description</b>	number	Min-links number. The range is from 1 to 16.
<b>Defaults</b>	1	
<b>Command Modes</b>	Interface configuration mode	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1))	This command was introduced.
<b>Usage Guidelines</b>	The min-link feature works only with the Link Aggregation Control Protocol (LACP) port channels. This command does not require a license.	
<b>Examples</b>	<p>This example shows how to configure port channel min-links and enter the interface configuration mode:</p> <pre>switch# configure terminal switch(config)# interface port-channel 100 switch(config-if)# lacp min-links 10</pre> <p>This example shows how to remove the port channel min-links configuration:</p> <pre>switch(config-if)# no lacp min-links switch(config)#</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	show running-config	Displays the port channel min-links configuration.
	interface port-channel	

# lacp port-priority

To set the priority for the physical interfaces for the Link Aggregation Control Protocol (LACP), use the **lacp port-priority** command. To return the port priority to the default value, use the **no** form of this command.

**lacp port-priority** *priority*

**no lacp port-priority**

Syntax Description	<i>priority</i>	Priority for the physical interfaces. The range of valid numbers is from 1 to 65535.
--------------------	-----------------	--

Command Default	System priority value is 32768.
-----------------	---------------------------------

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

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

Usage Guidelines	Each port configured to use LACP has an LACP port priority. You can configure a value between 1 and 65535. LACP uses the port priority in combination with the port number to form the port identifier. The port priority is used with the port number to form the port identifier. The port priority is used to decide which ports should be put into standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.
------------------	--

**Note**

When setting the priority, note that a *higher* number means a *lower* priority.

This command does not require a license.

Examples	This example shows how to set the LACP port priority for the interface to 2000:
----------	---

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# lacp port-priority 2000
switch(config-if)#
```

Related Commands	Command	Description
	<b>show lacp</b>	Displays LACP information.

# lacp rate fast

To configure the rate at which control packets are sent by the Link Aggregation Control Protocol (LACP), use the **lacp rate fast** command. To restore the rate to 30 seconds, use the **no** form of this command or the **lacp rate normal** command.

**lacp rate fast**

**no lacp rate**

**no lacp rate fast**

**lacp rate normal**

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

<b>Command Default</b>	1 second
------------------------	----------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

<b>Usage Guidelines</b>	<p>You must enable LACP before using this command.</p> <p>The LACP rate fast feature is used to set the rate (once every second) at which the LACP control packets are sent to an LACP-supported interface. The normal rate at which LACP packets are sent is 30 seconds.</p> <p>This command does not require a license.</p>
-------------------------	---

<b>Examples</b>	<p>This example shows how to configure the LACP fast rate feature on a specified Ethernet interface:</p>
-----------------	--

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# lacp rate fast
switch(config-if)#
```

This example shows how to remove the LACP fast rate configuration from a specified Ethernet interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no lacp rate fast
switch(config-if)#
```

Related Commands	Command	Description
	<b>feature lacp</b>	Enables or disables LACP on the switch.
	<b>interface ethernet</b>	Enters Ethernet interface configuration mode.
	<b>show lacp</b>	Displays the LACP configuration information.

# lacp system-priority

To set the system priority of the switch for the Link Aggregation Control Protocol (LACP), use the **lacp system-priority** command. To return the system priority to the default value, use the **no** form of this command.

**lacp system-priority** *priority*

**no lacp system-priority**

<b>Syntax Description</b>	<i>priority</i>	Priority for the physical interfaces. The range of valid numbers is from 1 to 65535.
---------------------------	-----------------	--

<b>Command Default</b>	System priority value is 32768.
------------------------	---------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

<b>Usage Guidelines</b>	Each device that runs LACP has an LACP system priority value. You can configure a value between 1 and 65535. LACP uses the system priority with the MAC address to form the system ID and also during negotiation with other systems.
-------------------------	---

When setting the priority, note that a *higher* number means a *lower* priority.

This command does not require a license.

<b>Examples</b>	This example shows how to set the LACP system priority for the device to 2500:
-----------------	--

```
switch# configure terminal
switch(config)# lacp system-priority 2500
switch(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show lacp</b>	Displays LACP information.

## lldp (interface)

To enable the reception, or transmission, of Link Layer Discovery Protocol (LLDP) packets on an interface, use the **lldp** command. To disable the reception or transmission of LLDP packets, use the **no** form of this command.

**lldp {receive | transmit}**

**no lldp {receive | transmit}**

<b>Syntax Description</b>	<b>receive</b>	Specifies that the interface receive LLDP packets.
	<b>transmit</b>	Specifies that the interface transmit LLDP packets.

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

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

### Usage Guidelines



#### Note

LLDP, which is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network, is enabled on the switch by default.

This command does not require a license.

### Examples

This example shows how to set an interface to transmit LLDP packets:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# lldp transmit
switch(config-if)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show interface</b>	Displays configuration information about interfaces.



# no switchport

To configure the interface as a Layer 3 Ethernet interface, use the **no switchport** command.

## no switchport

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

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

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

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

<b>Usage Guidelines</b>	<p>You can configure any Ethernet port as a routed interface. When you configure an interface as a Layer 3 interface, any configuration specific to Layer 2 on this interface is deleted.</p> <p>If you want to configure a Layer 3 interface for Layer 2, enter the <b>switchport</b> command. Then, if you change a Layer 2 interface to a routed interface, enter the <b>no switchport</b> command.</p> <p>This command requires the LAN Base Services license.</p>
-------------------------	--

<b>Examples</b>	<p>This example shows how to enable an interface as a Layer 3 routed interface:</p>
-----------------	---

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)#
```

This example shows how to configure a Layer 3 interface as a Layer 2 interface:

```
switch(config)# interface ethernet 1/5
switch(config-if)# switchport
switch(config-if)#
```

Related Commands	Command	Description
	<b>copy running-config startup-config</b>	Saves the running configuration to the startup configuration file.
	<b>interface ethernet (Layer 3)</b>	Configures an Ethernet routed interface or subinterface.
	<b>interface loopback</b>	Configures a loopback interface.
	<b>interface port-channel</b>	Configures an EtherChannel interface or subinterface.

no switchport

Command	Description
<b>ip address</b>	Sets a primary or secondary IP address for an interface.
<b>show interfaces</b>	Displays interface information.

# peer-keepalive

To configure the IPv4 address for the remote end of the vPC peer keepalive link that carries the keepalive messages, use the **peer-keepalive** command. To disassociate the peer keepalive link, use the **no** form of this command.

```
peer-keepalive destination ipv4_address [hold-timeout holdtime_seconds | interval mseconds
{timeout seconds} | precedence {prec_value | critical | flash | flash-override | immediate |
internet | network | priority | routine} | source ipv4_address | tos {tos_value | max-reliability
| max-throughput | min-delay | min-monetary-cost | normal} | tos-byte tos_byte_value |
udp-port udp_port | vrf {vrf_name | management}]
```

```
no peer-keepalive destination ipv4_address [hold-timeout holdtime_seconds | interval mseconds
{timeout seconds} | precedence {prec_value | critical | flash | flash-override | immediate |
internet | network | priority | routine} | source ipv4_address | tos {tos_value | max-reliability
| max-throughput | min-delay | min-monetary-cost | normal} | tos-byte tos_byte_value |
udp-port udp_port | vrf {vrf_name | management}]
```

Syntax Description	
<b>destination</b>	Specifies the remote (secondary) vPC device interface.
<i>ipv4_address</i>	IPv4 address of the vPC device in the <i>A.B.C.D</i> format.
<b>hold-timeout</b> <i>holdtime_seconds</i>	(Optional) Specifies the hold-timeout period (in seconds) for the secondary vPC peer device to ignore vPC peer-keepalive messages. The range is from 3 to 10. The default hold-timeout value is 3 seconds.
<b>interval</b> <i>mseconds</i>	(Optional) Specifies the time interval (in milliseconds) at which the vPC device receives peer-keepalive messages. The range is from 400 to 10000. The default interval time for the vPC peer-keepalive message is 1 second.
<b>timeout</b> <i>seconds</i>	(Optional) Specifies the timeout (in seconds) between retransmissions to the remote (secondary) vPC device. The range is from 3 to 20. The default timeout value is 5 seconds.
<b>precedence</b>	(Optional) Classifies the vPC peer-keepalive interface traffic based on the precedence value in the type of service (ToS) byte field of the IP header. The precedence value can be one of the following: <ul style="list-style-type: none"> <li>• <i>prec_value</i>—IP precedence value. The range is from 0 to 7. The default precedence value is 6.</li> <li>• <b>critical</b>—Critical precedence (5)</li> <li>• <b>flash</b>—Flash precedence (3)</li> <li>• <b>flash-override</b>—Flash-override precedence (4)</li> <li>• <b>immediate</b>—Immediate precedence (2)</li> <li>• <b>internet</b>—Internet precedence (6)</li> <li>• <b>network</b>—Network precedence (7)</li> <li>• <b>priority</b>—Priority precedence (1)</li> <li>• <b>routine</b>—Routine precedence (0)</li> </ul>
<b>source</b>	(Optional) Specifies the source (primary) vPC device interface.

<b>tos</b>	(Optional) Specifies the type of service (ToS) value. The ToS value can be one of the following: <ul style="list-style-type: none"> <li>• <i>tos_value</i>—A 4-bit TOS value. The range is from 0 to 15.</li> <li>• <b>max-reliability</b>—Max-reliability (2)</li> <li>• <b>max-throughput</b>—Max-throughput (4)</li> <li>• <b>min-delay</b>—Min-delay (8)</li> <li>• <b>min-monetary-cost</b>—Min-monetary-cost (1)</li> <li>• <b>normal</b>—Normal (0)</li> </ul>
<b>tos-byte</b> <i>tos_byte_value</i>	(Optional) Specifies a 8-bit ToS value. The range is from 0 to 255.
<b>udp-port</b> <i>udp_port</i>	(Optional) Specifies the UDP port number to be used for the peer keepalive link. The range is from 1024 to 65000.
<b>vrf</b> <i>vrf_name</i>	(Optional) Specifies the virtual routing and forwarding (VRF) name to be used for the peer keepalive link. The name is case sensitive and can be a maximum of 32 alphanumeric characters.
<b>management</b>	Specifies the management VRF. This is the default VRF.

**Command Default** Management port and VRF

**Command Modes** vPC domain configuration mode

Release	Modification
6.0(2)A3(1)	This command was introduced.

**Usage Guidelines** You must configure the vPC peer-keepalive link before the system can form the vPC peer link. Ensure that both the source and destination IP addresses used for the peer-keepalive message are unique in your network and these IP addresses are reachable from the VRF associated with the vPC peer-keepalive link.

The Cisco NX-OS software uses the peer-keepalive link between the vPC peers to transmit periodic, configurable keepalive messages. You must have Layer 3 connectivity between the peer devices to transmit these messages. The system cannot bring up the vPC peer link unless the peer-keepalive link is already up and running.



**Note**

We recommend that you configure a separate VRF instance and put a Layer 3 port from each vPC peer device into that VRF for the vPC peer-keepalive link. Do not use the peer link itself to send vPC peer-keepalive messages.

**Examples** This example shows how to set up the peer keepalive link connection between the primary and secondary vPC device:

```
switch(config)# vpc domain 100
switch(config-vpc-domain)# peer-keepalive destination 192.168.2.2 source 192.168.2.1
```

Note:

```
-----:: Management VRF will be used as the default VRF ::-----  
switch(config-vpc-domain)#
```

Related Commands	Command	Description
	<b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.
	<b>vpc peer-link</b>	Creates the vPC peer link between the vPC peer devices.
	<b>show running-config vpc</b>	Displays the running configuration information for vPCs.
	<b>show vpc peer-keepalive</b>	Displays the status of the peer-keepalive link.
	<b>show vpc statistics</b>	Displays information about the configuration for the keepalive messages.

# port-channel load-balance ethernet

To configure the load-balancing method among the interfaces in the channel-group bundle, use the **port-channel load-balance ethernet** command. To return the system priority to the default value, use the **no** form of this command.

**port-channel load-balance ethernet** *method*

**no port-channel load-balance ethernet** [*method*]

<b>Syntax Description</b>	<i>method</i>	Load-balancing method. See the “Usage Guidelines” section for a list of valid values.
---------------------------	---------------	---

<b>Command Default</b>	Loads distribution on the source and destination MAC address.
------------------------	---

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

<b>Usage Guidelines</b>	<p>By default, the Cisco Nexus 3548 Switch load balances on a port-channel based on source and destination IP addresses.</p> <p>If only MAC address-based load-balancing is desired, you must configure load balancing by using the <b>port-channel load-balance ethernet mac</b> command. There should be no L3 header in the packet and the packets must be link-local. The Ethertype in the packets must be 0xFFFF. Otherwise, the packets drop because of the parse error.</p>
-------------------------	--

The valid load-balancing *method* values are as follows:

- **destination-ip**—Loads distribution on the destination IP address.
- **destination-mac**—Loads distribution on the destination MAC address.
- **destination-port**—Loads distribution on the destination port.
- **source-destination-ip**—Loads distribution on the source and destination IP address.
- **source-destination-mac**—Loads distribution on the source and destination MAC address.
- **source-destination-port**—Loads distribution on the source and destination port.
- **source-ip**—Loads distribution on the source IP address.
- **source-mac**—Loads distribution on the source MAC address.
- **source-port**—Loads distribution on the source port.

Use the option that provides the balance criteria with the greatest variety in your configuration. For example, if the traffic on an EtherChannel is going only to a single MAC address and you use the destination MAC address as the basis of EtherChannel load balancing, the EtherChannel always chooses the same link in that EtherChannel; using source addresses or IP addresses might result in better load balancing.

This command does not require a license.

---

**Examples**

This example shows how to set the load-balancing method to use the source IP:

```
switch(config)# port-channel load-balance ethernet source-ip
```

This example shows how to set the load-balancing method to use the destination IP:

```
switch# configure sync
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-channel load-balance ethernet destination-ip
switch(config)#
```

---

**Related Commands**

Command	Description
<b>show port-channel load-balance</b>	Displays information on EtherChannel load balancing.

# role

To manually assign a primary or secondary role to a virtual Port Channel (vPC) device, use the **role** command. To restore the default role priority, use the **no** form of this command.

```
role priority priority_value

no role priority
```

Syntax Description	<b>priority</b>	Specifies the priority to define primary or secondary roles in the vPC configuration.
	<i>priority_value</i>	Priority value for the vPC device. The range is from 1 to 65535.

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

Command Modes	vPC domain configuration mode
---------------	-------------------------------

Command History	<b>Release</b>	<b>Modification</b>
	6.0(2)A3(1)	This command was introduced.

**Usage Guidelines**

By default, the Cisco NX-OS software elects a primary and secondary vPC peer device after you configure the vPC domain and both sides of the vPC peer link. However, you may want to elect a specific vPC peer device as the primary device for the vPC. Then, you would manually configure the role value for the vPC peer device that you want as the primary device to be lower than the other vPC peer device. vPC does not support role preemption. If the primary vPC peer device fails, the secondary vPC peer device takes over to become operationally the vPC primary device. However, the original operational roles are not restored if the formerly primary vPC comes up again.

**Examples**

This example shows how to configure the role priority of a vPC device:

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# role priority 100
switch(config-vpc-domain)#
```

This example shows how to restore the default role priority of a vPC device:

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# no role priority 100
switch(config-vpc-domain)#
```



Related Commands	Command	Description
	<b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.
	<b>show running-config vpc</b>	Displays the running configuration information for vPCs.
	<b>show vpc role</b>	Displays the vPC system priority.

# show interface brief

To display a brief summary of the interface configuration information, use the **show interface brief** command.

## show interface brief

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

**Command Default** None

**Command Modes** EXEC mode

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

**Examples** This example shows how to display the summary configuration information of the specified interface:

```
switch# show interface brief
```

```
-----
Ethernet      VLAN   Type Mode   Status Reason                Speed   Port
Interface                                           Ch #
-----
Eth1/1        1      eth  access down  SFP not inserted      10G (D) --
Eth1/2        1      eth  trunk  up      none                  10G (D) --
Eth1/3        1      eth  access down  SFP not inserted      10G (D) --
Eth1/4        1      eth  access down  SFP not inserted      10G (D) --
Eth1/5        1      eth  access down  SFP not inserted      10G (D) --
Eth1/6        1      eth  access down  SFP not inserted      10G (D) --
Eth1/7        1      eth  access down  SFP not inserted      10G (D) --
:
:
<--snip-->
Eth1/63       1      eth  access down  SFP not inserted      10G (D) --
Eth1/64       1      eth  access down  SFP not inserted      10G (D) --
-----

Port   VRF      Status IP Address                Speed   MTU
-----
mgmt0  --      up    192.168.0.150              100    1500
switch#
```

Related Commands	Command	Description
	<b>interface ethernet</b>	Configures an Ethernet IEEE 802.3 interface.

# show interface capabilities

To display detailed information about the capabilities of an interface, use the **show interface capabilities** command.

**show interface** [*ethernet slot/port*] **capabilities**

Syntax Description	<b>ethernet slot/port</b>	(Optional) Specifies an Ethernet interface slot number and port number. The <i>slot</i> number is from 1 to 255, and the <i>port</i> number is from 1 to 128.
--------------------	---------------------------	---

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

Command Modes	EXEC mode
---------------	-----------

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

Usage Guidelines	You can use the <b>show interface capabilities</b> command only for physical interfaces.
------------------	--

Examples	This example shows how to display the interface capabilities:
----------	---

```
switch# show interface capabilities
Ethernet1/1
  Model: -SUP
  Type (SFP capable): 10Gbase-SR
  Speed: 1000,10000
  Duplex: full
  Trunk encap. type: 802.1Q
  Channel: yes
  Broadcast suppression: percentage (0-100)
  Flowcontrol: rx- (off/on) ,tx- (off/on)
  Rate mode: none
  QOS scheduling: rx- (6qlt) ,tx- (1p6q0t)
  CoS rewrite: no
  ToS rewrite: no
  SPAN: yes
  UDLD: yes
  Link Debounce: yes
  Link Debounce Time: yes
  MDIX: no
  TDR capable: no
  Port mode: Routed,Switched

Ethernet1/2
<--Output truncated-->
switch#
```

This example shows how to display the interface capabilities for a specific interface:

## ■ show interface capabilities

```

switch# show interface ethernet 1/1 capabilities
Ethernet1/1
  Model: -SUP
  Type (SFP capable): 10Gbase-SR
  Speed: 1000,10000
  Duplex: full
  Trunk encap. type: 802.1Q
  Channel: yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol: rx-(off/on),tx-(off/on)
  Rate mode: none
  QOS scheduling: rx-(6q1t),tx-(1p6q0t)
  CoS rewrite: no
  ToS rewrite: no
  SPAN: yes
  UDLD: yes
  Link Debounce: yes
  Link Debounce Time: yes
  MDIX: no
  TDR capable: no
  Port mode: Routed,Switched

switch#

```

**Related Commands**

Command	Description
<b>interface ethernet</b>	Configures an Ethernet IEEE 802.3 interface.

# show interface debounce

To display the debounce time information for all interfaces, use the **show interface debounce** command.

## show interface debounce

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

**Command Default** None

**Command Modes** EXEC mode

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

**Examples** This example shows how to display the debounce status of all interfaces:

```
switch# show interface debounce
```

```
-----  
Port           Debounce time  Value(ms)  
-----  
Eth1/1         enable        100  
Eth1/2         enable        100  
Eth1/3         enable        100  
Eth1/4         enable        100  
Eth1/5         enable        100  
Eth1/6         enable        100  
Eth1/7         enable        100  
<--Output truncated-->  
switch#
```

Related Commands	Command	Description
	link debounce	Enables the debounce timer on an interface.

# show interface ethernet

To display information about the interface configuration, use the **show interface ethernet** command.

**show interface ethernet** *slot/port*[*,subintf-port-no*] [**brief** | **counters** | **description** | **status** | **switchport** | **transceiver** [**details**]]

Syntax	Description
<i>slot/port</i>	Ethernet interface slot number and port number. The <i>slot</i> number is from 1 to 255, and the <i>port</i> number is from 1 to 128.
.	(Optional) Specifies the subinterface separator.
	<b>Note</b> Applies to Layer 3 interfaces.
<i>subintf-port-no</i>	(Optional) Port number for the subinterface. The range is from 1 to 48.
	<b>Note</b> Applies to Layer 3 interfaces.
<b>brief</b>	(Optional) Displays brief information about the interfaces.
<b>counters</b>	(Optional) Displays information about the counters configured on an interface.
<b>description</b>	(Optional) Displays the description of an interface configuration.
<b>status</b>	(Optional) Displays the operational state of the interface.
<b>switchport</b>	(Optional) Displays the switchport information of an interface.
transceiver details	(Optional) Displays detailed information about the transceivers on an interface.

**Command Default** Displays all information for the interface.

**Command Modes** EXEC mode

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

**Examples** This example shows how to display the detailed configuration of the specified interface:

```
switch# show interface ethernet 1/1
Ethernet1/1 is up
  Hardware: 1000/10000 Ethernet, address: 0005.0505.050d (bia 0005.0505.050d)
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  Port mode is access
  full-duplex, 10 Gb/s, media type is 10G
  Beacon is turned off
  Input flow-control is off, output flow-control is off
  Rate mode is dedicated
  Switchport monitor is off
  EtherType is 0x8100
```

```

Last link flapped 09:09:55
Last clearing of "show interface" counters never
30 seconds input rate 0 bits/sec, 0 bytes/sec, 0 packets/sec
30 seconds output rate 0 bits/sec, 0 bytes/sec, 0 packets/sec
Load-Interval #2: 5 minute (300 seconds)
  input rate 0 bps, 0 pps; output rate 0 bps, 0 pps
RX
  0 unicast packets  0 multicast packets  0 broadcast packets
  0 input packets  0 bytes
  0 jumbo packets  0 storm suppression packets
  0 runts  0 giants  0 CRC  0 no buffer
  0 input error  0 short frame  0 overrun  0 underrun  0 ignored
  0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
  0 input with dribble  0 input discard
  0 Rx pause
TX
  0 unicast packets  10778 multicast packets  0 broadcast packets
  10778 output packets  755719 bytes
  0 jumbo packets
  0 output errors  0 collision  0 deferred  0 late collision
  0 lost carrier  0 no carrier  0 babble
  0 Tx pause
1 interface resets

```

switch#

This example shows how to display the counters configured on a specified interface:

```
switch# show interface ethernet 1/1 counters
```

```

-----
Port                               InOctets                               InUcastPkts
-----
Eth1/1                             0                                       0

-----
Port                               InMcastPkts                            InBcastPkts
-----
Eth1/1                             0                                       0

-----
Port                               OutOctets                               OutUcastPkts
-----
Eth1/1                             755719                                0

-----
Port                               OutMcastPkts                           OutBcastPkts
-----
Eth1/1                             10778                                0
switch#

```

This example shows how to display the switchport information for a specific interface:

```

switch# show interface ethernet 1/2 switchport
Name: Ethernet1/1
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: access
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1
  Unknown unicast blocked: disabled
  Unknown multicast blocked: disabled

```

```
switch#
```

This example shows how to display the operational status for a specific interface:

```
switch# show interface ethernet 1/5 status
```

```
-----
Port          Name          Status    Vlan    Duplex  Speed  Type
-----
Eth1/5        --          sfpAbsent 1       full    40G    40gb
switch#
```

This example shows how to display the calibration information about the transceivers connected to a specified Ethernet interface:

```
switch# show interface ethernet 1/2 transceiver calibrations
```

```
Ethernet1/2
transceiver is present
type is 10Gbase-SR
name is CISCO-AVAGO
part number is SFBR-7700SDZ
revision is B4
serial number is AGD1210210F
nominal bitrate is 10300 MBit/sec
Link length supported for 50/125um fiber is 80 m
Link length supported for 50/125um fiber is 300 m
Link length supported for 62.5/125um fiber is 20 m
cisco id is --
cisco extended id number is 4
Transceiver Internal Calibrations Information
-----
Slope Offset Rx4/Rx3/Rx2/Rx1/Rx0
-----
Temperature 0 0
Voltage 0 0
Current 0 0
Tx Power 0 0
Rx Power 0.0000/0.0000/0.0000/0.0000/0.0000
-----
```

## Related Commands

Command	Description
<b>interface ethernet</b>	Configures an Ethernet IEEE 802.3 interface.
<b>interface ethernet (Layer 3)</b>	Configures a Layer 3 Ethernet IEEE 802.3 interface.
<b>switchport monitor rate-limit</b>	Configures the rate limit for traffic on an interface.



# show interface loopback

To display information about the loopback interface, use the **show interface loopback** command.

**show interface loopback** *lo-number* [**brief** | **description**]

<b>Syntax Description</b>	<i>lo-number</i>	Loopback interface number. The range is from 0 to 1023.
	<b>brief</b>	(Optional) Displays a brief summary of the loopback interface information.
	<b>description</b>	(Optional) Displays the description provided for the loopback interface.

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

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

**Examples** This example shows how to display the configuration information for a specific loopback interface:

```
switch# show interface loopback 10
loopback10 is up
  Hardware: Loopback
  Description: Loopback interface 10
  MTU 1500 bytes, BW 8000000 Kbit, DLY 5000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK
    0 packets input 0 bytes
    0 multicast frames 0 compressed
    0 input errors 0 frame 0 overrun 0 fifo
    0 packets output 0 bytes 0 underruns
    0 output errors 0 collisions 0 fifo

switch#
```

Table 1 describes the significant fields shown in the display.

**Table 1** *show interface loopback* Field Description

Field	Description
Loopback is ...	Indicates whether the interface hardware is currently active (whether carrier detect is present), is currently inactive (down), or has been taken down by an administrator (administratively down).
Hardware	Hardware is Loopback.
MTU	Maximum transmission unit (MTU) of the interface.
BW	Bandwidth (BW) of the interface in kilobits per second.

**Table 1** *show interface loopback Field Description (continued)*

Field	Description
DLY	Delay (DLY) of the interface in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload	Load on the interface for transmitting packets as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
rxload	Load on the interface for receiving packets as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to interface.
LOOPBACK	Indicates whether loopback is set.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
multicast frames	Total number of multicast frames enabled on the interface.
compressed	Total number of multicast frames compressed on the interface.
input errors	Sum of all errors that prevented the receipt of datagrams on the interface being examined. This may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error and others may have errors that do not fall into any of the specifically tabulated categories.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
fifo	Number of First In, First Out (FIFO) errors in the receive direction.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the far-end transmitter has been running faster than the near-end router's receiver can handle. This may never happen (be reported) on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, as some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Loopback interface does not have collisions.
fifo	Number of First In, First Out (FIFO) errors in the transmit direction.

This example shows how to display the brief information for a specific loopback interface:

```
switch# show interface loopback 10 brief
```

```
-----  
Interface      Status      Description  
-----  
loopback10    up          Loopback interface 10  
switch#
```

**Related Commands**

Command	Description
<b>interface loopback</b>	Configures a loopback interface.

# show interface port-channel

To display the information about an EtherChannel interface configuration, use the **show interface port-channel** command.

**show interface port-channel** *number* [*.subinterface-number*] [**brief** | **counters** | **description** | **status**]

<b>Syntax Description</b>	<i>number</i>	EtherChannel number. The range is from 1 to 4096.
	<i>.subinterface-number</i>	(Optional) Port-channel subinterface configuration. Use the EtherChannel number followed by a dot (.) indicator and the subinterface number. The format is <i>portchannel-number.subinterface-number</i> .
	<b>counters</b>	(Optional) Displays information about the counters configured on the EtherChannel interface.
	<b>description</b>	(Optional) Displays the description of the EtherChannel interface configuration.
	<b>status</b>	(Optional) Displays the operational state of the EtherChannel interface.

**Command Default** None

**Command Modes** EXEC mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

**Examples** This example shows how to display the configuration information of a specified EtherChannel interface:

```
switch# show interface port-channel 100
port-channel100 is down (No operational members)
  Hardware: Port-Channel, address: 0000.0000.0000 (bia 0000.0000.0000)
  MTU 1500 bytes, BW 3000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  Port mode is access
  auto-duplex, auto-speed
  Beacon is turned off
  Input flow-control is off, output flow-control is off
  Switchport monitor is off
  EtherType is 0x8100
  No members
  Last clearing of "show interface" counters never
  0 seconds input rate 0 bits/sec, 0 bytes/sec, 0 packets/sec
  0 seconds output rate 0 bits/sec, 0 bytes/sec, 0 packets/sec
  Load-Interval #2: 0 seconds
    input rate 0 bps, 0 pps; output rate 0 bps, 0 pps
  RX
    0 unicast packets  0 multicast packets  0 broadcast packets
```

```

0 input packets 0 bytes
0 jumbo packets 0 storm suppression packets
0 runts 0 giants 0 CRC 0 no buffer
0 input error 0 short frame 0 overrun 0 underrun 0 ignored
0 watchdog 0 bad etype drop 0 bad proto drop 0 if down drop
0 input with dribble 0 input discard
0 Rx pause
TX
0 unicast packets 0 multicast packets 0 broadcast packets
0 output packets 0 bytes
0 jumbo packets
0 output errors 0 collision 0 deferred 0 late collision
0 lost carrier 0 no carrier 0 babble
0 Tx pause
0 interface resets

switch#

```

**Related Commands**

Command	Description
<b>interface port-channel</b>	Configures an EtherChannel interface.

# show interface mac-address

To display the information about the MAC address, use the **show interface mac-address** command.

**show interface** [*type slot/port* | *portchannel-no*] **mac-address**

<b>Syntax Description</b>	<i>type</i>	(Optional) Interface for which MAC addresses should be displayed. The <i>type</i> can be either Ethernet or EtherChannel.
	<i>slot/port</i>	Ethernet interface port number and slot number. The slot number is from 1 to 255, and the port number is from 1 to 128.
	<i>portchannel-no</i>	EtherChannel number. The EtherChannel number is from 1 to 4096.

**Command Default** None

**Command Modes** EXEC mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

**Usage Guidelines** If you do not specify an interface, the system displays all the MAC addresses.

**Examples** This example shows how to display the information on MAC addresses for the entire switch:

```
switch# show interface mac-address
switch(config)# sh interface mac-address
```

```
-----
Interface                Mac-Address      Burn-in Mac-Address
-----
Ethernet1/1              0005.0505.053c  0005.0505.050d
Ethernet1/2              0005.0505.053c  0005.0505.050e
Ethernet1/3              0005.0505.053c  0005.0505.050f
Ethernet1/4              0005.0505.053c  0005.0505.0510
Ethernet1/5              0005.0505.053c  0005.0505.0511
Ethernet1/6              0005.0505.053c  0005.0505.0512
Ethernet1/7              0005.0505.053c  0005.0505.0513
```

```
<--Output truncated-->
switch#
```

This example shows how to display the MAC address information for a specific port channel:

```
switch# show interface port-channel 100 mac-address
```

```
-----
Interface                Mac-Address      Burn-in Mac-Address
-----
port-channel100          0005.0505.053c  0000.0000.0000
```

```
switch#
```

Related Commands	Command	Description
	<b>mac address-table static</b>	Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address.
	<b>show mac address-table</b>	Displays information on the MAC address table.

# show interface status err-disabled

To display the error disabled state of interfaces, use the **show interface status err-disabled** command.

**show interface status err-disabled**

---

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

---

**Command Default** None

---

**Command Modes** EXEC mode

---

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

---



---

**Examples** This example shows how to display the error disabled state of interfaces:

```
switch# show interface status err-disabled
```

---

Related Commands	Command	Description
	<b>errdisable detect cause</b>	Enables the error disabled (err-disabled) detection.
	<b>errdisable recovery cause</b>	Enables error disabled recovery on an interface.

---



# show interface switchport

To display information about all the switch port interfaces, use the **show interface switchport** command.

## show interface switchport

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

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

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

<b>Command History</b>	Release	Modification
	5.0(3)A1(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to display information for all Ethernet interfaces:
-----------------	--

```
switch# show interface switchport
Name: Ethernet1/1
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: access
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1
  Unknown unicast blocked: disabled
  Unknown multicast blocked: disabled

Name: Ethernet1/2
<--Output truncated-->
switch#
```

<b>Related Commands</b>	Command	Description
	<b>switchport access vlan</b>	Sets the access VLAN when the interface is in access mode.
	<b>switchport monitor rate-limit</b>	Configures the rate limit for traffic on an interface.

# show interface transceiver

To display the information about the transceivers connected to a specific interface, use the **show interface transceiver** command.

**show interface** [*ethernet slot/port*] **transceiver** [*details*]

Syntax Description	<b>ethernet slot/port</b>	(Optional) Displays information about an Ethernet interface slot number and port number. The <i>slot</i> number is from 1 to 255, and the <i>port</i> number is from 1 to 128.
	<b>details</b>	(Optional) Displays detailed information about the transceivers on an interface.

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

Command Modes	EXEC mode
---------------	-----------

Command History	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

Usage Guidelines	You can use the <b>show interface transceiver</b> command only for physical interfaces.
------------------	---

Examples	This example shows how to display the transceivers for all Ethernet interfaces:
----------	---

```
switch# show interface transceiver
Ethernet1/1
  transceiver is present
  type is 10Gbase-SR
  name is CISCO-AVAGO
  part number is SFBR-7700SDZ
  revision is B4
  serial number is AGD121220VN
  nominal bitrate is 10300 MBit/sec
  Link length supported for 50/125um fiber is 80 m
  Link length supported for 50/125um fiber is 300 m
  Link length supported for 62.5/125um fiber is 20 m
  cisco id is --
  cisco extended id number is 4

Ethernet1/2
<--Output truncated-->
switch#
```

This example shows how to display the transceivers connected to a specified Ethernet interface:

```
switch# show interface ethernet 1/2 transceiver
Ethernet1/2
```

```

transceiver is present
type is 10Gbase-SR
name is CISCO-AVAGO
part number is SFBR-7700SDZ
revision is B4
serial number is AGD1210210F
nominal bitrate is 10300 MBit/sec
Link length supported for 50/125um fiber is 80 m
Link length supported for 50/125um fiber is 300 m
Link length supported for 62.5/125um fiber is 20 m
cisco id is --
cisco extended id number is 4

```

```
switch#
```

This example shows how to display the detailed information about the transceivers connected to a specified Ethernet interface:

```

switch# show interface ethernet 1/2 transceiver details
Ethernet1/2
  transceiver is present
  type is 10Gbase-SR
  name is CISCO-AVAGO
  part number is SFBR-7700SDZ
  revision is B4
  serial number is AGD1210210F
  nominal bitrate is 10300 MBit/sec
  Link length supported for 50/125um fiber is 80 m
  Link length supported for 50/125um fiber is 300 m
  Link length supported for 62.5/125um fiber is 20 m
  cisco id is --
  cisco extended id number is 4

```

#### Related Commands

Command	Description
<b>interface ethernet</b>	Configures an Ethernet IEEE 802.3 interface.
<b>show interface capabilities</b>	Displays detailed information about the capabilities of an interface.

# show ip nat statistics

To display Network Address Translation (NAT) statistics, use the **show ip nat statistics** EXEC command.

## show ip nat statistics

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

**Command Default** None

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	6.0(2)A8(9)	This command was introduced.

**Examples** This example displays the output the **show ip nat statistics** command:

```
switch# show show ip nat statistics
Pro Inside global      Inside local      Outside local      Outside global
uIP NAT Statistics
=====
Total active translations: 2
No.Static: 2
No.Dyn: 0
No.ICMP: 0
-----
Total expired Translations: 0
SYN timer expired: 0
FIN-RST timer expired: 0
Inactive timer expired: 0
-----
Total Hits: 0          Total Misses: 3
In-Out Hits: 0          In-Out Misses: 0
Out-In Hits: 0          Out-In Misses: 3
-----
Total SW Translated Packets: 0
In-Out SW Translated: 0
Out-In SW Translated: 0
-----
Total SW Dropped Packets: 0
In-Out SW Dropped: 0
Out-In SW Dropped: 0

Address alloc. failure drop: 0
Port alloc. failure drop: 0
Dyn. Translation max limit drop: 0
ICMP max limit drop: 0
Allhost max limit drop: 0
-----
NAT Inside Interfaces: 1
Ethernet1/1
```

```

NAT Outside Interfaces: 1
Ethernet1/3
-----
Inside source list:
+++++

Access list: ACL1
RefCount: 0
Pool: pool1      Overload
Total addresses: 200
Allocated: 0      percentage: 0%
Missed: 0

```

**Related Commands**

Command	Description
<b>ip nat</b>	Designates that traffic originating from or destined for the interface is subject to NAT.

The following table describes the output fields shown in the preceding display.

Field	Description
Total translations	Number of translations active in the system. This number is incremented each time a translation is created and is decremented each time a translation is cleared or times out
No.Static	Total number of static translations present in the system.
No.Dyn	Total number of dynamic translations present in the system.
No.ICMP	Total number of ICMP translations present in the system.
Total expired Translations	Total expired translation in the system.
SYN timer expired	Total TCP SYN timer expired translations in the system.
FIN-RST timer expired	Total FIN-RST timer expired translations in the system.
Inactive timer expired	Total inactive timer expired translations in the system.
Total Hits	Total number of times the software does a translations table lookup and finds an entry. Includes In-Out Traffic and Out-In Traffic
In-Out Hits	Total number of software translated packet for In-Out Traffic.
Out-In Hits	Total number of software translated packet for Out-In Traffic.

Field	Description
Total Misses	Total number of packet the software dropped Packet. Includes In-Out Traffic and Out-In Traffic
In-Out Misses	Total number of packet the software dropped Packet for In-Out Traffic.
Out-In Misses	Total number of packet the software dropped Packet for Out-In Traffic.
Total SW Translated Packets	Total number of packets software does the translation. Includes In-Out Traffic and Out-In Traffic
In-Out SW Translated	Total number of software translated packet for In-Out Traffic.
Out-In SW Translated	Total number of software translated packet for Out-In Traffic.
Total SW Dropped Packets	Total number of packet the software dropped Packet. Includes In-Out Traffic and Out-In Traffic
In-Out SW Dropped	Total number of packet the software dropped Packet for In-Out Traffic.
Out-In SW Dropped	Total number of packet the software dropped Packet for Out-In Traffic.
Address alloc. failure drop	Total number of packets dropped due to failed to allocate translated address.
Port alloc. failure drop	Total number of packets dropped due to failed to allocate translated address and port.
Dyn. Translation max limit drop	Total number of packets dropped due to configured maximum number of dynamic translation entry limit reached. (ip nat translation max-entries <1 - 1023>)
ICMP max limit drop	Total number of packets dropped due to configured maximum number of ICMP translation entry limit reached.
Allhost max limit drop	Total number of packets dropped due to configured maximum number of NAT entries for each host dynamic translation limit reached. (ip nat translation max-entries all-host <1 - 1023>)
NAT Inside Interfaces	List of interfaces marked as inside with the ip nat inside command.
NAT Outside Interfaces	List of interfaces marked as outside with the ip nat outside command.
Inside Source	Indicates that the information that follows is about an inside source translation.
Access list	Access list being used for the translation.

Field	Description
Refcount	Number of current references to this access list.
Pool	Name of the pool.
Total addresses	Number of addresses in the pool available for translation.
Allocated	Number of addresses being used.
Misses	Number of failed allocations from the pool.

# show ip nat translation

To display all NAT translations including static and dynamic translations, use the **show ip nat translation** command in EXEC mode.

## show ip nat translation

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

**Command Default** None

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

**Examples** This example shows how to display entries from the translation table before they time out:

```
switch# show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
udp  1.1.1.2:65372      5.5.5.1:6118      1.1.1.1:161        1.1.1.1:161
udp  1.1.1.2:65390      5.5.5.1:6119      1.1.1.1:161        1.1.1.1:161
any  11.11.1.2          183.1.1.2         ---                ---
any  11.11.1.3          183.1.1.3         ---                ---
any  11.11.2.3          183.1.2.3         ---                ---
any  11.11.2.4          183.1.2.4         ---                ---
```

This example shows how to display active NAT translations:

### Inside pool with overload

```
switch# show ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
icmp 20.1.1.3:64762     10.1.1.2:133     20.1.1.1:0         20.1.1.1:0
icmp 20.1.1.3:64763     10.1.1.2:134     20.1.1.1:0         20.1.1.1:0
```

### Outside pool without overload

```
switch# show ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
icmp 20.1.1.1:0         20.1.1.1:0       20.1.1.3:0         10.1.1.2:133
icmp 20.1.1.1:0         20.1.1.1:0       20.1.1.4:0         10.1.1.2:134
```

Related Commands	Command	Description
	<b>ip nat</b>	Designates that traffic originating from or destined for the interface is subject to NAT.



Command	Description
<b>ip nat inside source list</b>	Enables dynamic NAT of the inside source address by using an ACL.
<b>clear ip nat translations</b>	Clears active NAT translations.

# show lacp

To display Link Aggregation Control Protocol (LACP) information, use the **show lacp** command.

**show lacp** { **counters** | **interface ethernet** *slot/port* | **neighbor** [**interface port-channel** *number*] | **port-channel** [**interface port-channel** *number*] | **system-identifier** }

Syntax Description	<b>counters</b>	Displays information about the LACP traffic statistics.
	<b>interface ethernet</b> <i>slot/port</i>	Displays LACP information for a specific Ethernet interface. The <i>slot</i> number is from 1 to 255, and the <i>port</i> number is from 1 to 128.
	<b>neighbor</b>	Displays information about the LACP neighbor.
	<b>port-channel</b>	Displays information about all EtherChannels.
	<b>interface port-channel</b> <i>number</i>	(Optional) Displays information about a specific EtherChannel. The EtherChannel number is from 1 to 4096.
	<b>system-identifier</b>	Displays the LACP system identification. It is a combination of the port priority and the MAC address of the device.

Command Default None

Command Modes EXEC mode

Command History	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

Usage Guidelines Use the **show lacp** command to troubleshoot problems related to LACP in a network.

Examples This example shows how to display the LACP system identification:

```
switch# show lacp system-identifier
32768,0-5-5-5-5-3c
switch#
```

This example shows how to display the LACP information for a specific interface:

```
switch# show lacp interface ethernet 1/1
Interface Ethernet1/1 is invalid
Channel group is 0 port channel is
PDUs sent: 0
PDUs rcvd: 0
Markers sent: 0
Markers rcvd: 0
Marker response sent: 0
Marker response rcvd: 0
Unknown packets rcvd: 0
Illegal packets rcvd: 0
```

```

Lag Id: [ [(0, 0-0-0-0-0-0, 0, 0, 0), (0, 0-0-0-0-0-0, 0, 0, 0)] ]
Operational as aggregated link since Thu Jan  1 00:00:00 1970

Local Port: Eth1/1    MAC Address= 0-5-5-5-5-3c
  System Identifier=0x8000,0-5-5-5-5-3c
  Port Identifier=0x8000,0x0
  Operational key=0
  LACP_Activity=passive
  LACP_Timeout=Long Timeout (30s)
  Synchronization=NOT_IN_SYNC
  Collecting=false
  Distributing=false
  Partner information refresh timeout=Long Timeout (90s)
Actor Admin State=(Ac-0:To-0:Ag-0:Sy-0:Co-0:Di-0:De-0:Ex-0)
Actor Oper State=(Ac-0:To-0:Ag-0:Sy-0:Co-0:Di-0:De-0:Ex-0)
Neighbor: 0/0
  MAC Address= 0-0-0-0-0-0
  System Identifier=0x0,0-0-0-0-0-0
  Port Identifier=0x0,0x0
  Operational key=0
  LACP_Activity=unknown
  LACP_Timeout=Long Timeout (30s)
  Synchronization=NOT_IN_SYNC
  Collecting=false
  Distributing=false
Partner Admin State=(Ac-0:To-0:Ag-0:Sy-0:Co-0:Di-0:De-0:Ex-0)
Partner Oper State=(Ac-0:To-0:Ag-0:Sy-0:Co-0:Di-0:De-0:Ex-0)
switch#

```

**Related Commands**

Command	Description
<b>lacp port-priority</b>	Sets the priority for the physical interfaces for the LACP.
<b>lacp system-priority</b>	Sets the system priority of the switch for the LACP.

# show module

To display module information, use the **show module** command.

**show module** *module\_num*

Syntax Description	<i>module_num</i>	Module number in the switch chassis. The range is from 1 to 3.
--------------------	-------------------	--

Command Default	Display information of all modules	
-----------------	------------------------------------	--

Command Modes	EXEC mode	
---------------	-----------	--

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

## Examples

This example shows how to display the module information for a specific module:

```
switch# show module 1
Mod Ports  Module-Type                Model                Status
-----
1      40      40x10GE/Supervisor          N5K-C5020P-BF-SUP   active *

Mod  Sw                Hw      World-Wide-Name(s) (WWN)
---
1    4.2(1u)N1(1u)    1.3     --

Mod  MAC-Address(es)                Serial-Num
---
1    0005.9b78.6e48 to 0005.9b78.6e6f  JAF1413ADCS
switch#
```

Related Commands	Command	Description
	<b>show hardware inventory</b>	Displays information about the physical hardware.
	<b>show inventory</b>	Displays hardware inventory information.

# show port-channel capacity

To display the total number of port channels that are configured, or are still available on the device, use the **show port-channel capacity** command.

**show port-channel capacity**

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

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

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

<b>Examples</b>	This example shows how to display the port channels on a device:
-----------------	--

```
switch# show port-channel capacity
Port-channel resources
    64 total    4 used    60 free    6% used
switch#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>port-channel load-balance ethernet</b>	Configures the load-balancing algorithm for EtherChannels.
	<b>show tech-support port-channel</b>	Displays Cisco Technical Support information about EtherChannels.

# show port-channel compatibility-parameters

To display the parameters that must be the same among the member ports in order to join an EtherChannel interface, use the **show port-channel compatibility-parameters** command.

## show port-channel compatibility-parameters

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

**Command Default** None

**Command Modes** EXEC mode

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

**Examples** This example shows how to display the EtherChannel interface parameters:

```
switch# show port-channel compatibility-parameters
* port mode
```

Members must have the same port mode configured.

```
* port mode
```

Members must have the same port mode configured, either E,F or AUTO. If they are configured in AUTO port mode, they have to negotiate E or F mode when they come up. If a member negotiates a different mode, it will be suspended.

```
* speed
```

Members must have the same speed configured. If they are configured in AUTO speed, they have to negotiate the same speed when they come up. If a member negotiates a different speed, it will be suspended.

```
<--Output truncated-->
```

```
switch#
```

Related Commands	Command	Description
	<b>port-channel load-balance ethernet</b>	Configures the load-balancing algorithm for EtherChannels.
	<b>show tech-support port-channel</b>	Displays Cisco Technical Support information about EtherChannels.

# show port-channel database

To display the aggregation state for one or more EtherChannel interfaces, use the **show port-channel database** command.

