Cisco NX-OS Interfaces Commands

This chapter describes the Cisco NX-OS interfaces commands for the Cisco Nexus 7000 Series devices.

auto-recovery

To configure the virtual port channel (vPC) for auto recovery if its peer is presumed nonoperational, use the **auto-recovery** command. To reset the vPC to the standard behavior, use the **no** form of this command.

auto-recovery reload-delay *time-out-value*

no auto-recovery reload-delay *time-out-value*

Syntax Description

reload-delay	Specifies the duration to wait after reload to recovery vPCs.
time-out-value	Timeout value for restoring vPC links in seconds. The range is from 240 to 3600.

Defaults

None

Command Modes

VPC domain configuration mode (config-vpc-domain)

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the vPC for auto recovery:

```
switch# configure terminal
switch(config)# vpc domain 1
switch(config-vpc-domain)# auto-recovery reload-delay 350
Warning:
 Enables restoring of vPCs in a peer-detached state after reload, will wait for
350 seconds to determine if peer is un-reachable
switch(config-vpc-domain)#
```

This example shows how to revert the vPC to the standard behavior:

```
switch# configure terminal
switch(config)# vpc domain 1
switch(config-vpc-domain)# no auto-recovery reload-delay 350
switch(config-vpc-domain)#
```

Related Commands

Command	Description
vpc	Moves other port channels into the vPC.
vpc domain	Creates a vPC domain.

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

kbps	Intended bandwidth, in kilobits per second. The range is from 1 to 10000000.
inherit	(Optional) Specifies the inherited bandwidth such as how a subinterface inherits the bandwidth of its main interface.

Defaults

1000000 kbps

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

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.

Note This is a routing parameter only. It does not affect the physical interface.

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 inherit the current bandwidth of the main interface. If you configure a new bandwidth on the main interface, all subinterfaces 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 inherit the specified bandwidth.

In all cases, if an interface has an explicit bandwidth setting configured, that interface uses 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 all subinterfaces off this main interface to inherit the configured bandwidth:

```
switch(config-if)# bandwidth inherit 30000
```

Related Commands

Command	Description
show interface	Displays the interface configuration information.

bfd

To enable Bidirectional Forwarding Detection (BFD) for a protocol, use the **bfd** command. To disable BFD for a protocol, use the **no** form of this command.

bfd

no bfd

Syntax Description

This command has no arguments or keywords.

Defaults

BFD is not enabled on the protocol.

Command Modes

Router configuration mode
Neighbor configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

There are two methods to configure protocols to use BFD for failure detection. To enable BFD for all neighbors or interfaces of a protocol, enter the **bfd** command in router configuration mode for the Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPFv2), Open Shortest Path First (OSPFv3) and Intermediate-System-to-Intermediate-System (IS-IS) or in neighbor configuration mode for the Border Gateway Protocol (BGP). If you do not want to enable BFD on all interfaces, see the interface-level BFD enable commands in the Related Commands section.

Examples

This example shows how to enable BFD for all EIGRP neighbors:

```
switch# configure terminal
switch(config)# router eigrp Test1
switch(config-router)# bfd
```

This example shows how to enable BFD for all BGP neighbors:

```
switch# configure terminal
switch(config)# router bgp 1.1
switch(config-router)# neighbor 192.0.2.1 remote-as 1.0
switch(config-router-neighbor)# bfd
```

Related Commands

Command	Description
hsrp bfd	Enables BFD on an HSRP interface.
ip eigrp bfd	Enables BFD on an EIGRP interface.

Command	Description
ip ospf bfd	Enables BFD on an OSPFv2 interface.
isis bfd	Enables BFD on an IS-IS interface.

bfd authentication

To configure SHA-1 authentication for all Bidirectional Forwarding Detection (BFD) sessions on the interface, use the **bfd authentication** command. To remove the SHA-1 authentication configuration, use the **no** form of this command.

bfd [**ipv4 | ipv6**] **authentication keyed-SHA1 key-id** *id hex-key* **key** *ascii-key*

no bfd [**ipv4 | ipv6**] **authentication keyed-SHA1 key-id** *id* **key** *ascii-key*

Syntax Description

ipv4	(Optional) Enables BFD authentication for the IPv4 address.
ipv6	(Optional) Enables BFD authentication for the IPv6 IP address.
key-id	Specifies the key ID to use in BFD frames.
id	Key ID value. The range is from 1 to 255.
hex-key	HEX binary SHA1 secret. A hex-key can be any case-sensitive, alphanumeric string up to 40 characters.
key	Specifies the ASCII SHA1 secret.
ascii-key	SHA1 secret value. An ASCII key can be any case-sensitive, alphanumeric string up to 20 characters.

Defaults

None

Command Modes

Interface configuration mode (config-if)

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	Added **ipv4**, **ipv6** keywords to the syntax description.
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure SHA-1 authentication for all BFD sessions on the interface:

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# bfd authentication keyed-SHA1 key-id 23 key cisco123
switch(config-if)#
```

This example shows how to disable SHA-1 authentication on the interface:

```
switch(config-if)# no bfd authentication keyed-SHA1 key-id 23 key cisco123
switch(config-if)#
```

Related Commands

Command	Description
show running-config bfd	Displays the BFD running configuration.
show running-config interface	Displays the running configuration for a specific interface.

bfd echo

To enable Bidirectional Forwarding Detection (BFD) echo mode, use the **bfd echo** command. To disable BFD echo mode, use the **no** form of this command.

bfd [**ipv4** |**ipv6**] **echo**

no bfd [**ipv4** | **ipv6**] **echo**

Syntax Description

ipv4	(Optional) Enables BFD echo mode for the IPv4 address.
ipv6	(Optional) Enables BFD echo mode for the IPv6 address.

Defaults

BFD echo mode is enabled by default.

Command Modes

Interface configuration mode (config-if)

Command History

Release	Modification
6.2(2)	Added **ipv4**, **ipv6** keywords to the syntax description.
5.0(2)	This command was introduced.

Usage Guidelines

When echo mode is enabled, the required minimum receive interval value is taken from the BFD slow-timer setting.

Note Before using BFD echo mode, you must disable the IP packet verification check for identical IP source and destination addresses by entering the **no hardware ip verify address identical** command in the default virtual device context (VDC).

Note Before using BFD echo mode, you must disable the sending of Internet Control Message Protocol (ICMP) redirect messages by entering the **no ip redirects** command.

Use the **no bfd echo** command to stop sending echo packets and signify that the device is unwilling to forward echo packets that are received from BFD neighbors. The RequiredMinEchoRx BFD session parameter is set to zero when echo mode is disabled.

This command does not require a license.

Examples

This example shows how to configure BFD echo mode:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# bfd ipv4 echo
```

This example shows that the BFD session neighbor is up and using BFD echo mode. The relevant command output is shown in bold in the output:

```
switch# show bfd neighbors details
OurAddr       NeighAddr      LD/RD  RH/RS    Holdown(mult)State    Int
172.16.1.2    172.16.1.1     1/6    Up       0    (3 )    Up       Fa0/1
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
Uptime: 00:05:00
Last packet: Version: 1            - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 6          - Your Discr.: 1
             Min tx interval: 1000000    - Min rx interval: 1000000
             Min Echo interval: 50000
```

Related Commands

Command	Description
bfd interval	Configures the BFD session parameters.
bfd slow-timer	Configures the BFD RequiredminEchoRx interval.
feature bfd	Enables the BFD feature.
hardware ip verify address identical	Enables the verification of IP packets do not have the same address for IP source and IP destination fields.
ip redirects	Enables the sending of ICMP redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received.

bfd interval

To configure the Bidirectional Forwarding Detection (BFD) session parameters, use the **bfd interval** command. To return to the default setting, use the **no** form of this command.

bfd [**ipv4 | ipv6**] **interval** *mintx* **min_rx** *msec* **multiplier** *value*

no bfd [**ipv4 | ipv6**] **interval** *mintx* **min_rx** *msec* **multiplier** *value*

Syntax Description

ipv4	(Optional) Configures BFD session parameters for the IPv4 address.
ipv6	(Optional) Configures BFD session parameters for the IPv6 address.
mintx	Rate at which BFD control packets are sent to BFD neighbors. The configurable range is from 50 to 999.
min_rx *msec*	Specifies the rate at which BFD control packets are expected to be received from BFD neighbors. The range is from 50 to 999.
multiplier *value*	Specifies the number of consecutive BFD control packets that must be missed from a BFD neighbor before BFD declares that the neighbor is unavailable and the BFD neighbor is informed of the failure. The range is from 1 to 50.

Defaults

BFD interval: 50 milliseconds
min_rx: 50 milliseconds
multiplier: 3

Command Modes

Global configuration mode
Interface configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	Added **ipv4**, **ipv6** keywords to the syntax description.
5.0(2)	This command was introduced.

Usage Guidelines

BFD session parameters configured at the interface level take precedence over the globally configured BFD session parameters.

This command does not require a license.

Examples

This example shows how to set the BFD session parameters for Ethernet interface 3/1:

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# bfd ipv6 interval 50 min_rx 20 multiplier 3
```

Related Commands

Command	Description
feature bfd	Enables the BFD feature.
show bfd neighbors	Displays information about BFD neighbors.

bfd optimize subinterfaces

To optimize subinterfaces on a physical interface for Bidirectional Forwarding Detection (BFD), use the **bfd optimize subinterfaces** command. To return to the default setting, use the **no** form of this command.

bfd optimize subinterfaces

no bfd optimize subinterfaces

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You can optimize subinterfaces, because BFD creates sessions for all configured subinterfaces. BFD sets the subinterface with the lowest configured VLAN ID as the master subinterface and that subinterface uses the BFD session parameters of the parent interface. The remaining subinterfaces use the slow timer. If the master subinterface session detects an error, BFD marks all subinterfaces on that physical interface as down.

When the lowest configured VLAN has both an IPv4 and an IPv6 BFD session, there is no deterministic way to say which of the two sessions is always chosen as the master session.

This command does not require a license.

Examples

This example shows how to enable subinterface optimization:

```
switch(config)# interface Ethernet 1/1
switch(config-if)# bfd optimize subinterfaces
```

Related Commands

Command	Description
feature bfd	Enables the BFD feature.

bfd per-link

To enable Bidirectional Forwarding Detection (BFD) for all links in a port channel, use the **bfd per-link** command. To disable BFD for a port channel, use the **no** form of this command.

bfd per-link

no bfd per-link

Syntax Description

This command has no arguments or keywords.

Defaults

BFD is not enabled on the port channel.

Command Modes

Port channel configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

Use the **bfd per-link** command to enable BFD on each link in a port channel. BFD creates a session for each link in the port channel and provides an aggregate result to client protocols. For example, if the BFD session for one link on a port channel is up, BFD informs client protocols such as Open Shortest Path First (OSPF) that the port channel is up. The BFD session parameters are negotiated between the BFD peers in a three-way handshake.

bfd Per-link is not allowed with echo mode, or when there are BFD sessions on the port-channel. The port-channel must be shutdown before configuring per-link.

This command does not require a license.

Examples

This example shows how to enable BFD for port channel 3:

```
switch# configure terminal
switch(config)# interface port-channel 3
switch(config)# shutdown
switch(config-if)# bfd per-link
```

This example shows how to configure the BFD session parameters for a port channel:

```
switch# configure terminal
switch(config)# interface port-channel 3
switch(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

Related Commands

Command	Description
bfd echo	Enables BFD echo mode.
bfd interval	Configures the BFD session parameters
feature bfd	Enables the BFD feature.

bfd slow-timer

To configure the Bidirectional Forwarding Detection (BFD) slow timer value, use the **bfd slow-timer** command. To return to the default setting, use the **no** form of this command.

bfd [**ipv4 | ipv6**] **slow-timer** *milliseconds*

no [**ipv4 | ipv6**] **bfd slow-timer** *milliseconds*

Syntax Description

ipv4	Configures the slow timer in milliseconds, used in the echo function for the IPv4 address.
ipv6	Configures the slow timer in milliseconds, used in the echo function for the IPv6 address.
milliseconds	BFD slow timer value, in milliseconds. The range is from 1000 to 30000.

Defaults

The default BFD slow timer value is 2000 milliseconds.

Command Modes

Global configuration mode
Interface configuration mode

Command History

Release	Modification
6.2(2)	Added **ipv4**, **ipv6** keywords to the syntax description.
5.0(2)	This command was introduced.

Usage Guidelines

Use the **bfd slow-timer** command to configure how fast a BFD session comes up. This value also sets the RequiredMinRx (or min_rx) value when echo mode is enabled.

This command does not require a license.

Examples

This example shows that the BFD slow timer value is configured to 14,000 milliseconds for IPv6:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# bfd ipv6 slow-timer 14000
switch(config-if)#
```

This example shows that the BFD slow timer value of 14,000 milliseconds has been implemented. The values for the MinTxInt and MinRxInt correspond to the configured value for the BFD slow timer. The relevant command output is shown in bold.

```
switch# show bfd neighbors details

OurAddr       NeighAddr     LD/RD  RH/RS   Holdown(mult)  State     Int
172.16.10.1   172.16.10.2   1/1    Up      0    (3 )      Up        Et2/0
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
```

```
MinTxInt: 14000, MinRxInt: 14000, Multiplier: 3
Received MinRxInt: 10000, Received Multiplier: 3
Holdown (hits): 3600(0), Hello (hits): 1200(418)
Rx Count: 422, Rx Interval (ms) min/max/avg: 1/1480/1087 last: 112 ms ago
Tx Count: 420, Tx Interval (ms) min/max/avg: 1/2088/1090 last: 872 ms ago
Registered protocols: OSPF
Uptime: 00:07:37
Last packet: Version: 1            - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 1          - Your Discr.: 1
             Min tx interval: 14000 - Min rx interval: 14000
             Min Echo interval: 4000
```

Related Commands

Command	Description
bfd echo	Enables BFD echo mode.

carrier-delay

To set the carrier delay on an interface, use the **carrier-delay** command. To return to the default carrier delay value, use the **no** form of this command.

carrier-delay {*sec* | {**msec** *value*}}

no carrier-delay

Syntax Description

sec	Seconds of delay. The range is from 0 to 60.
msec	Specifies milliseconds of delay.
value	Milliseconds of delay. The range is from 0 to 1000.

Defaults

The default is 2 seconds or 100 milliseconds.

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0(3)	This command was introduced.

Usage Guidelines

Note You must enable the VLAN interface feature, using the **feature interface-vla**n command, before you can use this command.

If a link goes down and comes back up before the carrier delay timer expires, the down state is effectively filtered, and the rest of the software on the device is not aware that a link-down event occurred. A large carrier delay timer results in fewer link-up/link-down events being detected. When you set the carrier delay time to 0, the device detects each link-up/link-down event that occurs.

Note The **carrier-delay** command is supported only on the VLAN interface mode; no other interface modes support this command.

In most environments, a lower carrier delay time is better than a higher one. The value that you choose depends on the nature of the link outages and how long you expect these linkages to last in your network. If your data links are subject to short outages (especially if those outages last less time than it takes for your IP routing to converge), you should set a long carrier delay value to prevent these short outages

from causing unnecessary churn in your routing tables. However, if you outages tend to be longer, then you may want to set a shorter carrier delay time so that the outages are detected sooner, and the IP route convergence begins and ends sooner.

This command does not require a license.

Examples

This example shows how to set the carrier delay timer to 20 minutes for VLAN 6:

```
switch(config)# interface vlan 6
switch(config-if)# carrier-delay 20
switch(config-if)#
```

Related Commands

Command	Description
show interface vlan	Displays information about VLAN interfaces.

channel-group

To assign and configure a physical interface to a port-channel group, 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

number	Number of the channel group. The maximum number of port channels that can be configured is 256 across all virtual device contexts (VDCs), and the range is from 1 to 4096.
force	(Optional) Forces the interface to join the channel group, although some parameters are not compatible. For information on the compatibility parameters and which ones can be forced, see the Usage Guidelines section.
mode	Specifies the port-channel mode of the interface.
active	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.
on	Specifies the default channel mode and all port channels 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 device returns an error message. 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 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. The default mode is **on**.
passive	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.

Defaults

None

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	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 device automatically removes the specified port from its present channel group and adds that port to 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**. A port channel in the **on** channel mode is a pure port channel and can aggregate a maximum of eight ports. It does not run LACP.

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

All ports in one port channel must be in the same virtual device context (VDC). With LACP enabled, this requirement applies to the possible eight active ports and the possible eight standby ports. The port channels can originate in one VDC (with all ports in that channel in the same VDC) and partner with a port channel in another VDC (again, all ports in that channel must be in that VDC).

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

The compatibility check includes the following operational attributes:

- Network layer
- (Link) speed capability
- Speed configuration
- Duplex capability
- Duplex configuration
- Port mode
- Access VLAN
- Trunk native VLAN
- Tagged or untagged
- Allowed VLAN list
- MTU size
- SPAN—Cannot be a SPAN source or destination port
- Layer 3 Ports—Cannot have subinterfaces
- Storm control
- Flow control capability
- Flow control configuration

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

You can only add interfaces configured with the channel mode set to **on** to static port channels, that is without a configured aggregation protocol and you can only add interfaces configured with the channel mode as **active** or **passive** to port channels 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 port channel.

Alternatively, you can force ports with incompatible parameters to join the port channel as long the following parameters are the same:

- (Link) speed capability
- Speed configuration
- Duplex capability
- Duplex configuration
- Flow control capability
- Flow control configuration

When the interface joins a port channel, some of its individual parameters are removed and replaced with the values on the port channel as follows:

- Bandwidth
- Delay
- Extended Authentication Protocol over UDP
- VRF
- IP address (v4 and v6)
- MAC address
- Spanning Tree Protocol
- NAC
- Service policy
- Quality of Service (QoS)
- ACLs

Many of the following interface parameters remain unaffected when the interface joins or leaves a port channel:

- Beacon
- Description
- CDP
- LACP port priority
- Debounce
- UDLD
- MDIX
- Rate mode
- Shutdown
- SNMP trap

If subinterfaces are configured for the port-channel interface and a member port is removed from the port channel, the configuration of the port-channel subinterface is not propagated to the member ports.

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

You do not have to create a port-channel interface before you assign a physical interface to a channel group. A port-channel interface is created automatically when the channel group gets its first physical interface, if it is not already created.

You can create either a Layer 2 or a Layer 3 port channel by entering the **interface port-channel** command or when the channel group gets its first physical interface assignment. The port channels are not created at run time or dynamically.

Note The number of ports allowed in a port channel (for the ON mode) is different between M1 Series modules and F1 Series modules on VDCs only. The number is 8 for M1 Series modules or M1-F1 Series VDCs and 16 for F1 Series modules.

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(config-if)# channel-group 5 mode active
switch(config-if)#
```

Related Commands

Command	Description
show interface port-channel	Displays information about the traffic on the specified port-channel interface.
show lacp	Displays LACP information.
show port-channel summary	Displays information about the port channels.

clear counters interface

To clear the Ethernet and management interface counters, use the **clear counters interface** command.

clear counters interface {**all** [**snmp**]| **ethernet** *slot/port* | **loopback** *number* | **mgmt** *number* | **port-channel** *channel-number* | **tunnel** *tunnel-number* | **vlan** *vlan-number*}

Syntax Description

all	Clears all interface counters.
snmp	(Optional) clears SNMP interface counters.
ethernet *slot/port*	Clears the Ethernet interface counter for the slot number and port number specified.
loopback *number*	Clears the loopback interface counter for the virtual interface number specified. The range is from 0 to 1023.
mgmt *number*	Clears the management interface counter for the number specified. The number is 0.
port-channel *channel-number*	Clears the port-channel interface for the number specified. The range is from 1 to 4096.
tunnel *tunnel-number*	Clears the port-channel interface for the number specified. The range is from 0 to 65535.
vlan *vlan-number*	Clears the port-channel interface for the number specified. The range is from 1 to 4096.

Defaults

None

Command Modes

Global configuration mode
Interface Configuration mode.

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	Added the **snmp** keyword to the syntax description.
4.0	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear an SNMP counter interface:

```
switch# clear counters interface all snmp
```

This example shows how to clear and reset the counters on Ethernet port 5/5:

```
switch# clear counters interface ethernet 5/5
```

Related Commands

Command	Description
show interface counters	Displays in and out counters for all interfaces in the system.

clear l2protocol tunnel counters

To clear the Layer 2 protocol tunnel statistics counters, use the **clear l2protocol tunnel counters** command.

clear l2protocol tunnel counters [**interface** *if-range*]

Syntax Description

interface	(Optional) Specifies the interface statistics to clear.
if-range	Range of interfaces.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

If no interfaces are specified, the Layer 2 protocol tunnel statistics are cleared for all interfaces.

This command does not require a license.

Examples

This example shows how to clear the Layer 2 protocol tunnel statistics counters:

```
switch# clear l2protocol tunnel counters
```

RelatedCommands

Command	Description
show l2protocol tunnel	Displays Layer 2 protocol tunnel information.

clear lacp counters

To clear the statistics for all interfaces for Link Aggregation Control Protocol (LACP) groups, use the **clear lacp counters** command.

clear lacp counters [**interface port-channel** *channel-number*]

Syntax Description

interface port-channel	(Optional) Specifies the interface port channel.
channel-number	(Optional) LACP port-channel number. The range is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

If you enter this command for a static port-channel group without enabling the aggregation protocol, the device ignores the command.

If you do not specify a channel number, the LACP counters for all LACP port groups are cleared.

This command does not require a license.

Examples

This example shows how to clear all LACP counters:

```
switch(config)# clear lacp counters
switch(config) #
```

This example shows how to clear all LACP counters for the LACP port-channel group 20:

```
switch(config)# clear lacp counters interface port-channel 20
switch(config)#
```

Related Commands

Command	Description
show lacp counters	Displays information about LACP statistics.

clear vpc statistics

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

clear vpc statistics {**all** | **peer-keepalive** | **peer-link** | **vpc** *number*}

Syntax Description

all	Clears all vPC statistics on the local vPC peer device.
peer-keepalive	Clears the vPC peer-keepalive statistics on the local vPC peer device.
peer-link	Clears statistics on the local vPC peer device.
vpc *number*	Clears vPC statistics on the specified vPC. The range is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

Use the **clear vpc statistics** command to clear the vPC statistics. If the feature is not enabled, this command is unavailable.

The **clear vpc statistics peer-link** and **clear vpc statistics vpc** *number* commands are redirected to the appropriate port channel and the **clear statistics port-channel** *channel-number* command.

This command does not require a license.

Examples

This example shows how to clear the statistics for vPC 10:

```
switch(config)# clear vpc statistics vpc 10
switch(config) #
```

Related Commands

Command	Description
show vpc statistics	Displays vPC statistical information on vPCs. If the feature is not enabled, the system displays an error when you enter this command.

default interface

To create a checkpoint of the running configuration for rollback purposes, use the **default interface** command.

default interface *if* [**checkpoint** *name*]

Syntax Description

if	Interface type and number in module/slot format.
checkpoint	(Optional) Creates a configuration rollback checkpoint.
name	(Optional) Checkpoint name. The maximum size is 80 alphanumeric characters.

Defaults

None

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

Use this command to return an interface to its default state. All the user configuration under the specified interface(s) is deleted upon the successful completion of the command. You can optionally create a checkpoint before deleting the interface configuration, so that you can later choose to roll back to the original configuration.

Caution When using this command, you delete the configuration of the specified interfaces unless you enter the checkpoint keyword. The optional checkpoint keyword allows you to create a checkpoint of the interface configuration to that you can later roll back to the original configuration.

This command does not require a license.

Examples

This example shows how to create a checkpoint of the running configuration for rollback purposes:

```
switch(config)# default interface ethernet 2/1 checkpoint test
.......Done
switch(config)#
```

Related Commands

Command	Description
show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

delay

To configure the interface throughput delay for Ethernet interfaces, use the **delay** command. To remove the configured throughput delay, use the **no** form of this command.

delay *value*

no delay

Syntax Description

value	Delay time in tens of microseconds. The range is from 1 to 16777215.

Defaults

10 microseconds for all interfaces except loopback ports

5000 microseconds for loopback ports

Command Modes

Interface configuration mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Beginning with Cisco NX-OS Release 4.2(1) for the Cisco Nexus 7000 Series devices, the default delay values are changed. Prior to this release, all the default delay value for all interfaces was 100 microseconds.

After upgrading from an older release, when you enter the **show running** command on a VLAN interface, the display shows an additional configuration of "delay 100." If you want to revert the delay value to the new default, enter the **no delay** command for that VLAN interface.