**show port-channel database** [**interface port-channel** *number*]

Syntax Description	<b>interface</b>	(Optional) Displays information for an EtherChannel interface.
	<b>port-channel</b> <i>number</i>	(Optional) Displays aggregation information for a specific EtherChannel interface. The <i>number</i> range is from 1 to 4096.

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

Command Modes	EXEC mode
---------------	-----------

Command History	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

Examples	<p>This example shows how to display the aggregation state of all EtherChannel interfaces:</p>
----------	--

```
switch# show port-channel database
port-channel10
  Last membership update is successful
  0 ports in total, 0 ports up
  Age of the port-channel is 0d:00h:04m:04s

switch#
```

This example shows how to display the aggregation state for a specific EtherChannel interface:

```
switch# show port-channel database interface port-channel 21
```

Related Commands	<b>Command</b>	<b>Description</b>
	<b>port-channel load-balance ethernet</b>	Configures the load-balancing algorithm for EtherChannels.
	<b>show tech-support port-channel</b>	Displays Cisco Technical Support information about EtherChannels.

# show port-channel load-balance

To display information about EtherChannel load balancing, use the **show port-channel load-balance** command.

**show port-channel load-balance** [**forwarding-path interface port-channel** *number* | **src-interface** *interface* { **vlan** *vlan\_ID* } [**dst-ip** *ipv4-addr*] [**dst-mac** *dst-mac-addr*] [**l4-dst-port** *dst-port*] [**l4-src-port** *src-port*] [**src-ip** *ipv4-addr*] [**src-mac** *src-mac-addr*]]

Syntax Description	
<b>forwarding-path interface port-channel</b>	(Optional) Identifies the port in the EtherChannel interface that forwards the packet.
<i>number</i>	EtherChannel number for the load-balancing forwarding path that you want to display. The range is from 1 to 4096.
<b>src-interface</b>	(Optional) Identifies the port in source interface interface that forwards the packet.
<i>interface</i>	Interface for the load-balancing forwarding path that you want to display.
<b>vlan</b>	(Optional) Identifies the VLAN for hardware hashing.
<i>vlan_ID</i>	VLAN ID. The range is from 1 to 3967 and 4048 to 4093.
<b>dst-ip</b>	(Optional) Displays the load distribution on the destination IP address.
<i>ipv4-addr</i>	IPv4 address to specify a source or destination IP address. The format is <i>A.B.C.D</i> .
<b>dst-mac</b>	(Optional) Displays the load distribution on the destination MAC address.
<i>dst-mac-addr</i>	Destination MAC address. The format is <i>AAAA:BBBB:CCCC</i> .
<b>l4-dst-port</b>	(Optional) Displays the load distribution on the destination port.
<i>dst-port</i>	Destination port number. The range is from 0 to 65535.
<b>l4-src-port</b>	(Optional) Displays the load distribution on the source port.
<i>src-port</i>	Source port number. The range is from 0 to 65535.
<b>src-ip</b>	(Optional) Displays the load distribution on the source IP address.
<b>src-mac</b>	(Optional) Displays the load distribution on the source MAC address.
<i>src-mac-addr</i>	source MAC address. The format is <i>AA:BB:CC:DD:EE:FF</i> .

**Command Default** None

**Command Modes** EXEC mode

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

**Usage Guidelines** You must use the **vlan** keyword to determine the use of hardware hashing.



**Note**

- Only hardware-based hashing is supported on Cisco Nexus 3548 Switch. There is no software hashing.
- For an L2 port, cache hit indicates that the source and destination mac addresses are learnt in the MAC table whereas for an L3 port cache hit indicates that the IP addresses are resolved.

When you do not use hardware hashing, the output displays all parameters used to determine the outgoing port ID. Missing parameters are shown as zero values in the output.

If you do not use hardware hashing, the outgoing port ID is determined by using control-plane selection. Hardware hashing is not used in the following scenarios:

- The specified VLAN contains an unknown unicast destination MAC address.
- The specified VLAN contains a known or an unknown multicast destination MAC or destination IP address.
- The specified VLAN contains a broadcast MAC address.
- The EtherChannel has only one active member.
- The destination MAC address is unknown when the load distribution is configured on the source IP address (src-ip), source port (l4-src-port), or source MAC address (src-mac).

To get accurate results, you must do the following:

- (For unicast frames) Provide the destination MAC address (dst-mac) and the VLAN for hardware hashing (vlan). When the destination MAC address is not provided, hardware hashing is assumed.
- (For multicast frames) For IP multicast, provide either the destination IP address (dst-ip) or destination MAC address (dst-mac) with the VLAN for hardware hashing (vlan). For non-ip multicast, provide the destination MAC address with the VLAN for hardware hashing.
- (For broadcast frames) Provide the destination MAC address (dst-mac) and the VLAN for hardware hashing (vlan).

**Examples**

This example shows how to display the port channel load balance information in wrap mode:

```
switch# show port-channel load-balance forwarding-path interface port-channel 1
src-interface ethernet 1/6 vlan 1 src-ip 1.1.1.1 dst-ip 2.2.2.2
Missing params will be substituted by 0's.
Load-balance Algorithm on switch: source-dest-ip
  Outgoing port id (no cache hit): Ethernet1/29
  Outgoing port id (cache hit): Ethernet1/32
Param(s) used to calculate load-balance:
  dst-ip: 2.2.2.2
  src-ip: 1.1.1.1
  dst-mac: 0000.0000.0000
  src-mac: 0000.0000.0000
  VLAN: 1
```

**Related Commands**

Command	Description
<b>port-channel</b>	Configures the load-balancing method among the interfaces in the channel-group bundle.
<b>load-balance ethernet</b>	

# show port-channel summary

To display summary information about EtherChannels, use the **show port-channel summary** command.

## show port-channel summary

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

**Command Default** None

**Command Modes** Global configuration mode  
EXEC mode

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

**Usage Guidelines** Before you use this command, you must configure an EtherChannel group using the **interface port-channel** command.

**Examples** This example shows how to display summary information about EtherChannels:

```
switch# show port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        S - Suspended    r - Module-removed
        S - Switched      R - Routed
        U - Up (port-channel)

-----
Group Port-      Type      Protocol  Member Ports
      Channel
-----
10    Po10 (SD)   Eth       NONE     --
switch#
```

Related Commands	Command	Description
	<b>channel-group (Ethernet)</b>	Assigns and configures a physical interface to an EtherChannel.
	<b>interface port-channel</b>	Creates an EtherChannel interface and enters interface configuration mode.

# show port-channel traffic

To display the traffic statistics for EtherChannels, use the **show port-channel traffic** command.

**show port-channel traffic** [**interface port-channel** *number*]

Syntax Description	<b>interface</b>	(Optional) Displays traffic statistics for a specified interface.
	<b>port-channel</b> <i>number</i>	(Optional) Displays information for a specified EtherChannel. The range is from 1 to 4096.

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

Command Modes	EXEC mode
---------------	-----------

Command History	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

Examples	This example shows how to display the traffic statistics for all EtherChannels:  switch# <b>show port-channel traffic</b>
	This example shows how to display the traffic statistics for a specific EtherChannel:  switch# <b>show port-channel traffic interface port-channel 10</b>

Related Commands	<b>Command</b>	<b>Description</b>
	<b>port-channel load-balance ethernet</b>	Configures the load-balancing algorithm for EtherChannels.
	<b>show tech-support port-channel</b>	Displays Cisco Technical Support information about EtherChannels.

# show port-channel usage

To display the range of used and unused EtherChannel numbers, use the **show port-channel usage** command.

**show port-channel usage**

---

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

---

**Command Default** None

---

**Command Modes** EXEC mode

---

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

---



---

**Examples** This example shows how to display the EtherChannel usage information:

```
switch# show port-channel usage
```

---

Related Commands	Command	Description
	<b>port-channel load-balance ethernet</b>	Configures the load-balancing algorithm for EtherChannels.
	<b>show tech-support port-channel</b>	Displays Cisco Technical Support information about EtherChannels.

---

# show resource

To display the number of resources currently available in the system, use the **show resource** command.

**show resource** [*resource*]

<b>Syntax Description</b>	<i>resource</i>	Resource name, which can be one of the following: <ul style="list-style-type: none"> <li>• <b>monitor-session</b>—Displays the number of sessions available in the system.</li> <li>• <b>port-channel</b>—Displays the number of EtherChannels available in the system.</li> <li>• <b>vlan</b>—Displays the number of VLANs available in the system.</li> <li>• <b>vrf</b>—Displays the number of virtual routing and forwardings (VRFs) available in the system.</li> </ul>
---------------------------	-----------------	--

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

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

**Examples** This example shows how to display the resources available in the system:

```
switch# show resource
```

Resource	Min	Max	Used	Unused	Avail
-----	----	----	----	-----	-----
vlan	16	4094	7	9	4041
monitor-session	0	4	0	0	4
vrf	2	1000	2	0	998
port-channel	0	32	0	0	32
u4route-mem	32	32	1	31	31
u6route-mem	16	16	1	15	15
m4route-mem	58	58	4	54	54
m6route-mem	8	8	0	8	8
bundle-map	0	32	0	0	32

```
switch#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show interface port-channel</b>	Displays information about EtherChannels.

# show running-config interface

To display the running configuration for a specific port channel, use the **show running-config interface** command.

**show running-config interface** [**all** | {**ethernet** {*slot/port*} [**all**]} | {**loopback** {*number*} [**all**]} | {**mgmt 0** [**all**]} | **port-channel** {*channel-number*} [**membership**]}]

<b>Syntax Description</b>	<b>all</b>	(Optional) Displays configured and default information.
	<b>ethernet</b> <i>slot/port</i>	Displays the Ethernet interface slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
	<b>loopback</b> <i>number</i>	Displays the number of the loopback interface. The range of values is from 1 to 4096.
	<b>mgmt 0</b>	Displays the configuration information of the management interface.
	<b>port-channel</b> <i>channel-number</i>	Displays the number of the port-channel group. The range of values is from 0 to 1023.
	<b>membership</b>	Displays the membership of the specified port channel.

**Command Default** None

**Command Modes** Any command mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(3)U21(1)	This command was introduced.

**Examples** This example shows how to display the running configuration for port channel 100 on a switch that runs Cisco NX-OS Release 5.0(3)A1(1):

```
switch(config)# show running-config interface port-channel 100

!Command: show running-config interface port-channel100
!Time: Tue Aug 23 09:25:00 2011

version 5.0(3)A1(1)

interface port-channel100
  speed 10000

switch(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show startup-config</b>	Displays the running configuration on the device.

# show running-config nat

To display the running configuration for Network Address Translation (NAT), use the **show running-config nat** command.

**show running-config nat [all]**

<b>Syntax Description</b>	<b>all</b> (Optional) Displays configured and default information.
---------------------------	--

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

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	6.0(2)A1(1)	This command was introduced.