Specifying a value for the throughput delay provides a value for use by Layer 3 protocols; it does not change the actual throughput delay of an interface.

This command does not require a license.

Examples

This example shows how to configure the throughput-delay time to 100,000 microseconds for the slot 3 port 1 Ethernet interface:

```
switch(config)# interface ethernet 3/1
switch(config-if)# delay 10000
```

Related Commands

Command	Description
show interface	Displays information about the interface, which includes the delay parameter.

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 return to the default value, use the **no** form of this command.

delay restore *seconds*

no delay restore *seconds*

Syntax Description

seconds	Number of seconds to delay bringing up the restored vPC peer device. The range is from 1 to 3600.

Defaults

30 seconds

Command Modes

vpc-domain command mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **delay restore** command to avoid upstream traffic from the access device to the core from being dropped when you restore the vPC peer devices. If the restored vPCs come up before the routing tables are converged, you might see packet drops.

This command does not require a license.

Examples

This example shows how to configure the delay reload:

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# delay restore 40
```

Related Commands

Command	Description
delay restore interface-vlan	Allows Layer 3 routing protocols to converge and Forwarding Information Base (FIB) programming to complete for a more graceful restoration of switched virtual interfaces (SVIs).
feature vpc	Enables vPC configuration on the device.

delay restore interface-vlan

To allow Layer 3 routing protocols to converge and Forwarding Information Base (FIB) programming to complete for a more graceful restoration of switched virtual interfaces (SVIs) on the restored virtual port channel (vPC) after the delay of the vPC from coming up on the restored vPC peer device, use the **delay restore interface-vlan** command. To return to the default value, use the **no** form of this command.

delay restore interface-vlan *seconds*

no delay restore interface-vlan *seconds*

Syntax Description

seconds	Number of seconds to delay bringing up the SVIs on the vPC peer device. The range is from 1 to 3600.

Defaults

10 seconds

Command Modes

vpc-domain command mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **delay restore** command to avoid upstream traffic from the access device to the core from being dropped when you restore the vPC peer devices. If the restored vPCs come up before the routing tables are converged, you might see packet drops.

This command does not require a license.

Examples

This example shows how to configure the delay reload:

```
switch# config t
switch(config)# vpc domain 1
switch(config-vpc-domain)# delay restore 60
switch(config-vpc-domain)# delay restore interface-vlan 30
switch(config-vpc-domain)#
```

Related Commands

Command	Description
delay restore	Delays the virtual port channel (vPC) from coming up on the restored vPC peer device after a reload when the peer adjacency is already established.
feature vpc	Enables vPC configuration on the device.

description

To provide textual interface descriptions for the Ethernet and management interfaces, use the **description** command. To remove the description, use the **no** form of this command.

description *text*

Syntax Description

text	Description for the interface that you are configuring. The maximum range is 80 alphanumeric, case-sensitive characters.

Defaults

None

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

You use the **description** command to provide textual interface descriptions.

This command does not require a license.

Examples

This example shows how to add the description server1 to the Ethernet interface on slot 5, port 2:

```
switch(config)# interface ethernet 5/1
switch(config-if)# description server1
```

Related commands

Command	Description
show interface	Displays information about the interface, which includes the description parameter.

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 by the vPC configuration, 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 {*range*}

Syntax Description

range	Range of VLAN interfaces that you want to exclude from shutting down. The range is from 1 to 4094.

Defaults

None

Command Modes

vpc-domain configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **dual-active exclude interface-vlan** command to ensure that those VLAN interfaces on the vPC secondary peer device that are carried on the vPC peer link but not by the vPC configuration do not go down if the vPC peer link fails. The VLAN interfaces must have already been configured.

Caution We do not recommend that you configure an interface-VLAN exclude for a VLAN carried on a vPC because this action might cause packet losses on dual-active devices if the interface-VLAN still captures Layer 3 traffic while the vPC primary device and the vPC peer link are down.

This command does not require a license.

Examples

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

Related commands

Command	Description
vpc-domain	Configures a vPC domain and enters the vpc-domain configuration mode.

duplex

To specify the duplex mode as full, half, or autonegotiate, use the **duplex** command. To return the system to default mode, use the **no** form of this command.

duplex {**full** | **half** | **auto**}

no duplex {**full** | **half** | **auto**}

Syntax Description

full	Specifies the duplex mode as full.
half	Specifies the duplex mode as half.
auto	Specifies the duplex mode as autonegotiate.

Defaults

None

Command Modes

Interface configuration mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The interface speed that you specify can affect the duplex mode used for an interface, so you should set the speed before setting the duplex mode. If you set the speed for autonegotiation, the duplex mode is automatically set to be autonegotiated. If you specify 10- or 100-Mbps speed, the port is automatically configured to use half-duplex mode, but you can specify full-duplex mode instead. Gigabit Ethernet is full duplex only. You cannot change the duplex mode on Gigabit Ethernet ports or on a 10/100/1000-Mbps port that is set for Gigabit Ethernet.

See the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide Release 5.x* for more information about interface speed and duplex settings.

This command does not require a license.

Examples

This example shows how to specify the duplex mode for full duplex:

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

Related commands

Command	Description
show interface	Displays information about the interface, which includes the duplex parameter.

encapsulation dot1Q

To enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN), use the **encapsulation dot1q** command. To disable encapsulation, use the **no** form of this command.

encapsulation dot1Q *vlan-id*

no encapsulation dot1Q *vlan-id*

Syntax Description

vlan-id	VLAN to set when the interface is in access mode. The range is from 1 to 4094 except for the VLANs reserved for internal switch use.

Defaults

No encapsulation

Command Modes

Subinterface configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

IEEE 802.1Q encapsulation is configurable on Ethernet interfaces. IEEE 802.1Q is a standard protocol for interconnecting multiple switches and routers and for defining VLAN topologies.

Use the **encapsulation dot1q** command in subinterface range configuration mode to apply a VLAN ID to the subinterface.

This command does not require a license.

Examples

This example shows how to enable dot1Q encapsulation on a subinterface for VLAN 30:

```
switch(config-subif)# encapsulation dot1q 30
```

Related Commands

Command	Description
show vlan dot1Q	Displays dot1Q encapsulation information for a VLAN.

errdisable detect cause

To enable error-disabled (errdisable) detection for an application, use the **errdisable detect cause** command. To return to the default setting, use the **no** form of this command.

errdisable detect cause {**acl-exception** | **all** | **link-flap** | **loopback**}

no errdisable detect cause {**acl-exception** | **all** | **link-flap** | **loopback**}

Syntax Description

acl-exception	Enables error-disabled detection for access-list installation failures.
all	Enables error-disabled detection on all causes.
link-flap	Enables error-disabled disable detection on link-state flapping.
loopback	Enables error-disabled detection on loopback.

Defaults

Disabled

Command Modes

Global configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **errdisable detect cause** command to enable error detection for an application.

A cause is defined as the reason why the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in an error-disabled state. This error-disabled state is an operational state that is similar to the link-down state. You must enter the **shutdown** command and then the **no shutdown** command to recover an interface manually from the error-disabled state.

This command does not require a license.

Examples

This example shows how to enable error-disabled detection on all cases:

```
switch(config)# errdisable detect cause all
```

Related Commands

Command	Description
shutdown	Brings the port down administratively.
no shutdown	Brings the port up administratively.
err-disabled	Displays the interface error-disabled state.

errdisable recovery cause

To enable an automatic recovery from the error-disabled (errdisable) state for an application, use the **errdisable recovery cause** command. To return to the default setting, use the **no** form of this command.

errdisable recovery cause {**all** | **bpduguard** | **link-flap** | **loopback failed-port-state** | **psecure-violation** | **security-violation** | **storm-control** | **udld** | **vpc-peerlink**}

no errdisable recovery cause {**all** | **bpduguard** | **link-flap** | **loopback failed-port-state** | **psecure-violation** | **security-violation** | **storm-control** | **udld** | **vpc-peerlink**}

Syntax Description

all	Enables an automatic recovery from all causes.
bpduguard	Enables an automatic recovery from BPDU Guard error-disabled state.
loopback	Enables the timer to recover from loopback error-disabled state detected by UDLD.
failed-port state	Enables a timer automatic recovery from the STP set port state failure.
link-flap	Enables an automatic recovery from link-state flapping.
psecure-violation	Enables a timer automatic recovery from the psecure violation disable state.
security-violation	Enables an automatic recovery from the 802.1X violation disable state.
storm-control	Enables an automatic recovery from the storm control error-disabled state.
udld	Enables an automatic recovery from the UDLD error-disabled state.
vpc-peerlink	Enables an automatic recovery from an inconsistent virtual port channel (vPC) peer-link error-disabled state.

Defaults

Disabled

Command Modes

Global configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.0(2)	Added the **loopback** keyword.
4.1(3)	Added the **vpc-peerlink** parameter.
4.0	This command was introduced.

Usage Guidelines

Use the **errdisable recovery cause** command to enable an automatic recovery on the interface from the error-disabled state for an application. This command tries to bring the interface out of the error-disabled state and retry operation once all the causes have timed out. The interface automatically tries to come up again after 300 seconds. To change this interval, use the **errdisable recovery interval** command.

This command does not require a license.

Examples

This example shows how to automatically recover from the error-disabled state for link flapping after you have enabled the recovery timer:

```
switch(config)# errdisable recovery cause link-flap
```

Related Commands

Command	Description
errdisable recovery interval	Enables the recovery timer.
show interface status err-disabled	Displays interface error-disabled state.

errdisable recovery interval

To enable the recovery timer, use the **errdisable recovery interval** command.

errdisable recovery interval *interval*

Syntax Description

interval	Error detection for access-list installation failures. The range is from 30 to 65535.

Defaults

300 seconds

Command Modes

Global configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **errdisable recovery interval** command to configure the recovery timer.

This command does not require a license.

Examples

This example shows how to configure the recovery timer:

```
switch(config)# errdisable recovery interval 32
```

Related Commands

Command	Description
errdisable recovery cause	Enables the error-disabled recovery for an application.
show interface status err-disabled	Displays the interface error-disabled state.

fabricpath switch-id

To configure an emulated switch ID, use the **fabricpath switch-id** command. To return to the default setting, use the **no** form of this command.

fabricpath switch-id *switch-id*

no fabricpath switch-id *switch-id*

Syntax Description

switch-id	Emulated switch ID. The range is from 1 to 4095.

Defaults

None

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure an emulated switch ID:

```
switch# config t
switch(config)# vpc domain 1
switch(config-vpc-domain)# fabricpath switch-id 4
Configuring fabricpath switch id will flap vPCs. Continue (yes/no)? [no] yes
Note:
--------:: Re-init of peer-link and vPCs started  ::--------
switch(config-vpc-domain)#
```

This example shows how to set the default ID value:

```
switch# config t
switch(config)# vpc domain 1
switch(config-vpc-domain)# no fabricpath switch-id 4
Deconfiguring fabricpath switch id will flap vPCs. Continue (yes/no)? [no] yes
Note:
--------:: Re-init of peer-link and vPCs started  ::--------
switch(config-vpc-domain)#
```

Related Commands

Command	Description
show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

feature bfd

To enable Bidirectional Forwarding Detection (BFD), use the **feature bfd** command. To return to the default setting, use the **no** form of this command.

feature bfd

no feature bfd

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must use the **feature bfd** command to enable the BFD functionality.

Note The device does not display any BFD commands until you enable the feature.

This command does not require a license.

Examples

This example shows how to enable BFD functionality on the device:

```
switch# config t
switch(config)# feature bfd
switch(config)#
```

Related Commands

Command	Description
show feature	Displays information about the features enabled on the device.

feature interface-vlan

To enable the creation of VLAN interfaces (switched virtual interfaces [SVI]), use the **feature interface-vlan** command. To disable the VLAN interface feature, use the **no** form of this command.

feature interface-vlan

no feature interface-vlan

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

You must use the **feature interface-vlan** command before you can create VLAN interfaces.

This command does not require a license.

Examples

This example shows how to enable the interface VLAN feature:

```
switch(config)# feature interface-vlan
```

Related Commands

Command	Description
interface vlan	Creates a VLAN interface.

feature lacp

To enable Link Aggregation Control Protocol (LACP) port channeling on the device, use the **feature lacp** command. To disable LACP on the device, use the **no** form of this command.

feature lacp

no feature lacp

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

You must remove all the LACP configuration parameters from all port channels on the device before you can disable LACP. You cannot disable LACP while LACP configurations remain on the device.

Even after you enable LACP globally, you do not have to run LACP on all port channels on the device. You enable LACP on each channel mode using the **channel-group mode** command.

When you enter the **no** form of this command, the system removes all the LACP configuration from the device.

This command does not require a license.

Examples

This example shows how to enable LACP port channeling on the device:

```
switch(config)# feature lacp
```

Related Commands

Command	Description
show lacp port-channel	Displays information on port channels with LACP enabled.

feature tunnel

To enable the creation of tunnel interfaces, use the **feature tunnel** command. To disable the tunnel interface feature, use the **no** form of this command.

feature tunnel

no feature tunnel

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

You must use the **feature tunnel** command before you can create tunnel interfaces.

This command requires the Enterprise license.

Examples

This example shows how to enable the interface tunnel feature:

```
switch(config)# feature tunnel
```

Related Commands

Command	Description
interface tunnel	Creates a tunnel interface.

feature udld

To enable Unidirectional Link Detection (UDLD) globally on the device, use the **feature udld** command. To disable UDLD globally on the device, use the **no** form of this command.

feature udld

no feature udld

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **feature udld** command to enable UDLD globally on the device. UDLD must be also enabled on the other linked interface and its device. After enabling the devices, it is possible to enable a UDLD *mode* for an interface.

Use the **no feature udld** command to disable UDLD globally for Ethernet interfaces on the device.

This command does not require a license.

Examples

This example shows how to enable the UDLD for a device:

```
switch# config t
switch(config)# feature udld
```

This example shows how to disable UDLD for a device:

```
switch# config t
switch(config)# no feature udld
```

Related Commands

Command	Description
show udld	Displays information about the UDLD configuration.

feature vpc

To enable virtual port channels (vPCs), use the **feature vpc** command. To return to the default setting, use the **no** form of this command.

feature vpc

no feature vpc

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

You must use the **feature vpc** command to enable the vPC functionality. You must enable vPCs before you can configure them.

Note When you disable vPC, the device clears all the vPC configurations.

This command does not require a license.

Examples

This example shows how to enable vPC functionality on the device:

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

Related Commands

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

flowcontrol

To enable or disable the ability of the Ethernet port to send and receive flow-control pause frames, use the **flowcontrol** command. To return to the default flow-control settings, use the **no** form of this command.

flowcontrol {**send** | **receive**} {**desired** | **on** | **off**}

no flowcontrol {**send** | **receive**}

Syntax Description

send	Specifies the flow-control send setting for ports that run at 1000 Mbps or faster.
receive	Specifies the flow-control receive setting for ports that run at any speed.
desired	Specifies the remote port setting to desired for both send and receive, if the configuration of the remote port is unknown.
on	Specifies the remote port setting to on, if you want the local port to send flow-control pause frames.
off	Specifies the remote port's send and receive parameter settings to off, if you do not want to use flow control.

Defaults

1-Gb/s interfaces—Off for receive and send

10-Gb/s interfaces—Off for receive and send

Command Modes

Interface configuration mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **flowcontrol** command to enable or disable the ability of the Ethernet port to send and receive flow-control pause frames.

Make sure that the remote port has the corresponding setting for the flow control that you need. If you want the local port to send flow-control pause frames, the remote port has a receive parameter set to on or desired. If you want the local port to receive flow-control frames, you must make sure that the remote port has a send parameter set to on or desired. If you do not want to use flow control, you can set the remote port's send and receive parameters to off.

For Ethernet ports that run at 1 Gbps or faster speeds, you can enable or disable the port's ability to send and receive flow-control pause frames. For Ethernet ports that run slower than 1 Gbps, you can enable or disable only the port's ability to receive pause frames.

When enabling flow control for the local port, you either fully enable the local port to send or receive frames regardless of the flow-control setting of the remote port or you set the local port to use the desired setting used by the remote port. If you enable both the local and remote ports for flow control, set the desired flow control of the other port, or set a combination of those two states, flow control is enabled for those ports.

Note For ports that run at 10 Gbps, you cannot use the desired state for the send or receive parameter.

To see how the different port flow-control states affect the link flow-control state, see Table 1-1.

Table 1-1 Port Flow-Control Influences on Link Flow Control

Port Flow Control States		
Port Receiving Data (Sends Pause Frames)	**Port Transmitting Data (Receives Pause Frames)**	**Link Flow Control State**
Enabled	Enabled	Enabled
Enabled	Desired	Enabled
Enabled	Disabled	Disabled
Desired	Enabled	Enabled
Desired	Desired	Enabled
Desired	Disabled	Disabled
Disabled	Enabled	Disabled
Disabled	Desired	Disabled
Disabled	Disabled	Disabled

This command does not require a license.

Examples

This example shows how to set Ethernet port 3/1 to send flow-control pause frames:

```
switch# config t
switch(config)# interface ethernet 3/1
switch(config-if)# flowcontrol send on
```

Related Commands

Command	Description
show interface	Displays information about the interface, which includes the flow-control parameter.
show interface flowcontrol	Displays information about the interface flow control.

graceful consistency-check

To enable a graceful type-1 consistency check on per VLAN basis, use the **graceful consistency-check** command. To disable the graceful consistency check, use the **no** form of this command.

graceful consistency-check

no graceful consistency-check

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

VPC domain configuration mode (config-vpc-domain)

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable the graceful type-1 consistency check:

```
switch# configure terminal
switch(config)# vpc domain 1
switch(config-vpc-domain)# graceful consistency-check
switch(config-vpc-domain)#
```

This example shows how to disable the graceful type-1 consistency check:

```
switch# configure terminal
switch(config)# vpc domain 1
switch(config-vpc-domain)# no graceful consistency-check
switch(config-vpc-domain)#
```

Related Commands

Command	Description
vpc	Moves other port channels into the vPC.
vpc domain	Creates a vPC domain.

hsrp bfd

To enable Bidirectional Forwarding Detection (BFD) on a Hot Standby Router Protocol (HSRP) interface, use the **hsrp bfd** command. To return to the default setting, use the **no** form of this command.

hsrp bfd

no hsrp bfd

Syntax Description

This command has no keywords or arguments.

Defaults

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

Use the **hsrp bfd** command to enable BFD on an HSRP interface.

This command does not require a license.

Examples

This example shows how to enable BFD for an HSRP interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# hsrp bfd
```

Related Commands

Command	Description
feature bfd	Enables the BFD feature.

inherit port-profile

To assign a port profile to an interface or range of interfaces and to inherit an additional port profile onto an existing port profile, use the **inherit port-profile** command. To remove an inherited port profile or to remove a port profile from specified interfaces, use the **no** form of this command.

inherit port-profile *name*

no inherit port-profile *name*

Syntax Description

name	Port profile that you want to assign to interfaces or to inherit onto the existing port profile.

Defaults

None

Command Modes

Interface configuration mode
Port-profile configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **inherit port-profile** command to do the following:

- Assign the port profile to a specified interface or range of specified interfaces. You do this action in the interface configuration mode. The maximum number of interfaces that can inherit a single profile is 512.
- Inherit configuration parameters from another port profile onto an existing port profile. You do this action in the port-profile mode, using the name of the port profile that you want to inherit configurations into. Only port profiles of the same type can be inherited by another port profile. The device supports four levels of inheritance except for the **switchport private-vlan mapping** and the **private-vlan mapping** commands, which support only one inheritance level. The same port profile can be inherited by any number of port profiles. In a port-profile inheritance hierarchy, all the profiles must have the same switchport configuration.

See the **port-profile** command and the **state-enabled** command for information about creating, configuring, and enabling port profiles.

If you attempt to inherit a port profile to the wrong type of interface, the system returns an error.

When you remove a port profile from a range of interfaces, the system undoes the configuration from the interfaces first and then removes the port-profile link. Also, when you remove a port profile, the system checks the interface configuration and either skips port-profile commands that have been overridden by directly entered interface commands or returns the command to the default value.

You can also choose a subset of interfaces from which to remove a port profile from those interfaces to which you originally applied the profile. For example, if you configured a port profile and configured 10 interfaces to inherit that port profile, you can remove the port profile from just some of the specified 10 interfaces. The port profile continues to operate on the remaining interfaces to which it is applied.

You use the port-profile configuration mode to remove an inherited port profile from an original port profile.

This command does not require a license.

Examples

This example shows how to assign a specified port profile to a range of interfaces:

```
switch(config)# interface ethernet 2/1-10
switch(config-if)# port-profile test
```

This example shows how to inherit the configuration parameters from the port profile named switch onto the port profile named test:

```
switch(config)# test
switch(config-ppm)# inherit port-profile switch
```

Related Commands

Command	Description
show port-profile	Displays information about port profiles.

interface cmp-mgmt module

To create a Connectivity Management Processor (CMP) management interface and enter interface configuration mode, use the **interface cmp-mgmt module** command.

interface cmp-mgmt module *number*

Syntax Description

number	Active or standby supervisor module number. Valid values are 9 or 10.

Defaults

None

Command Modes

Global configuration mode
Interface configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **interface cmp-mgmt module** command to create a CMP management interface.

This command does not require a license.

Examples

This example shows how to create a CMP management interface:

```
switch(config)# interface cmp-mgmt module 9
switch(config-if-cmp)#
```

interface ethernet

To configure an Ethernet interface and enter interface configuration mode, use the **interface ethernet** command.

interface ethernet *slot/port-list*

Syntax Description

slot/port-list	Slot number and port list for the Ethernet interface. The range is from 1 to 253 for slots and from 1 to 128 for ports.

Defaults

None

Command Modes

Global configuration mode
Interface configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **interface ethernet** command to enter the interface configuration mode for the specified interface or range of interfaces.

Note *slot/port-list* is a space-separated list of slots and ports.

This command does not require a license.

Examples

This example shows how to enter the interface command mode for the Ethernet interface on slot 2, port 1:

```
switch(config)# interface ethernet 2/1
switch(config-if)#
```

Related Commands

Command	Description
show interface ethernet	Displays information about the Ethernet 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.

Defaults

None

Command Modes

Global configuration mode
Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

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

This command does not require a license.

Examples

This example shows how to create a loopback interface:

```
switch(config)# interface loopback 50
switch(config-if)#
```

Related Commands

Command	Description
show interface loopback	Displays information about the traffic on the specified loopback interface.

interface mgmt

To configure the management interface and enter interface configuration mode, use the **interface mgmt** command.

interface mgmt *number*

Syntax Description

number	Interface number. The range is from 0 to 1023.

Defaults

None

Command Modes

Global configuration mode
Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **interface mgmt** command to configure the management interface and to enter the interface configuration mode.

This command does not require a license.

Examples

This example shows how to enter the interface configuration mode to configure the management interface:

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

Related Commands

Command	Description
show interface mgmt0	Displays information about the traffic on the management interface.

interface port-channel

To create a port-channel interface and enter interface configuration mode, use the **interface port-channel** command. To remove a logical port-channel interface or subinterface, use the **no** form of this command.

interface port-channel *channel-number*

no interface port-channel *channel-number*

Syntax Description

channel-number	Channel number that is assigned to this port-channel logical interface. The range is from 1 to 4096.

Defaults

None

Command Modes

Global configuration mode
Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **interface port-channel** command to create or delete port-channel groups and to enter the interface configuration mode for the port channel.

You can create port channels implicitly using the **auto-recovery** command or explicitly using the **feature tunnel** command.

A port can belong to only one channel group.

You can create subinterfaces on a Layer 3 port-channel interface. However, you cannot add a Layer 3 interface that has existing subinterfaces to a port channel.

Note The Layer 3 port-channel interface is the routed interface.

The Link Aggregation Control Protocol (LACP) system ID is unique for each virtual device context (VDC), and channel-group numbers and names can be reused in different VDCs.

When you use the **interface port-channel** command, 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 port-channel interface.

- If you do not assign a static MAC address on the port-channel interface, a MAC address is automatically assigned. If you assign a static MAC address and then later remove it, the MAC address is automatically assigned.
- The MAC address of the port channel 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.

This command does not require a license.