**Examples** This example shows how to display the running configuration for NAT:

```
switch(config)# show running-config nat

!Command: show running-config nat
!Time: Thu Apr 24 04:06:59 2014

version 6.0(2)A3(1)
feature nat

ip nat inside source list list1 pool pool1
ip nat inside source list list2 pool pool2 overload
ip nat inside source list list7 pool pool7 overload
ip nat outside source list list3 pool pool3
ip nat pool pool1 30.1.1.1 30.1.1.2 prefix-length 24
ip nat pool pool2 10.1.1.1 10.1.1.2 netmask 255.0.255.0
ip nat pool pool3 30.1.1.1 30.1.1.8 prefix-length 24
ip nat pool pool5 20.1.1.1 20.1.1.5 netmask 255.0.255.0
ip nat pool pool7 netmask 255.255.0.0
    address 40.1.1.1 40.1.1.5
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>feature nat</b>	Enables NAT on the switch.
	<b>show ip nat translations</b>	Displays active NAT translations.

# show tech-support port-channel

To display troubleshooting information about EtherChannel interfaces, use the **show tech-support port-channel** command.

**show tech-support port-channel**

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

**Command Default** None

**Command Modes** EXEC mode

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

**Usage Guidelines** The output from the **show tech-support port-channel** command is very long. To better manage this output, you can redirect the output to a file.

**Examples** This example shows how to display Cisco technical support information for EtherChannel interfaces:

```
switch# show tech-support port-channel
`show port-channel internal event-history all`
Low Priority Pending queue: len(0), max len(1) [Fri May 28 11:07:02 2010]
High Priority Pending queue: len(0), max len(64) [Fri May 28 11:07:02 2010]
PCM Control Block info:
pcm_max_channels      : 4096
pcm_max_channel_in_use : 1
pc count              : 0
hif-pc count          : 0
Max PC Cnt            : 1600
=====
PORT CHANNELS:
=====

ALL PORTS:
Ethernet1/62
state      : down
update     : none
mode       : on
flags      :
cfg flags  :
up_time    : 0 usecs after Thu Jan  1 00:00:00 1970
auto pc    : none
<--Output truncated-->
switch#
```



Related Commands	Command	Description
	<b>port-channel load-balance ethernet</b>	Configures the load-balancing method among the interfaces in the channel-group bundle.
	<b>show port-channel load-balance</b>	Displays information on EtherChannel load balancing.

# show version

To display information about the software and hardware version, use the **show version** command.

## show version

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

**Command Default** All version information

**Command Modes** EXEC mode

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

**Examples** This example shows how to display the version information of a switch that runs Cisco NX-OS Release 5.0(3)A1(1):

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  BIOS:          version 1.8.0
  loader:        version N/A
  kickstart:     version 5.0(3)A1(1) [build 5.0(3)U2(0.125)]
  system:        version 5.0(3)A1(1) [build 5.0(3)U2(0.125)]
  power-seq:     Module 1: version v4.1
  BIOS compile time:    03/08/2011
  kickstart image file is: bootflash:///125.k
  kickstart compile time: 8/11/2011 16:00:00 [08/11/2011 23:16:27]
  system image file is:  bootflash:///125.s
  system compile time:   8/11/2011 16:00:00 [08/12/2011 00:09:45]

Hardware
  cisco Nexus3064 Chassis ("48x10GE + 16x10G/4x40G Supervisor")
  Intel(R) Celeron(R) CPU          with 4007288 kB of memory.
  Processor Board ID FOC152107X4

  Device name: BLR-QSP-5
  bootflash:   2007040 kB

Kernel uptime is 3 day(s), 5 hour(s), 7 minute(s), 7 second(s)
```

```
Last reset at 331149 usecs after Sat Aug 20 04:40:54 2011
```

```
Reason: Reset Requested by CLI command reload
System version: 5.0(3)A1(1)
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
switch#
```

# show vpc brief

To display brief information about the virtual port channels (vPCs), use the **show vpc brief** command.

**show vpc brief** [*vpc number*]

<b>Syntax Description</b>	<b>vpc number</b>	(Optional) Displays the brief information for the specified vPC. The range is from 1 to 4096.
---------------------------	-------------------	---

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

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	6.0(2)A3(1)	This command was introduced.

**Usage Guidelines** The **show vpc brief** command displays the vPC domain ID, the peer-link status, the keepalive message status, whether the configuration consistency is successful, and whether a peer link formed or failed to form.

This command is not available if you have not enabled the vPC feature. See the **feature vpc** command for information about enabling vPCs.

You can display the track object if you have configured a tracked object for running vPCs on a single module in the vpc-domain configuration mode.

**Examples** This example shows how to display brief information about the vPCs on a switch:

```
switch(config)# show vpc brief
```

Legend:

(\*) - local vPC is down, forwarding via vPC peer-link

```
vPC domain id           : 100
Peer status             : peer link not configured
vPC keep-alive status   : Disabled
Configuration consistency status: failed
Per-vlan consistency status : failed
Configuration consistency reason: vPC peer-link does not exist
Type-2 consistency status : failed
Type-2 consistency reason : vPC peer-link does not exist
vPC role                : none established
Number of vPCs configured : 0
Peer Gateway            : Enabled
Dual-active excluded VLANs : 200
Graceful Consistency Check : Disabled (due to peer configuration)
switch(config)#
```

Related Commands	Command	Description
	<b>feature vpc</b>	Enables vPCs on the device.
	<b>show port channel summary</b>	Displays information about port channels.
	<b>vpc</b>	Configures vPC domains and peers.

# show vpc consistency-parameters

To display the consistency of parameters that must be compatible across the virtual port-channel (vPC) interfaces, use the **show vpc consistency-parameters** command.

**show vpc consistency-parameters** { **global** | **interface** { **ethernet** *slot/port* | **port-channel** *channel-number* } | **vlan**s | **vpc** *number* }

Syntax Description		
<b>global</b>		Displays the configuration of all Type 1 global parameters on both sides of the vPC peer link.
<b>interface</b>		Displays the configuration for an Ethernet or EtherChannel interface on both sides of the vPC peer link.
<b>ethernet</b> <i>slot/port</i>		Displays the configuration of all Type 1 parameters for an Ethernet interface. The slot number is from 1 to 255, and the port number is from 1 to 128.
<b>port-channel</b> <i>channel-number</i>		Displays the configuration of all Type 1 parameters for an EtherChannel interface. The channel number is from 1 to 4096.
<b>vlan</b> s		Displays the configuration of all VLANs, including incompatible VLANs, on both sides of the vPC peer link for the specified vPC.
<b>vpc</b> <i>number</i>		Displays the configuration of all Type 1 interface parameters on both sides of the vPC peer link for the specified vPC.

**Command Default** None

**Command Modes** Any command mode

Command History	Release	Modification
	6.0(2)A3(1)	This command was introduced.

**Usage Guidelines** The **show vpc consistency-parameters** command displays the configuration of all the vPC Type 1 parameters on both sides of the vPC peer link.



## Note

All the Type 1 configurations must be identical on both sides of the vPC peer link, or the link will not come up.

The vPC Type 1 configuration parameters are as follows:

- Port-channel mode: on, off, or active
- Link speed per channel
- Duplex mode per channel
- Trunk mode per channel

- Native VLAN
- VLANs allowed on trunk
- Tagging of native VLAN traffic
- Spanning Tree Protocol (STP) mode
- STP region configuration for Multiple Spanning Tree
- Enable/disable state the same per VLAN
- STP global settings
  - Bridge Assurance setting
  - Port type setting—We recommend that you set all vPC peer link ports as network ports.
  - Loop Guard settings
- STP interface settings:
  - Port type setting
  - Loop Guard
  - Root Guard
- Maximum transmission unit (MTU)
- Allowed VLAN bit set

This command is not available if you have not enabled the vPC feature. See **feature vpc** for information on enabling vPCs.

### Examples

This example shows how to display the vPC global consistency parameters on a switch:

```
switch# show vpc consistency-parameters global
```

This example shows how to display the vPC consistency parameters for the specified port channel on a switch:

```
switch# show vpc consistency-parameters interface port-channel 10
```

This example shows how to display the vPC consistency parameters for the specified vPC on a switch:

```
switch# show vpc consistency-parameters vpc 5
```

This example shows how to display the vPC consistency parameters for VLANs on a switch:

```
switch# show vpc consistency-parameters vlans
```

### Related Commands

Command	Description
<b>show vpc brief</b>	Displays information about vPCs. If the feature is not enabled, the system displays an error when you enter this command.
<b>show port channel summary</b>	Displays information about port channels.
<b>vpc</b>	Configures vPC domains and peers.

# show vpc orphan-ports

To display ports that are not part of the virtual port channel (vPC) but have common VLANs, use the **show vpc orphan-ports** command.

**show vpc orphan-ports**

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

**Command Default** None

**Command Modes** Any command mode

Command History	Release	Modification
	6.0(2)A3(1)	This command was introduced.

**Usage Guidelines** The **show vpc orphan-ports** command displays those ports that are not part of the vPC but that share common VLANs with ports that are part of the vPC.

This command is not available if you have not enabled the vPC feature. See the **feature vpc** command for information about enabling vPCs.

**Examples** This example shows how to display vPC orphan ports:

```
switch(config)# show vpc orphan-ports
```

Related Commands	Command	Description
	<b>feature vpc</b>	Enables vPCs on the device.
	<b>vpc orphan-port suspend</b>	Suspends a non-vPC port.
	<b>show vpc brief</b>	Displays brief information about vPCs.



# show vpc peer-keepalive

To display the destination IP for the virtual port-channel (vPC) peer keepalive message and the status of the messages, use the **show vpc peer-keepalive** command.

## show vpc peer-keepalive

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

**Command Default** None

**Command Modes** Any command mode

Command History	Release	Modification
	6.0(2)A3(1)	This command was introduced.

**Usage Guidelines** The **show vpc peer-keepalive** command displays the destination IP of the peer keepalive message for the vPC. The command also displays the send and receive status as well as the last update from the peer in seconds and milliseconds.



### Note

We recommend that you create a separate VRF on the peer devices to send and receive the vPC peer keepalive messages. Do not use the peer link itself to send the vPC peer-keepalive messages.


This command is not available if you have not enabled the vPC feature. See the **feature vpc** command for information about enabling vPCs.

**Examples** This example shows how to display information about the peer-keepalive message:

```
switch# show vpc peer-keepalive

vPC keep-alive status           : Disabled
--Send status                   : Failed
--Receive status                : Failed
--Last update from peer        : (-n-a-) seconds, (-n-a-) msec

vPC Keep-alive parameters
--Destination                   : N/A
--Keepalive interval            : 1000 msec
--Keepalive timeout             : 5 seconds
--Keepalive hold timeout        : 3 seconds
--Keepalive vrf                 : management
--Keepalive udp port            : 3200
--Keepalive tos                 : 192
switch#
```

 show vpc peer-keepalive

Related Commands	Command	Description
	show vpc brief	Displays information about vPCs. If the feature is not enabled, the system displays an error when you enter this command.

# show vpc role

To display information about the virtual port-channel (vPC) role of the peer device, use the **show vpc role** command.

## show vpc role

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

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

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	6.0(2)A3(1)	This command was introduced.

<b>Usage Guidelines</b>	The <b>show vpc role</b> command displays the following information about the vPC status:
-------------------------	---

- Status of peer adjacency
- vPC role
- vPC MAC address
- vPC system priority
- MAC address of the device that you are working on
- System priority for the device that you are working on

This command is not available if you have not enabled the vPC feature. See the **feature vpc** command for information on enabling vPCs.

<b>Examples</b>	This example shows how to display the vPC role information of the device that you are working on:
-----------------	---

```
switch# show vpc role
```

```
vPC Role status
-----
vPC role                : none established
Dual Active Detection Status : 0
vPC system-mac          : 00:00:00:00:00:00
vPC system-priority     : 32667
vPC local system-mac    : 00:05:73:ff:5b:01
vPC local role-priority : 0
switch#
```

Related Commands	Command	Description
	<b>role</b>	Assigns a primary or secondary role to a vPC device.
	<b>show vpc brief</b>	Displays information about vPCs. If the feature is not enabled, the system displays an error when you enter this command.
	<b>show port channel summary</b>	Displays information about port channels.

# show vpc statistics

To display virtual port-channel (vPC) statistics, use the **show vpc statistics** command.

**show vpc statistics** {**peer-keepalive** | **peer-link** | **vpc number**}

Syntax Description	<b>peer-keepalive</b>	Displays statistics about the peer-keepalive message.
	<b>peer-link</b>	Displays statistics about the peer link.
	<b>vpc number</b>	Displays statistics about the specified vPC. The range is from 1 to 4096.

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

Command Modes	Any command mode
---------------	------------------


Command History	Release	Modification
	6.0(2)A3(1)	This command was introduced.

Usage Guidelines	The <b>peer-link</b> parameter displays the same information as the <b>show interface port-channel channel number</b> command for the vPC peer-link port channel.
	The <b>vpc number</b> parameter displays the same information as the <b>show interface port-channel channel number</b> command for the specified vPC port channel.
	This command is not available if you have not enabled the vPC feature. See the <b>feature vpc</b> command for information on enabling vPCs.

Examples	This example shows how to display statistics about the peer-keepalive message:
	<pre>switch# show vpc statistics peer-keepalive  vpc keep-alive status           : Suspended (Destination IP not reachable)  vpc keep-alive statistics ----- peer-keepalive tx count:         469 peer-keepalive rx count:         0 average interval for peer rx:    0 Count of peer timeouts:         0 switch(config)#</pre>

This example shows how to display statistics about a specific vPC:

```
switch# show vpc statistics vpc 5
```

 show vpc statistics

Related Commands	Command	Description
	show vpc brief	Displays information about vPCs. If the feature is not enabled, the system displays an error when you enter this command.
	show port channel summary	Displays information about port channels.

# shutdown

To shut down the local traffic on an Ethernet interface or Ethernet port-channel interface, use the **shutdown** command. To return the interface to its default operational state, use the **no** form of this command.

**shutdown**

**no shutdown**

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

<b>Command Default</b>	Not shut down
------------------------	---------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

<b>Usage Guidelines</b>	You can use this command on the following interfaces:
-------------------------	---

- Layer 2 interface
- Layer 3 interface



<b>Note</b>	Use the <b>no switchport</b> command to configure an interface as a Layer 3 interface.
-------------	--

- Layer 3 subinterface

This command does not require a license but if you want to enable Layer 3 interfaces, you must install the LAN Base Services license.

<b>Examples</b>	This example shows how to shut down, or disable, a Layer 2 interface:
-----------------	---

```
switch(config)# interface ethernet 1/10
switch(config-if)# shutdown
switch(config-if)#
```

This example shows how to shut down a Layer 3 Ethernet subinterface:

```
switch(config)# interface ethernet 1/5.1
switch(config-subif)# shutdown
switch(config-subif)#
```

Related Commands	Command	Description
	<b>no switchport</b>	Converts an interface to a Layer 3 routed interface.
	<b>show interface ethernet</b>	Displays the Ethernet interface configuration information.
	<b>show interface port-channel</b>	Displays information on traffic about the specified EtherChannel interface.



## speed (Ethernet)

To configure the transmit and receive speed for an Ethernet interface, use the **speed** command. To reset to the default speed, use the **no** form of this command.

**speed** { **10** | **100** | **1000** | **10000** | **40000** | **auto** }

**no speed**

Syntax Description		
	10	Sets the interface speed to 10 Mbps.
	100	Sets the interface speed to 100 Mbps.
	1000	Sets the interface speed to 1 Gbps.
	10000	Sets the interface speed to 10 Gbps. This is the default speed.
	40000	Sets the interface speed to 40 Gbps.
	auto	Sets the interface speed automatically.

**Command Default** The default speed is 10000 (10-Gigabit).

**Command Modes** Interface configuration mode

Command History	Release	Modification
	6.0(2)A1(1)	Added the <b>40000</b> keyword
	5.0(3)A1(1)	This command was introduced.

**Usage Guidelines** The default interface speed is 10-Gigabit. To configure these ports for 1-Gigabit Ethernet, insert a 1-Gigabit Ethernet SFP transceiver into the applicable port and then set its speed with the **speed** command.

You can enable 40-Gigabits per second (Gbps) speed on up to 12 interfaces. You enable 40-Gbps speed on the first port of a group of four adjacent ports. For example, you enable 40-Gbps speed only on port 1 of port group 1-4, port 5 of port group 5-8, and port 9 of port group 9-12, and so on. These ports are numbered in a 2-tuple naming convention and the first number in the 2-tuple is always 1. Hence, the 40-Gbps port numbering is Ethernet interface 1/1, 1/5, 1/9, 1/13, 1/17, and so on.

The configuration is applied to the first port, not to the remaining three ports in the group. The remaining ports act like the ports without an enhanced small form-factor pluggable (SFP+) transceiver inserted. The configuration takes effect immediately. You do not need to reload the switch.

An SFP+ transceiver security check is performed only on the first port of the group.

You can reconfigure interface speeds from 40-Gigabit to 10-Gigabit, and from 10-Gigabit back to 40-Gbps by using the **speed** command.

**Note**

If the interface and transceiver speed is mismatched, the SFP validation failed message is displayed when you enter the **show interface ethernet slot/port** command. For example, if you insert a 1-Gigabit SFP transceiver into a port without configuring the **speed 1000** command, you will get this error.

This command does not require a license.

**Examples**

This example shows how to set the speed for a 1-Gigabit Ethernet port:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# speed 1000
switch(config-if)#
```

This example shows how to set the speed for a 40-Gigabit Ethernet port:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# speed 40000
switch(config-if)#
```

**Related Commands**

Command	Description
<b>show interface</b>	Displays the interface configuration information.

# switchport host

To configure the interface to be an access host port, use the **switchport host** command. To remove the host port, use the **no** form of this command.

**switchport host**

**no switchport host**

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

**Command Default** None

**Command Modes** Interface configuration mode

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

**Usage Guidelines** Ensure that you are configuring the correct interface. It must be an interface that is connected to an end station.

An access host port handles the Spanning Tree Protocol (STP) like an edge port and immediately moves to the forwarding state without passing through the blocking and learning states. Configuring an interface as an access host port also disables EtherChannel on that interface.

This command does not require a license.

**Examples** This example shows how to set an interface as an Ethernet access host port with EtherChannel disabled:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# switchport host
switch(config-if)#
```

Related Commands	Command	Description
	<b>show interface brief</b>	Displays a summary of the interface configuration information.
	<b>show interface switchport</b>	Displays information on all interfaces configured as switch ports.

# switchport mode

To configure the interface as a nontrunking nontagged single-VLAN Ethernet interface, use the **switchport mode** command. To remove the configuration and restore the default, use the **no** form of this command.

**switchport mode** { **access** | **trunk** }

**no switchport mode** { **access** | **trunk** }

Syntax Description	<b>access</b>	Specifies that the interface is in access mode.
	<b>trunk</b>	Specifies that the interface is in trunk mode.

Command Default	An access port carries traffic for VLAN 1.
-----------------	--

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

Command History	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

**Usage Guidelines**

An access port can carry traffic in one VLAN only. By default, an access port carries traffic for VLAN 1. To set the access port to carry traffic for a different VLAN, use the **switchport access vlan** command. The VLAN must exist before you can specify that VLAN as an access VLAN. The system shuts down an access port that is assigned to an access VLAN that does not exist.

This command does not require a license.

**Examples**

This example shows how to set an interface as an Ethernet access port that carries traffic for a specific VLAN only:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 5
switch(config-if)#
```

Related Commands	<b>Command</b>	<b>Description</b>
	<b>show interface ethernet</b>	Displays information about a specified Ethernet interface.

Command	Description
<b>show interface switchport</b>	Displays information on all interfaces configured as switch ports.
<b>switchport access vlan</b>	Sets the access VLAN when the interface is in access mode.

# switchport trunk allowed vlan

To set the list of allowed VLANs on the trunking interface, use the **switchport trunk allowed vlan** command. To allow all VLANs on the trunking interface, use the **no** form of this command.

**switchport trunk allowed vlan** { *vlan-list* | **add** *vlan-list* | **all** | **except** *vlan-list* | **none** | **remove** *vlan-list* }

**no switchport trunk allowed vlan**

Syntax Description		
<i>vlan-list</i>		Allowed VLANs that transmit through this interface in tagged format when in trunking mode; the range of valid values is from 1 to 4094.
<b>add</b>		Adds the defined list of VLANs to those currently set instead of replacing the list.
<b>all</b>		Allows all appropriate VLANs to transmit through this interface in tagged format when in trunking mode.
<b>except</b>		Allows all VLANs to transmit through this interface in tagged format when in trunking mode except the specified values.
<b>none</b>		Blocks all VLANs transmitting through this interface in tagged format when in trunking mode.
<b>remove</b>		Removes the defined list of VLANs from those currently set instead of replacing the list.

**Defaults** No VLANs

**Command Modes** Interface configuration mode

**Supported Use Roles** network-admin

Command History	Release	Modification
	5.0(3)A1(1)	This command was introduced.

**Usage Guidelines** You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter the **switchport trunk allowed vlan** command. This action is required only if you have not entered the **switchport** command for the interface.

You can enter the **switchport trunk allowed vlan** command on interfaces where the Switched Port Analyzer (SPAN) destination port is either a trunk or an access port.

If you remove VLAN 1 from a trunk, the trunk interface continues to send and receive management traffic in VLAN 1.

When you create a switchport trunk, by default it is not a member of any VLAN. You must explicitly add VLANs to the trunk port for traffic on those VLANs to be allowed on the trunk port. To remove all allowed VLANs from a trunk port, use the **no** form of this command and the trunk port becomes a member of no VLANs.

This command does not require a license.

---

**Examples**

This example shows how to add a series of consecutive VLANs to the list of allowed VLANs on a trunking port:

```
switch(config-if)# switchport trunk allowed vlan add 40-50
```

---

**Related Commands**

Command	Description
<b>show interface switchport</b>	Displays the administrative and operational status of a switching (nonrouting) port.

# ttag

With Cisco Nexus 3500 platform switches, you can truncate the packets after a user-defined threshold at ingress and time-stamp the packets using Precision Time Protocol (PTP) with nanosecond accuracy.

---

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

---

**Command Default** None

---

**Command Modes** Interface configuration mode

---

**Usage Guidelines** With PTP, the IEEE 1588 packet is time-stamped at the ingress port to record the event message arrival time in the hardware at the parser level. The time stamp points to the first bit of the packet (following the start frame delimiter [SFD]). Next, the packet is copied to the CPU with the time stamp and the destination port number. The packet next traverses the PTP stack. The advanced PTP clock algorithm in the Cisco Nexus 3548 Series switches keeps a track of all the timing and the frequency information and it makes the necessary adjustments to help ensure accurate time.

Finally, the packet is internally marked as a high-priority packet to ensure priority egress out of the switch and it is sent out at the egress port. The corresponding time stamp for the transmitted packet is available from the First In, First Out (FIFO) transmission time stamp.

The timestamp tagging feature is used to provide precision time information to monitor the devices remotely and to track the real time when the packets arrive at the Cisco Nexus 3500 Series switches. The timestamp tagging feature configures the ttag command on the egress interface.

The **ether-type <type>** option sets the Ethertype field of the ethernet frame. The Ethertype is used to indicate which protocol is encapsulated in the payload. Ethertype 1 (type 0x88B5/0x88B6) is used for this purpose.

---

**Examples** This example shows how to configure timestamp tagging:

```
switch# hardware internal mtc-usd ttag-eth-type 0x88B5
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# ttag
switch(config-if)#
```

---

Related Commands	Command	Description
	<b>show interface brief</b>	Displays a summary of the interface configuration information.

---



# ttag-marker

To enable the timestamp tagging marker packet on the interface, use the **ttag-marker** command with **enable**. To disable the timestamp tagging marker packet on the interface, use the **no** form of this command:

**ttag-marker enable**

**no ttag-marker enable**

## Command Default

Enable	Disable/Enable marker packet on interface.
--------	--

## Command Default

Interface configuration mode

## Command History

Release	Modification
6.0(2)A8(1)	This command was introduced.

## Usage Guidelines

Once enabled on a Layer 2 port, the ttag marker sends out the periodic marker frames at specific intervals, based on the interval configured. The marker frame format includes the marker Ethertype that is followed by:

- 64 bit magic number
- 8 bit version
- 8 bit granularity
- 8 bit utc offset
- 16 bits reserved
- 48 bit timestamp (last 32 bits to be used)
- 32 bit utc\_sec
- 32 bit utc usec
- 32 bit reserved
- 32 bit signature

The actual ttag packet also contains the hardware timestamp. It is computed with the marker timestamp to calculate the latency of the packet.