Examples

This example shows how to create a port-channel group interface with channel-group number 50:

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

Related Commands

Command	Description
show lacp	Displays LACP information.
show interface port-channel	Displays information on traffic on the specified port-channel interface.
show port-channel summary	Displays information on the port channels.

interface tunnel

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

interface tunnel *number-list*

no interface tunnel *number-list*

Syntax Description

number-list	Identifying interface number list. The range is from 0 to 4095.

Defaults

None

Command Modes

Global configuration mode
Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
5.0(1)	The maximum valid range of values was changed from 65535 to 4095.
4.0	This command was introduced.

Usage Guidelines

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

Cisco NX-OS supports the generic routing encapsulation (GRE) header defined in IETF RFC 2784. Cisco NX-OS does not support tunnel keys and other options from IETF RFC 1701.

You can configure IP tunnels only in the default virtual device context (VDC).

Note *number-list* is a space-separated list of tunnels.

This command requires the Enterprise license.

Examples

This example shows how to create a tunnel interface:

```
switch(config)# interface tunnel 50
switch(config-if)#
```

Related Commands

Command	Description
show interface tunnel	Displays information about the traffic on the specified tunnel interface.
tunnel destination	Sets the destination of the IP tunnel.
tunnel source	Sets the source of the IP tunnel.

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*

Syntax Description

vlan-id	VLAN to set when the interface is in access mode. The range is from 1 to 4094, except for the VLANs reserved for the internal switch use.

Defaults

None

Command Modes

Global configuration mode
Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **interface vlan** command to create or modify VLAN interfaces.

The VLAN interface is created the first time that you enter the **interface vlan** command for a particular VLAN. The *vlan-id* argument corresponds to the VLAN tag that is associated with the data frames on an Inter-Switch Link (ISL), the IEEE 802.1Q-encapsulated trunk, or the VLAN ID that is configured for an access port.

This command does not require a license.

Examples

This example shows how to create a VLAN interface for VLAN 50:

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

Related Commands

Command	Description
feature interface-vlan	Enables the ability to create VLAN interfaces.
show interface vlan	Displays information about the traffic on the specified VLAN interface.

ip eigrp bfd

To enable Bidirectional Forwarding Detection (BFD) on an Enhanced Interior Gateway Routing Protocol (EIGRP) interface, use the **ip eigrp bfd** command. To return to the default setting, use the **no** form of this command.

ip eigrp *instance-tag* **bfd**

no ip eigrp *instance-tag* **bfd**

Syntax Description

instance-tag	EIGRP instance tag. The instance tag can be any case-sensitive, alphanumeric string up to 20 characters.

Defaults

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

Use the **ip eigrp bfd** command to enable BFD on an EIGRP interface. This command takes precedence over the **bfd** command in router configuration mode.

This command does not require a license.

Examples

This example shows how to enable BFD for an EIGRP interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip eigrp Test1 bfd
```

Related Commands

Command	Description
bfd	Enables BFD on all EIGRP interfaces.
feature bfd	Enables the BFD feature.

ip ospf bfd

To enable Bidirectional Forwarding Detection (BFD) on an Open Shortest Path First version 2 (OSPFv2) interface, use the **ip ospf bfd** command. To return to the default setting, use the **no** form of this command.

ip ospf bfd

no ip ospf bfd

Syntax Description

This command has no keywords or arguments.

Defaults

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

Use the **ip ospf bfd** command to enable BFD on an OSPFv2 interface. This command takes precedence over the **bfd** command in router configuration mode.

This command does not require a license.

Examples

This example shows how to enable BFD for an OSPF interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip ospf bfd
```

Related Commands

Command	Description
bfd	Enables BFD on all OSPFv2 interfaces.
feature bfd	Enables the BFD feature.

ip pim bfd

To enable Bidirectional Forwarding Detection (BFD) for Protocol Independent Multicast (PIM), use the **ip pim bfd** command. To return to the default setting, use the **no** form of this command.

ip pim bfd

no ip pim bfd

Syntax Description

This command has no keywords or arguments.

Defaults

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

Use the **ip pim bfd** command to enable BFD for PIM.

This command does not require a license.

Examples

This example shows how to enable BFD for PIM:

```
switch# configure terminal
switch(config)# ip pim bfd
```

Related Commands

Command	Description
feature bfd	Enables the BFD feature.

ip pim bfd-instance

To enable Bidirectional Forwarding Detection (BFD) for Protocol Independent Multicast (PIM) on an interface, use the **ip pim bfd-instance** command. To return to the default setting, use the **no** form of this command.

ip pim bfd-instance [**disable**]

no ip pim bfd-instance [**disable**]

Syntax Description

disable	(Optional) Disables BFD for PIM on this interface.

Defaults

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

Use the **ip pim bfd-instance** command to enable BFD for PIM on an interface. This configuration (with or without the **disable** keyword) overrides the BFD configuration for PIM at the global or VRF configuration level.

This command does not require a license.

Examples

This example shows how to disable BFD for PIM on interface ethernet 2/1 when BFD is enabled globally for PIM:

```
switch# configure terminal
switch(config)# ip pim bfd
switch(config)# interface ethernet 2/1
switch(config-if)# ip pim bfd-instance disable
```

Related Commands

Command	Description
feature bfd	Enables the BFD feature.

ip pim bfd-instance

To enable Bidirectional Forwarding Detection (BFD) for Protocol Independent Multicast (PIM) on an interface, use the **ip pim bfd-instance** command. To return to the default setting, use the **no** form of this command.

ip pim bfd-instance [**disable**]

no ip pim bfd-instance [**disable**]

Syntax Description

disable	Disables BFD for PIM on this interface.

Defaults

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

Use the **ip pim bfd-instance** command to enable BFD for PIM on an interface. This configuration (with or without the **disable** keyword) overrides the BFD configuration for PIM at the global or VRF configuration level.

This command does not require a license.

Examples

This example shows how to disable BFD for PIM on interface ethernet 2/1 when BFD is enabled globally for PIM:

```
switch# configure terminal
switch(config)# ip pim bfd
switch(config)# interface ethernet 2/1
switch(config-if)# ip pim bfd-instance disable
```

Related Commands

Command	Description
feature bfd	Enables the BFD feature.

ipv6 eigrp bfd

To enable Bidirectional Forwarding Detection (BFD) on an Enhanced Interior Gateway Routing Protocol (EIGRP), use the **ipv6 eigrp bfd** command. To return to the default setting, use the **no** form of this command.

ipv6 eigrp *instance-tag* **bfd**

no ipv6 eigrp *instance-tag* **bfd**

Syntax Description

instance-tag	EIGRP instance tag. The instance tag can be any case-sensitive, alphanumeric string up to 20 characters.

Defaults

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

Use the **ipv6 eigrp bfd** command to enable BFD on an EIGRP interface. This command takes precedence over the **bfd** command in router configuration mode.

This command does not require a license.

Examples

This example shows how to enable BFD for an EIGRP interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 eigrp Test1 bfd
```

Related Commands

Command	Description
bfd	Enables BFD on all EIGRP interfaces.
feature bfd	Enables the BFD feature.

isis bfd

To enable Bidirectional Forwarding Detection (BFD) on an Intermediate System-to-Intermediate System (IS-IS) interface, use the **isis bfd** command. To return to the default setting, use the **no** form of this command.

isis [ipv6] **bfd**

no isis bfd

Syntax Description

ipv6	(Optional) Enables IPv6 BFD on a specific interface that is configured for IS-IS.

Defaults

None

Defaults

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.2(2)	Added the **ipv6** keyword to the syntax description.
5.0(2)	This command was introduced.

Usage Guidelines

Use the **isis bfd** command to enable BFD on an IS-IS interface. This command takes precedence over the **bfd** command in router configuration mode.

This command does not require a license.

Examples

This example shows how to enable BFD for an IS-IS interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# isis ipv6 bfd
switch(config-if)#
```

Related Commands

Command	Description
bfd	Enables BFD on all IS-IS interfaces.
feature bfd	Enables the BFD feature.

l2protocol tunnel

To enable Layer 2 protocol tunneling, use the **l2protocol tunnel** command. To disable protocol tunneling, use the **no** form of this command.

l2protocol tunnel [**cdp** | **stp** | **vtp**]

no l2protocol tunnel [**cdp** | **stp** | **vtp**]

Syntax Description

cdp	(Optional) Enables Cisco Discovery Protocol (CDP) tunneling.
stp	(Optional) Enables Spanning Tree Protocol (STP) tunneling.
vtp	(Optional) Enables VLAN Trunking Protocol (VTP) tunneling.

Defaults

Layer 2 protocol tunneling is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable Layer 2 protocol tunneling:

```
switch(config-if)# l2protocol tunnel cdp
```

Related Commands

Command	Description
show l2protocol tunnel	Displays Layer 2 protocol tunnel information.

l2protocol tunnel cos

To specify a global class of service (CoS) value on all Layer 2 protocol tunneling interfaces, use the **l2protocol tunnel cos** command. To reset the global CoS value to its default, use the **no** form of this command.

l2protocol tunnel cos *cos-value*

no l2protocol tunnel cos

Syntax Description

cos-value	CoS value. The range is from 0 to 7. The default value is 5.

Defaults

CoS value is 5.

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to specify a global CoS value on all Layer 2 protocol tunneling interfaces:

```
switch(config)# l2protocol tunnel cos 7
```

Related Commands

Command	Description
show l2protocol tunnel	Displays Layer 2 protocol tunnel information.

l2protocol tunnel drop-threshold

To specify the maximum number of packets that can be processed on a Layer 2 protocol tunneling interface before being dropped, use the **l2protocol tunnel drop-threshold** command. To reset the values to 0 and disable the drop threshold, use the **no** form of this command.

l2protocol tunnel drop-threshold [**cdp** | **stp** | **vtp**] *packets-per-sec*

no l2protocol tunnel drop-threshold [**cdp** | **stp** | **vtp**]

Syntax Description

cdp	(Optional) Specifies the number of Cisco Discovery Protocol (CDP) packets that can be processed on an interface.
stp	(Optional) Specifies the number of Spanning Tree Protocol (STP) packets that can be processed on an interface.
vtp	(Optional) Specifies the number of VLAN Trunking Protocol (VTP) packets that can be processed on an interface.
packets-per-sec	Maximum number of packets that can be processed on an interface before being dropped. The range is from 1 to 4096.

Defaults

The drop threshold is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to specify the maximum number of CDP packets that can be processed on an Layer 2 protocol tunneling interface before being dropped:

```
switch(config-if)# l2protocol tunnel drop-threshold cdp 1024
```

Related Commands

Command	Description
show l2protocol tunnel	Displays Layer 2 protocol tunnel information.

l2protocol tunnel shutdown-threshold

To specify the maximum number of packets that can be processed on a Layer 2 protocol tunneling interface, use the **l2protocol tunnel shutdown-threshold** command. To reset the values to 0 and disable the shutdown threshold, use the **no** form of this command

l2protocol tunnel shutdown-threshold [**cdp** | **stp** | **vtp**] *packets-per-sec*

no l2protocol tunnel shutdown-threshold [**cdp** | **stp** | **vtp**]

Syntax Description

cdp	(Optional) Specifies the number of Cisco Discovery Protocol (CDP) packets that can be processed on an interface.
stp	(Optional) Specifies the number of Spinning Tree Protocol (STP) packets that can be processed on an interface.
vtp	(Optional) Specifies the number of VLAN Trunking Protocol (VTP) packets that can be processed on an interface.
packets-per-sec	Maximum number of packets that can be processed on an interface. When the number of packets is exceeded, the port is put in error-disabled state. The range is from 1 to 4096.

Defaults

The shutdown threshold is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

When the number of packets is exceeded, the port is put in error-disabled state.

This command does not require a license.

Examples

This example shows how to specify the maximum number of packets that can be processed on an Layer 2 protocol tunneling interface before the port is put in error-disabled state:

```
switch(config-if)# l2protocol tunnel shutdown-threshold 2048
```

Related Commands

Command	Description
show l2protocol tunnel	Displays Layer 2 protocol tunnel information.

lacp max-bundle

To configure a port channel maximum bundle, use the **lacp max-bundle** command. To return to the default setting, use the **no** form of this command.

lacp max-bundle *max-bundle-number*

no lacp mac-bundle *max-bundle-number*

Syntax Description

max-bundle-number	Maximum bundle number. The range is from 1 to 16.

Command Default

The default for the port channel max-bundle is 16.

The allowed range is from 1 to 16.