The Ethertype that has to be taken for the marker frames can be specified manually, similar to ttag Ethertype.

The **ether-type** <type> option sets the Ethertype field of the Ethernet frame. The Ethertype is used to indicate which protocol is encapsulated in the payload. Ethertype 1 (type 0x88B5/0x88B6) is used for this purpose.

---

**Examples**

This example shows how to enable the timestamp tagging marker on the interface:

```
switch(config-if)# ttag-marker enable
switch(config-if)#
```

---

**Related Commands**

Command	Description
<b>show interface brief</b>	Displays a summary of the interface configuration information.

# ttag-marker-interval

To send out periodic timestamp tagging marker frames on an L2 port at specific intervals, use the `ttag-marker-interval` command:

**ttag-marker-interval seconds**

## Command Default

Interval	Interval time in seconds. Values: 1-4.
----------	--

## Command Default

1 Second

## Command Modes

Global configuration mode

## Command History

Release	Modification
6.0(2)A8(1)	This command was introduced.

## Usage Guidelines

The ttag marker interval once configured may not be effective unless the ttag marker is enabled on a specific Layer 2 interface. Once the ttag marker is enabled on the interface, the marker frames are sent out of the configured interface. The default interval is 1 second.

## Examples

This example shows how to specify the ttag marker interval to 4 seconds:

```
switch(config)# ttag-marker-interval 4
switch(config)#
```

## uddl (configuration mode)

To configure the Unidirectional Link Detection (UDLD) protocol on the switch, use the **uddl** command. To disable UDLD, use the **no** form of this command.

**uddl** { **aggressive** | **message-time** *timer-time* | **reset** }

**no uddl** { **aggressive** | **message-time** | **reset** }

<b>Syntax Description</b>	<b>aggressive</b>	Enables UDLD in aggressive mode on the switch.
	<b>message-time</b> <i>timer-time</i>	Sets the period of time between UDLD probe messages on ports that are in advertisement mode and are currently determined to be bidirectional. The range is from 7 to 90 seconds. The default is 15 seconds.
	<b>reset</b>	Resets all the ports that are shut down by UDLD and permit traffic to begin passing through them again. Other features, such as spanning tree, will behave normally if enabled.

**Command Default** Disabled

**Command Modes** Global configuration mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

**Usage Guidelines** UDLD aggressive mode is disabled by default. You can configure UDLD aggressive mode only on point-to-point links between network devices that support UDLD aggressive mode. If UDLD aggressive mode is enabled, when a port on a bidirectional link that has a UDLD neighbor relationship established stops receiving UDLD frames, UDLD tries to reestablish the connection with the neighbor. After eight failed retries, the port is disabled.

To prevent spanning tree loops, normal UDLD with the default interval of 15 seconds is fast enough to shut down a unidirectional link before a blocking port transitions to the forwarding state (with default spanning tree parameters).

When you enable the UDLD aggressive mode, the following occurs:

- One side of a link has a port stuck (both transmission and receive)
- One side of a link remains up while the other side of the link is down

In these cases, the UDLD aggressive mode disables one of the ports on the link, which prevents traffic from being discarded.

This command does not require a license.

---

**Examples**

This example shows how to enable the aggressive UDLD mode for the switch:

```
switch# configure terminal
switch(config)# udld aggressive
switch(config)#
```

This example shows how to reset all ports that were shut down by UDLD:

```
switch# configure terminal
switch(config)# udld reset
switch(config)#
```

---

**Related Commands**

Command	Description
<b>show udld</b>	Displays the administrative and operational UDLD status.

# uddl (Ethernet)

To enable and configure the Unidirectional Link Detection (UDLD) protocol on an Ethernet interface, use the **uddl** command. To disable UDLD, use the **no** form of this command.

**uddl {aggressive | disable | enable}**

**no uddl {aggressive | disable | enable}**

Syntax Description	<b>aggressive</b>	Enables UDLD in aggressive mode on the interface.
	<b>disable</b>	Disables UDLD on the interface.
	<b>enable</b>	Enables UDLD in normal mode on the interface.

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

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

Command History	<b>Release</b>	<b>Modification</b>
	5.0(3)A1(1)	This command was introduced.

**Usage Guidelines**

You can configure normal or aggressive UDLD modes for an Ethernet interface. Before you can enable a UDLD mode for an interface, you must make sure that UDLD is enabled on the switch. UDLD must also be enabled on the other linked interface and its device.

To use the normal UDLD mode on a link, you must configure one of the ports for normal mode and configure the port on the other end for the normal or aggressive mode. To use the aggressive UDLD mode, you must configure both ends of the link for aggressive mode.

This command does not require a license.

**Examples**

This example shows how to enable the normal UDLD mode for an Ethernet port:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# uddl enable
switch(config-if)#
```

This example shows how to enable the aggressive UDLD mode for an Ethernet port:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# uddl aggressive
switch(config-if)#
```

This example shows how to disable UDLD for an Ethernet port:

```
switch# configure terminal
```

```
switch(config)# interface ethernet 1/1
switch(config-if)# udld disable
switch(config-if)#
```

**Related Commands**



Command	Description
<b>show udld</b>	Displays the administrative and operational UDLD status.

# vpc

To move other port channels into a virtual port channel (vPC) to connect to the downstream device, use the **vpc** command. To remove the port channels from the vPC, use the **no** form of this command.

**vpc** *number*

**no vpc** *number*

<b>Syntax Description</b>	<table> <tr> <td data-bbox="342 543 618 583"><i>number</i></td><td data-bbox="618 543 1479 611">Port channel number to connect to the downstream device. The range is from 1 to 4096.</td></tr> <tr> <td data-bbox="342 611 618 730"><b>Note</b></td><td data-bbox="618 611 1479 730">The vPC number that you assign to the port channel that connects to the downstream device from the vPC peer device must be identical on both vPC peer devices.</td></tr> </table>	<i>number</i>	Port channel number to connect to the downstream device. The range is from 1 to 4096.	<b>Note</b>	The vPC number that you assign to the port channel that connects to the downstream device from the vPC peer device must be identical on both vPC peer devices.
<i>number</i>	Port channel number to connect to the downstream device. The range is from 1 to 4096.				
<b>Note</b>	The vPC number that you assign to the port channel that connects to the downstream device from the vPC peer device must be identical on both vPC peer devices.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Interface configuration mode				
<b>Command History</b>	<table> <tr> <th data-bbox="342 1018 618 1058">Release</th><th data-bbox="618 1018 1479 1058">Modification</th></tr> <tr> <td data-bbox="342 1058 618 1108">6.0(2)A3(1)</td><td data-bbox="618 1058 1479 1108">This command was introduced.</td></tr> </table>	Release	Modification	6.0(2)A3(1)	This command was introduced.
Release	Modification				
6.0(2)A3(1)	This command was introduced.				
<b>Usage Guidelines</b>	You can use any module in the device for the port channels.				
<div data-bbox="250 1234 302 1276"></div> <div data-bbox="250 1276 302 1308"><b>Note</b></div>	<div data-bbox="342 1276 1479 1308">We recommend that you attach the vPC domain downstream port channel to two devices for redundancy.</div> <div data-bbox="342 1346 1479 1507">To connect to the downstream device, you create a port channel from the downstream device to the primary vPC peer device, and you create another port channel from the downstream device to the secondary peer device. Finally, working on each vPC peer device, you assign a vPC number to the port channel that connects to the downstream device. You will experience minimal traffic disruption when you are creating vPCs.</div> <div data-bbox="250 1524 302 1566"></div> <div data-bbox="250 1566 302 1598"><b>Note</b></div> <div data-bbox="342 1566 1479 1640">The port channel number and vPC number can be different, but the vPC number must be the same on both switches.</div>				
<b>Examples</b>	<p>This example shows how to configure the selected port channel into the vPC to connect to the downstream device:</p> <pre>switch# configure terminal switch(config)# interface port-channel 20 switch(config-if)# vpc 5 switch(config-if)#</pre>				



Related Commands	Command	Description
	<b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.
	<b>show running-config vpc</b>	Displays the running configuration information for vPCs.
	<b>show vpc brief</b>	Displays information about each vPC, including information about the vPC peer link.
	<b>show vpc consistency-parameters</b>	Displays the status of those parameters that must be consistent across all vPC interfaces.

# vpc domain

To create a virtual port channel (vPC) domain and assign a domain ID, use the **vpc domain** command. To revert to the default vPC configuration, use the **no** form of this command.

```
vpc domain domain_id

no vpc domain domain_id
```

Syntax Description	domain_id	vPC domain ID. The range is from 1 to 1000.
--------------------	-----------	---

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

Command Modes	Global configuration mode
---------------	---------------------------

Command History	Release	Modification
	6.0(2)A3(1)	This command was introduced.

**Usage Guidelines**

Before you can create a vPC domain and configure vPC on the switch, you must enable the vPC feature using the **feature vpc** command.

The vPC domain includes both vPC peer devices, the vPC peer keepalive link, the vPC peer link, and all the port channels in the vPC domain connected to the downstream device. You can have only one vPC domain ID on each device.

When configuring the vPC domain ID, make sure that the ID is different from the ID used by a neighboring vPC-capable device with which you may configure a double-sided vPC. This unique ID is needed because the system ID is derived from the MAC address ID of the switch. For a vPC, this MAC address is derived from the domain ID. As a result, in a peer-to-peer vPC configuration, if the neighboring switches use the same domain ID, a system ID conflict may occur in the LACP negotiation that may cause an unsuccessful LACP negotiation.

Under the vPC domain, make sure to configure the primary vPC device to ignore type checks by using the **peer-config-check-bypass** command.

**Examples**

This example shows how to create a vPC domain:

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)#
```

Related Commands	Command	Description
	<b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.
	<b>feature vpc</b>	Enables or disables a vPC on the switch.
	<b>peer-config-check-bypass</b>	Ignores type checks on primary when the MCT is down.
	<b>peer-keepalive</b>	Configures the vPC peer keepalive link.
	<b>reload restore</b>	Restores the vPC peer links after a specified period of time.
	<b>role priority</b>	Configures the role priority for the vPC device.
	<b>show vpc brief</b>	Displays brief information about each vPC domain.

# vpc peer-link

To create a virtual port channel (vPC) peer link by designating the port channel that you want on each device as the peer link for the specified vPC domain, use the **vpc peer-link** command. To remove the peer link, use the **no** form of this command.

**vpc peer-link**

**no vpc peer-link**

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

**Command Default** None

**Command Modes** Interface configuration mode

Command History	Release	Modification
	6.0(2)A3(1)	This command was introduced.

**Usage Guidelines**

We recommend that you configure the Layer 2 port channels that you are designating as the vPC peer link in trunk mode and that you use two ports on separate modules on each vPC peer device for redundancy.

The Cisco Nexus 3000 Series switch supports 64 hardware port channels. Use the **show port-channel capacity** command to display the total number of port channels supported by the hardware.

**Examples**

This example shows how to select the port channel that you want to use as the vPC peer link for this device and configure the selected port channel as the vPC peer link:

```
switch# configure terminal
switch(config)# interface port-channel 20
switch(config-if)# vpc peer-link
switch(config-if)#
```

This example shows how to remove the vPC peer link:

```
switch# configure terminal
switch(config)# interface port-channel 20
switch(config-if)# no vpc peer-link
switch(config-if)#
```

Related Commands	Command	Description
	<b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.
	<b>reload restore</b>	Restores the vPC peer links after a specified period of time.
	<b>show port-channel capacity</b>	Reports the number of port channels that are configured and the number of port channels that are still available on the device.
	<b>show running-config vpc</b>	Displays the running configuration information for vPCs.
	<b>show vpc brief</b>	Displays a brief information about the vPCs.
	<b>show vpc brief</b>	Displays information about each vPC, including information about the vPC peer link.
	<b>show vpc peer-keepalive</b>	Displays information on the peer-keepalive messages.