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

Note Even if the default value is 16, the number of active members in a port channel is the minimum number of the maximum bundle configured and the maximum active members that are allowed in the portchannel.

This command does not require a license.

Examples

This example shows how to configure port channel maximum bundles:

```
switch(config)# interface port-channel 1
switch(config-if)# lacp max-bundle 2
switch(config-if)#
```

Related Commands

Command	Description
interface	Enters the interface configuration mode and configures the types and identities of interfaces.

lacp min-links

To configure the minimum links for a port channel, use the **lacp min-links** command. To return to the default setting, use the **no** form of this command.

lacp min-links *number*

no lacp min-links *number*

Syntax Description

number	Minimum link number. The range is from 1 to 16.

Defaults

The default for the port channel minimum link is 1.

The allowed range is from 1 to 16.

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the minimum link for a port channel:

```
switch(config)# interface port-channel 1
switch(config-if)# lacp min-links 3
switch(config-if)#
```

RelatedCommands

Command	Description
interface	Enters the interface configuration mode and configures the types and identities of interfaces.

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

priority	Priority for the physical interfaces. The range is from 1 to 65535.

Defaults

32768

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Each port configured to use LACP has an LACP port priority. You can accept the default value of 32768 for the LACP port priority, or you can configure a value between 1 and 65535. LACP uses the port priority 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 or when you have more than eight ports configured for the channel group.

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(config-if)# lacp port-priority 2000
```

Related Commands

Command	Description
show lacp	Displays LACP information.

lacp rate

To set the rate at which the Link Aggregation Control Protocol (LACP) sends LACP control packets to an LACP-supported interface, use the **lacp rate** command. To reset the rate to its default, use the **no** form of this command.

lacp rate {fast | normal}

no lacp rate {fast | normal}

Syntax Description

fast	Specifies the fast rate of 1 second.
normal	Specifies the default rate of 30 seconds.

Defaults

30 seconds

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

You can change the LACP timer rate to modify the duration of the LACP timeout. Use the **lacp rate** command to set the rate at which LACP control packets are sent to an LACP-supported interface. You can change the timeout rate from the default rate (30 seconds) to the fast rate (1 second).

This command is supported only on LACP-enabled interfaces.

This command does not require a license.

Examples

This example shows how to configure the LACP fast rate on Ethernet interface 1/4:

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

Related Commands

Command	Description
show lacp	Displays LACP information.

lacp system-priority

To set the system priority of the device 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

Syntax Description

priority	Priority for the physical interfaces. The range is from 1 to 65535.

Defaults

32768

Command Modes

Global configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Each device that runs LACP has an LACP system priority value. You can accept the default value of 32768 for this parameter, or 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. The system ID is unique for each virtual device context (VDC).

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 system priority for the device to 2500:

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

Related Commands

Command	Description
show lacp	Displays LACP information.
show lacp system identifier	Displays information on the LACP system identifier.

link debounce

To enable the debounce timer for Ethernet ports and specify a debounce time, use the **link debounce** command. To disable the timer, use the **no** form of this command.

link debounce [**time** *milliseconds*]

no link debounce

Syntax Description

time *milliseconds*	(Optional) Specifies the debounce timer for the time you want to specify. The range is from 0 to 5000.

Defaults

Enabled

300 milliseconds

Command Modes

Interface configuration mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **link debounce** command to enable the debounce timer for Ethernet ports and set it for a specified amount of time in milliseconds. The default debounce time applies when you enter the **link debounce** command with no arguments.

The range of time is from 1 to 5000 ms. The debounce timer is disabled if you specify the time to 0 ms.

This command does not require a license.

Examples

This example shows how to enable the debounce timer and set the debounce time to 1000 ms for the Ethernet port 3/1:

```
switch# config t
switch(config)# interface ethernet 3/1
switch(config-if)# link debounce time 1000
```

This example shows how to disable the debounce timer for the Ethernet port 3/1:

```
switch# config t
switch(config)# interface ethernet 3/1
switch(config-if)# no link debounce
```

Related Commands

Command	Description
show interface debounce	Displays the debounce time information about the interface.

load-interval

To change the sampling interval for statistics collections on interfaces, use the **load-interval** command. To return to the default sampling interval, use the **no** form of this command.

load-interval [**counter** {**1** | **2** | **3**}] *seconds*

no load-interval [**counter** {**1** | **2** | **3**}] [*seconds*]

Syntax Description

counter	(Optional) Specifies the counter for this load interval.
1 | **2** | **3**	Specifies the number of counters configured on the interface.
seconds	Interval between sampling statistics on the interface. The range is from 60 to 300 seconds for VLAN network interfaces, and the range is from 30 to 300 seconds for Ethernet and port-channel interfaces.

Defaults

1—30 seconds; 60 seconds for VLAN network interface

2—300 seconds

3—not configured

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **load-interval** command to obtain bit-rate and packet-rate statistics for three different durations.

You can set the statistics collection intervals on the following types of interfaces:

- Ethernet interfaces
- Port-channel interfaces
- VLAN network interfaces

You cannot use this command on the management interface or subinterfaces.

This command sets the sampling interval for such statistics as packet rate and bit rate on the specified interface.

This command does not require a license.

Examples

This example shows how to set the three sample intervals for the Ethernet port 3/1:

```
switch# config t
switch(config)# interface ethernet 3/1
switch(config-if)# load-interval counter 1 60
switch(config-if)# load-interval counter 2 135
switch(config-if)# load-interval counter 3 225
```

Related Commands

Command	Description
show interface	Displays information about the interface.

max-ports

To assign a maximum possible number of interfaces that a port profile can inherit, use the **max-ports** command. To return to the default value, use the **no** form of this command.

max-ports *number*

no max-ports *number*

Syntax Description

number	Maximum number of interfaces that a port profile can inherit. The range is from 1 to 512, and there is no default value.

Defaults

None

Command Modes

Port-profile configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

You must be in the port-profile configuration mode in order to use this command.

You must enable each specific port profile by using the **state-enabled** command.

This command does not require a license.

Examples

This example shows how to enter the port-profile configuration mode and to configure the maximum possible number of interfaces that a port profile can inherit:

```
switch(config)# port-profile type ethernet type test
switch(config-ppm)# max-ports 500
```

Related Commands

Command	Description
show port-profile	Displays information about port profiles.
state-enabled	Enables a specified port profile.

mdix auto

To enable automatic medium-dependent independent crossover (MDIX) detection for the interface, use the **mdix auto** command. To turn automatic detection off, use the **no** form of this command.

mdix auto

no mdix

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **mdix auto** command to enable automatic MDIX detection for the port. Use the **no mdix** command to disable MDIX detection for the port.

This command is only available on copper Ethernet ports. To detect the type of connection (crossover or straight) with another copper Ethernet port, enable the MDIX parameter for the local port. Before you begin, MDIX must be enabled on the remote port.

This command does not require a license.

Examples

This example shows how to enable MDIX for Ethernet port 3/1:

```
switch# config t
switch(config)# interface ethernet 3/1
switch(config-if)# mdix auto
```

This example shows how to disable MDIX for Ethernet port 3/1:

```
switch# config t
switch(config)# interface ethernet 3/1
switch(config-if)# no mdix
```

Related Commands

Command	Description
show interface	Displays information about the interface, which includes the MDIX status.

medium

To set the medium mode for an interface, use the **medium** command. To remove the entry, use the **no** form of this command.

medium {**broadcast** | **p2p**}

no medium {**broadcast** | **p2p**}

Syntax Description

broadcast	Configures the interface as a broadcast medium.
p2p	Configures the interface as a point-to-point medium.

Defaults

None

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The **medium** command is used to configure the interface as broadcast or point to point.

This command does not require a license.

Examples

This example shows how to configure the interface for point-to-point medium:

```
switch(config-if)# medium p2p
```

mtu

To configure the maximum transmission unit (MTU) size for Layer 2 and Layer 3 Ethernet interfaces, use the **mtu** command. To return to the default value, use the **no** form of this command.

mtu *size*

no mtu

Syntax Description

size	For a Layer 2 interface, specify either the default MTU size (1500) in bytes or the system jumbo MTU size (9216, unless you have changed the default system jumbo size). For a Layer 3 interface, specify any even number between the range of 576 and 9216.

Defaults

1500 bytes

Command Modes

Interface configuration mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **mtu** *size* command to configure the MTU size for Layer 2 and Layer 3 Ethernet interfaces.

For Layer 3 interfaces, you can configure the MTU to be between 576 and 9216 bytes (even values are required). For Layer 2 interfaces, you can configure the MTU to be either the system default MTU (1500 bytes) or the system jumbo MTU size (which has the default size of 9216 bytes).

Note You can change the system jumbo MTU size, but if you change that value, you should also update the Layer 2 interfaces that use that value so that they use the new system jumbo MTU value. If you do not update the MTU value for Layer 2 interfaces, those interfaces use the system default MTU (1500 bytes).

This command does not require a license.

Examples

This example shows how to configure the Layer 2 Ethernet port 3/1 with the default MTU size (1500):

```
switch# config t
switch(config)# interface ethernet 3/1
switch(config-if)# mtu 1500
```

Related Commands

Command	Description
show interface	Displays information about the interface, which includes the MTU size.

mode auto

To enable specific commands for virtual port channels (vPCs) simultaneously, use the **mode auto** command.

mode auto

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

VPC domain configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

None

Examples

This example shows how to enable specific commands for vPCs simultaneously:

```
switch# configure terminal
switch(config)# vpc domain 1
switch(config-vpc-domain)# mode auto
The following commands are executed:
peer-gateway ;
auto-recovery ;
ip arp synchronize ;
ipv6 nd synchronize ;
fabricpath multicast load-balance ;
Warning:
 Enables restoring of vPCs in a peer-detached state after reload, will wait for 240
seconds to determine if peer is un-reachable
switch(config-vpc-domain)#
```

Related Commands

Command	Description
show bfd clients	Displays the BFD client list.

no autostate

To enable the switch virtual interface (SVI) autostate feature on a specified interface, use the **autostate** command. To disable the default autostate behavior, use **no** form of this command.

no autostate

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

None

Examples

This example shows how to disable the default autostate behavior for the device:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no autostate
switch(config-if)# exit
switch(config)# show running-config interface vlan 3

!Command: show running-config interface Vlan3
!Time: Mon Aug 19 07:52:48 2013

version 6.2(2)

interface Vlan3
  no shutdown
  bfd interval 50 min_rx 50 multiplier 3
  no ip redirects
  isis ipv6 bfd
  ip ospf bfd
  ospfv3 bfd disable

switch(config)#
```

Related commands

Command	Description
show bfd	Displays the BFD commands.

no ip redirects

To enable sending of Internet Control Message Protocol (ICMP) redirect messages, use the **ip redirects** command. To disable sending ICMP redirect messages, use **no** form of this command.

ip redirects

no ip redirects

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

None

Examples

This example shows how to disable Internet Control Message Protocol (ICMP) redirect messages from being sent:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip ospf bfd
switch(config-if)# no ip redirects
switch(config-if)# bfd interval 50 min_rx 50 multiplier 3
switch(config-if)# exit
```

Related Commands

Command	Description
ip redirect	Sends ICMP redirect messages.

ospfv3 bfd

To configure Bidirectional Forwarding Detection (BFD) for Open Shortest Path First version 3 (OSPFv3) on one or more interfaces, use the **ospfv3 bfd** command.

ospfv3 bfd [**disable**]

Syntax Description

disable	(Optional) Enables BFD on a per-interface basis for one or more interfaces associated with the OSPFv3 routing process.

Defaults

None

Command Modes

Interface configuration mode

Supported User Roles

None

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

OSPFv3 must be running on all participating devices. You must configure the baseline parameters for BFD sessions on the interfaces over which you want to run BFD sessions to discover BFD neighbors.

Examples

This example shows how to configure BFD for OSPFv3 on one or more interfaces:

```
switch# config terminal
switch(config)# interface ethernet 3/1
switch(config-router)# ospfv3 bfd disable
switch(config-if)# exit
switch(config)#
```

Related Commands

Command	Description
show ospfv3	Displays information about OSPFv3 routing processes.

peer-gateway

To configure the device to send virtual port-channel (vPC) packets to the device's MAC address, use the **peer-gateway** command. To return to the default value, use the **no** form of this command.

peer-gateway

no peer-gateway

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

vpc-domain configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **peer-gateway** command to have a vPC peer device act as the gateway even for packets that are sent to the vPC peer device's MAC address.

This command does not require a license.

Examples

This example shows how to configure the device to use the switch gateway even for the packets that are sent to the vPC:

```
switch# config t
switch(config)# vpc-domain 5
switch(config-vpc-domain)# peer-gateway
```

Related Commands

Command	Description
vpc-domain	Configures a vPC domain and enters the vpc-domain configuration mode.

peer-keepalive destination

To configure the virtual port-channel (vPC) peer-keepalive link and message between vPC peer devices, use the **peer-keepalive destination** command.

peer-keepalive destination *ip address* [**hold-timeout** *secs*] [**interval** *msecs* {**timeout** *secs*}[{**precedence** {*prec-value* | **network** | **internet** | **critical** | **flash-override** | **flash** | **immediate** | **priority** | **routine**}} | {**tos** {*tos-value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal**}} | **tos-byte** *tos-byte-value*][**source** *ipaddress*][**udp-port** *number*] [**vrf** {*name* | **management** | **vpc-keepalive**}]

Syntax Description

ipaddress	IP address of the remote vPC peer device. **Note** You must use an IPv4 address.
hold-timeout *secs*	(Optional) Specifies when the peer-keepalive link goes down, the secondary vPC peer device waits the hold-timeout interval. The range is from 3 to 10. During the hold-timeout, the vPC secondary device does not take any action based on any keepalive messages received, because the keepalive might be received just temporarily, such as if a supervisor fails a few seconds after the peer link goes down.
interval *msecs*	Specifies the number of milliseconds that you want between sending keepalive messages to the remote vPC peer device. This variable configures the interval between sending peer-keepalive messages to the remote vPC peer device and the maximum period to wait to receive a keepalive message from the remote vPC peer device. The range is from 400 to 10,000.
timeout *secs*	(Optional) Specifies that the timeout timer starts at the end of the hold-timeout interval. During the timeout period, the secondary vPC peer device checks for vPC peer-keepalive hello messages from the primary vPC peer device. If the secondary vPC peer device receives a single hello message, that device disables all vPC interfaces on the secondary vPC peer device. The range is from 3 and 20. During the timeout, the vPC secondary device takes action to become the vPC primary device if no keepalive message is received by the end of the configured interval.
precedence *prec-value*	(Optional) Specifies the precedence value for the peer-keepalive message. Valid values are as follows: • 0 to 7 • network (7) • internet (6) • critical (5) • flash-override (4) • flash (3) • immediate (2) • priority (1) • routine (0)

tos *tos-value*	(Optional) Specifies the precedence or ToS value for the peer-keepalive message. Valid values are as follows: • 0, 1, 2, 4, 8 • max-reliability (2) • max-throughput (4) • min-delay (8) • min-monetary-cost (1) • normal (0) **Note** The only valid values are shown here.
tos-byte	(Optional) Specifies the precedence, or 8-bit ToS value, for the peer-keepalive message. A higher numerical value indicates the higher throughput priority. The range is from 0 to 255.
source	(Optional) Specifies the IP address of the local vPC peer device. **Note** Must be an IPv4 address.
number	(Optional) Number of the UDP port to send and receive the vPC peer-keepalive messages. The range is from 1024 to 6500.
name	(Optional) Name of the virtual routing and rorwarding (VRF) instance that you want to use for the vPC peer-keepalive link and messages.
vrf *vrf-name*	(Optional) Specifies a VRF instance.
management	(Optional) Specifies the management interface.
vpc-keepalive	(Optional) Specifies a vPC keepalive.

Defaults

Peer-keepalive is disabled.

Hold-timeout is 3 seconds.

Interval is 1000 milliseconds.

Timeout is 5 seconds.

Precedence is default, with a level of 6 (internet).

UDP port is 3200.

VRF is management VRF.

Command Modes

vpc-domain configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

You must enable the vPC feature before you can configure the peer-keepalive parameters. The vPC keepalive messages notify the system if one of the vPC peer devices goes down.

You must configure the peer-keepalive messages on each of the vPC peer devices to enable the functionality.

Although the keepalive messages can transmit over any Layer 3 topology, we recommend that you create and configure a separate VRF with Layer 3 ports on each vPC peer device as the source and destination for the vPC keepalive messages. The default ports and VRF for the peer-alive link are the management ports and the management VRF. Do not use the peer link itself for the vPC peer-keepalive messages.

Ensure that both the source and destination IP addresses used for the peer-keepalive messages are unique in your network.

The vPC keepalive messages are IP/UDP messages.

This command accepts only IPv4 addresses.

The device assumes that its vPC peer device is down when the device does not receive any messages from the peer during the timeout period. We recommend that you configure the timeout value to be three times the interval value.

You can configure either the **precedence**, **tos**, or **tos-byte** value to ensure throughput for the vPC peer-keepalive message.

Note We recommend that you create a separate VRF and assign a Layer 3 port on each vPC peer device for the peer-keepalive link.

This command does not require a license.

Examples

This example shows how to configure the IP address of the remote vPC peer device for the fault-tolerant link:

```
switch(config-vpc-domain)# peer-keepalive destination 172.28.231.85
```

Related Commands

Command	Description
show running-config vpc all	Displays information on the vPC peer-keepalive status. If the feature is not enabled, the system displays an error when you enter this command.
show vpc peer-keepalive	Displays information on the vPC peer-keepalive status. If the feature is not enabled, the system displays an error when you enter this command.

peer-switch

To enable the virtual port channel (vPC) switch pair to appear as a single Spanning Tree Protocol (STP) root in the Layer 2 topology, use the **peer-switch** command. To disable the peer switch vPC topology, use the **no** form of this command.

peer-switch

no peer-switch

Syntax Description

This command has no arguments or keywords.

Defaults

Peer switch Layer 2 topology is disabled.

Command Modes

vPC domain configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable the vPC switch pair to appear as a single STP root in the Layer 2 topology:

```
switch(config)# vpc domain 5
switch(config-vpc-domain)# peer-switch
2010 Apr 28 14:44:44 switch %STP-2-VPC_PEERSWITCH_CONFIG_ENABLED: vPC peer-switch
configuration is enabled. Please make sure to configure spanning tree "bridge" priority as
per recommended guidelines to make vPC peer-switch operational.
```

Related Commands

Command	Description
vpc domain	Creates a virtual port-channel (vPC) domain.

port-channel limit

To configure more than 244 virtual port channels (vPCs), use the **port-channel limit** command. To disable this feature, use the **no** form of this command.

port-channel limit

no port-channel limit

Syntax Description

This command has no arguments or keywords.

Defaults

Limit to 244 vPCs

Command Modes

vPC domain configuration

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
6.1(2)E1	This command was introduced.

Usage Guidelines

To enable this command, first enter the **fabricpath multicast load-balance** command.

Following guidelines when using the **no port-channel limit** command:

- Entering this command causes the peer links and vPCs to go up and down and could cause traffic losses.
- Only F2 series modules support this configuration. It cannot be configured on VDCs that do not have an F2 series module.
- Entering this command changes FabricPath MAC addresses that are used by vPC+ port channels. It leads to some transient flooding until the MAC addresses are learned again.
- In-service software upgrades (ISSUs) and In-service software downgrades (ISSDs) are not supported.
- Remove the no port-channel limit configuration before attempting an ISSD to an image that does not support this configuration. To revert to an earlier configuration, the number of vPCs that you must be 244 or less.
- To unconfigure the FabricPath multicast load-balance configuration, you must first remove the no port-channel limit configuration.

This command does not require a license.

Examples

This example shows how to configure the maximum number of supported vPCs:

```
switch# switchto vdc peer1
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2012, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch-peer1(config)# vpc domain 1
switch(config-vpc-domain)# port-channel limit
switch(config-vpc-domain)# no port-channel limit
switch(config-vpc-domain)#
```

This example shows how to configure no port-channel limit:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vpc domain 1
switch(config-vpc-domain)# fabricpath multicast load-balance
switch(config-vpc-domain)# no port-channel limit
switch(config-vpc-domain)#
```

This example shows how to enable support of more than 244 vPC+ port channels:

```
switch1# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch1(config)# vpc domain 1
switch1(config-vpc-domain)# fabricpath multicast load-balance
switch1(config-vpc-domain)# no port-channel limit
```

Related Commands

Command	Description
show vpc brief	Displays a brief status of the vPC.

port-channel load-balance

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

port-channel load-balance *method* [**module** *slot*]

no port-channel load-balance *method* [**module** *slot*]]

Syntax Description

method	Load-balancing method. See the "Usage Guidelines" section for a list of valid values.
module *slot*	(Optional) Specifies the module slot number.

Defaults

Layer 2 packets—**src-dst-mac**

Layer 3 packets—**src-dst-ip**

Command Modes

Global configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
6.2(2)	Added the new method "**vlan-only**" which is applicable at the module level (for F2/F2e modules only).
5.1(3)	The word **ethernet** was removed from the command name.
4.0	This command was introduced.

Usage Guidelines

When you do not specify a module, you are configuring load balancing for the entire device. When you use the **module** parameter, you are configuring load balancing for the specified modules

Valid *method* values are as follows:

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

- **src-mac**—Loads distribution on the source MAC address.
- **src-port**—Loads distribution on the source port.
- **vlan-only**—Loads distribution on the vlan modules only.

Note You cannot configure load balancing using port channels per virtual device context (VDC). You must be in the default VDC to configure this feature; if you attempt to configure this feature from another VDC the system returns an error.

Use the **module** keyword to configure the module independently for port-channeling and load-balancing mode. The remaining module uses current load-balancing method configured for the entire device or the default method if you have not configured a method for the entire device. When you enter the **no** form with the **module** keyword, the load-balancing method for the specified module takes the current load-balancing method that is in use for the entire device. If you configured a load-balancing method for the entire device, the specified module uses that configured method rather than the default **src-dst-ip/src-dst-mac**. The per-module configuration takes precedence over the load-balancing method configured for the entire device.

You can configure one load-balancing mode for the entire device, a different mode for specified modules, and another mode for other specified modules. The per-module configuration takes precedence over the load-balancing configuration for the entire device.

Use the option that provides the balance criteria with the greatest variety in your configuration. For example, if the traffic on a port channel is going only to a single MAC address and you use the destination MAC address as the basis of port channel load balancing, the port channel always chooses the same link in that port channel; 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 for the entire device to use the source port:

```
switch(config)# port-channel load-balance src-port
```

This example shows how to set the load-balancing method for the module level (for F2/F2e modules only).

```
switch(config)# port-channel load-balance vlan-only module 1
ERROR: Command is valid for F2/F2E Module only

switch(config)# port-channel load-balance vlan-only module 4
switch(config)#
```

Related Commands

Command	Description
show port-channel load-balance	Displays information about port-channel load balancing.

port-channel load-balance hash-modulo

To enable the modulo hash for Cisco nexus 7000 Series modules, use the **port-channel load-balance hash-modulo command**. To turn off this feature command, use the **no** form of this command.

port-channel load-balance hash-modulo force

no port-channel load-balance hash-modulo force

Syntax Description

force	Specifies the force.

Defaults

Disabled

Command Modes

Global configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
6.1(3)	This command was introduced.

Usage Guidelines

Caution Once you enter the force keyword, the command immediately reinitializes all of the port channels.

By default, when the system comes if the system allows M1 Series Module capability and so, the port-channel load-balance hash-modulo displays an error. Enter the **system module-type** command to remove “M1 Series Module capability” first and then the command will work.

This command does not require a license.

Examples

This example shows how to enable the modulo hash for the Cisco nexus 7000 Series Module:

```
switch# port-channel load-balance hash-modulo
This command will reinitialize all the port-channels. Do you want to continue(y/n)? [no] y
Warning: This operation may take some time to complete
switch(config)#
```

This example shows how to specify the force:

```
switch# port-channel load-balance hash-modulo force
Warning: This operation may take some time to complete
```

This example shows how to turn on and off this feature:

```
switch(config)# no port-channel load-balance hash-modulo force
Warning: This operation may take some time to complete
switch(config)#
```

Related Commands

Command	Description
show port-channel load-balance	Displays information about port-channel load balancing.

port-channel load-defer

To set the load defer time interval, use the **port-channel load-defer** command. To return the system priority to the default value, use the **no** form of this command.

port-channel load-defer *seconds*

no port-channel load-defer *seconds*

Syntax Description

seconds	Time interval in seconds. The range is from 1 to 1800.

Defaults

120 seconds

Command Modes

Global configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
5.1(2)	This command was introduced.

Examples

This example shows how to set the load defer time interval:

```
switch(config)# port-channel load-defer 100
switch(config)#
```

Related Commands

Command	Description
show port-channel load-balance	Displays information about port-channel load balancing.

port-profile

To create a port profile and enter the port-profile configuration mode or to enter into the port-profile configuration mode of a previously created port profile, use the **port-profile** command. To remove the port profile, use the **no** form of this command.

port-profile [**type** {**ethernet | interface-vlan | port-channel**}] *name*

no port-profile [**type** {**ethernet | interface-vlan | port-channel**}] *name*

Syntax Description

type	(Optional) Specifies the type of interfaces.
ethernet	Specifies Layer 2 or Layer 3 interfaces.
interface-vlan	Specifies VLAN network interfaces.
port-channel	Specifies port-channel interfaces.
name	Name of the port profile.

Defaults

None

Command Modes

Interface configuration mode

Port-profile configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **port-profile** command to group configuration commands and apply them to several interfaces simultaneously. All interfaces in the range must be the same type. The maximum number of interfaces that can inherit a single port profile is 512.

The port-profile name must be globally unique across types and networks.

Each port profile can be applied only to a specific type of interface; the choices are as follows:

- Ethernet
- VLAN network interface
- Port channel

Note When you choose **ethernet** as the interface type, the port profile is in the default mode which is Layer 3. Enter the **switchport** command to change the port profile to Layer 2 mode.

A subset of commands are available under the port-profile configuration mode, depending on which interface type you specify. Layer 3 and CTS commands are not supported by port profiles.

You can configure the following port-profile operations:

- Create port profiles
- Delete port profiles
- Add commands to and delete commands from port profiles
- Inherit port profiles at interfaces
- Enable and disable port profiles
- Inherit between port profiles
- Configure maximum number of ports that a profile can inherit

You inherit the port profile when you attach the port profile to an interface or range of interfaces. The maximum number of interfaces that can inherit a single profile is 512. When you attach, or inherit, a port profile to an interface or range of interfaces, the system applies all the commands in that port profile to the interfaces.

Additionally, you can have one port profile inherit another port profile, which allows the initial port profile to assume all of the commands of the second, inherited port profile that do not conflict with the initial port profile. Four levels of inheritance are supported except for the **switchport private-vlan mapping** and **private-vlan mapping** commands, which support only one level of inheritance. See the **inherit port-profile** command for information about inheriting an additional port profile and assigning port profiles to specified interfaces.

The system applies the commands inherited by the interface or range of interfaces according to the following guidelines:

- Commands that you enter under the interface mode take precedence over the port profile's commands if there is a conflict. However, the port profile retains that command in the port profile.
- The port profile's commands take precedence over default commands on the interface, unless it is explicitly overridden by the default command.
- When a range of interfaces inherits a second port profile, the commands of the initial port profile override those commands of the second port profile if there is a conflict.
- After you inherit a port profile onto an interface or range of interfaces, you can override individual configuration values by entering the new value at the interface configuration level. If you then remove the individual configuration values at the interface configuration level, the interface again uses the values in the port profile again.
- There are no default configurations associated with a port profile.

Note You cannot use port profiles with Session Manager.

If you delete a specific configuration for a specified range of interfaces using the interface configuration mode, that configuration is also deleted from the port profile for that range of interfaces only. For example, if you have a channel group inside a port profile and you are in the interface configuration mode and you delete that port channel, the specified port channel is also deleted from the port profile as well.

Just as in the device, you can enter a configuration for an object in port profiles without that object being applied to interfaces. For example, you can configure a VRF instance without it being applied to the system. If you then delete that VRF and its configurations from the port profile, the system is unaffected.

After you inherit a port profile on an interface or range of interfaces and you delete a specific configuration value, that port-profile configuration does not operate on the specified interfaces.

You must enable each specific port profile using the **state-enabled** command.

This command does not require a license.

Examples

This example shows how to configure, name a port profile, and enter the port-profile configuration mode:

```
switch(config)# port-profile type ethernet test
switch(config-ppm)#
```

Related Commands

Command	Description
state-enable	Enables a specified port profile.
show port-profile	Displays information about port profiles.

rate-mode dedicated

To set the dedicated rate mode for the specified ports, use the **rate-mode dedicated** command.

rate-mode dedicated

no rate-mode

Syntax Description

This command has no arguments or keywords.

Defaults

Shared rate mode is the default.

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **rate-mode dedicated** command to set the dedicated rate mode for the specified ports.

On a 32-port,10-Gigabit Ethernet module, each set of four ports can handle 10 gigabits per second (Gb/s) of bandwidth. You can use the rate-mode parameter to dedicate that bandwidth to the first port in the set of four ports or share the bandwidth across all four ports.

Note When you dedicate the bandwidth to one port, you must first administratively shut down the ports in the group, change the rate mode to dedicated, and then bring the dedicated port administratively up.

Table 1-2 identifies the ports that are grouped together to share each 10 Gb/s of bandwidth and which port in the group can be dedicated to utilize the entire bandwidth.

Table 1-2 Dedicated and Shared Ports

Ports Groups that Can Share Bandwidth	Ports that Can be Dedicated to Each 10-Gigabit Ethernet of Bandwidth
1, 3, 5, 7	1
2, 4, 6, 8	2
9, 11, 13, 15	9

Table 1-2 Dedicated and Shared Ports (continued)

Ports Groups that Can Share Bandwidth	Ports that Can be Dedicated to Each 10-Gigabit Ethernet of Bandwidth
10, 12, 14, 16	10
17, 19, 21, 23	17
18, 20, 22, 24	18
25, 27, 29, 31	25
26, 28, 30, 32	26

Note All ports in each port group must be part of the same virtual device context (VDC). For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x*.

When you enter the **rate-mode dedicated** command, the full bandwidth of 10 Gbps is dedicated to one port. When you dedicate the bandwidth, all subsequent commands for the port are for dedicated mode.

This command does not require a license.

Examples

This example shows how to configure the dedicated rate mode for Ethernet ports 4/17, 4/19, 4/21, and 4/23:

```
switch# config t
switch(config)# interface ethernet 4/17, ethernet 4/19, ethernet 4/21, ethernet 4/23
switch(config-if)# shutdown
switch(config-if)# interface ethernet 4/17
switch(config-if)# rate-mode dedicated
switch(config-if)# no shutdown
```

Related Commands

Command	Description
show interface	Displays interface information, which includes the current rate mode dedicated.

rate-mode shared

To set the shared rate mode for the specified ports, use the **rate-mode shared** command.

rate-mode shared

Syntax Description

This command has no arguments or keywords.

Defaults

Shared rate mode is the default.

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **rate-mode shared** command to set the shared rate mode for the specified ports. This is the default rate mode for the module.

That is, use the **rate-mode shared** command to specify that each 10 Gbps of bandwidth on a 32-port 10-Gigabit Ethernet module is shared by ports in the same port group.

If the port group is in dedicated rate mode, you must first administratively shut down the ports in the group, change the rate mode to shared, and then bring the ports administratively up.

This command does not require a license.

Examples

This example shows how to configure the shared rate mode for Ethernet ports 4/17, 4/19, 4/21, and 4/23:

```
switch# config t
switch(config)# interface ethernet 4/17, ethernet 4/19, ethernet 4/21, ethernet 4/23
switch(config-if)# shutdown
switch(config-if)# interface ethernet 4/17
switch(config-if)# rate-mode shared
switch(config-if)# no shutdown
```

Related Commands

Command	Description
show interface	Displays interface information, which includes the current rate mode shared.

reload restore

To configure a virtual port channel (vPC) device to assume that its peer is not functional and to bring up the vPC, use the **reload restore** command. To reset the vPC to the standard behavior, use the **no** form of this command.

reload restore [**delay** *time-out*]

no reload restore

Syntax Description

delay *time-out*	(Optional) Sets the timeout for the vPC device. The range is from 240 to 3600.

Defaults

Delay of 240 seconds

Command Modes

vPC domain configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.2(1)	This command was deprecated.
5.0(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a vPC device to assume that its peer is not functional and to bring up the vPC:

```
switch(config)# vpc domain 5
switch(config-vpc-domain)# reload restore
Warning:
 Enables restoring of vPCs in a peer-detached state after reload, will wait for 240
seconds (by default) to determine if peer is un-reachable
```

Related Commands

Command	Description
vpc domain	Creates a virtual port-channel (vPC) domain.

role priority

To override the default selection of virtual port-channel (vPC) primary and secondary devices when you create a vPC domain, use the **role priority** command. To return to the default vPC system priority, use the **no** form of this command.

role priority *priority*

no role priority

Syntax Description

priority	Role priority. The range is from 1 to 65636.

Defaults

32667

Command Modes

vpc-domain command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

You must enable the vPC feature before you can create a vPC system priority

By default, the system 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 the system 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 primary to be lower than that of the other vPC peer device.

This command does not require a license.

Examples

This example shows how to create a vPC role priority:

```
switch# config t
switch(config)# vpc domain 5
switch(config-vpc-domain)# role priority 2000
```

Related Commands

Command	Description
show vpc role	Displays the role for this device for the vPC domain as primary or secondary.

router ospfv3

To configure Bidirectional Forwarding Detection (BFD) for the Open Shortest Path First version 3 (OSPFv3) routing process for all interfaces, use **router ospfv3** command.

router ospfv3 *process-id*

Syntax Description

process-id	Configures an OSPFv3 routing process and that allows you to enter router configuration mode.

Defaults

None

Command Modes

Global configuration mode

SupportedUserRoles

None

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

OSPFv3 must be running on all participating devices. You must configure the baseline parameters for BFD sessions on the interfaces over which you want to run BFD sessions to discover BFD neighbors.

Examples

This example shows how to configure BFD for OSPFv3 for all interfaces:

```
switch# configure terminal
switch(config)# router ospfv3 3
switch(config-router)# bfd
switch(config-router)# exit
switch(config)#
```

Related Commands

Command	Description
show bfd	Displays the BFD commands.

show bfd neighbors

To display information about Bidirectional Forwarding Detection (BFD) neighbors, use the **show bfd neighbors** command.

show bfd neighbors [**application** *name* | {**dest-ip** | **src-ip**} *ipaddr* **interface** *int-if*] [**vrf** *vrf-name*] [**details**]

Syntax Description

application *name*	(Optional) Displays BFD information for the named protocol that BFD is enabled on.
dest-ip *ipaddr*	(Optional) Displays BFD information for the destination IP address. The IP address is in dotted decimal notation for IPv4 and in A:B::C:D format for IPv6.
src-ip *ipaddr*	(Optional) Displays BFD information for the source IP address. The IP address is in dotted decimal notation for IPv4 and in A:B::C:D format for IPv6.
interface *int-if*	(Optional) Displays BFD information for the interface. Use the **?** keyword to display a list of supported interfaces.
vrf *vrf-name*	(Optional) Displays BFD information for the virtual routing and forwarding (VRF) instance.
details	(Optional) Displays detailed BFD information.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

Use the **show bfd neighbors** command to display information about BFD sessions. If you use the applications keyword, the application name is one of the following:

- bfd_app (bfd_app is a stub client and not real client)
- bgp
- eigrp
- hsrp
- isis
- ospf
- pim
- static

This command does not require a license.

Examples

This example shows how to display the output from the **show bfd neighbors** command:

```
switch# show bfd neighbors

OurAddr  NeighAddr  LD/RD                    RH/RS    Holdown(mult)     State      Int
10.0.0.2  10.0.0.1  1124073474/1107296257     Up         582(3)           Up         Po10
```

This example shows how to display the output from the **show bfd neighbors application details** command for BFD:

```
switch# show bfd neighbors application bfd_app details

OurAddr NeighAddr LD/RD                  RH/RS       Holdown(mult)     State       Int
1.1.1.2 1.1.1.1 1090519041/1107296257    Up            137(3)          Up          Eth4/37

Session state is Up and not using echo function
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000 us, MinRxInt: 50000 us, Multiplier: 3
Received MinRxInt: 50000 us, Received Multiplier: 3
Holdown (hits): 150 ms (2), Hello (hits): 50 ms (1232223)
Rx Count: 1267540, Rx Interval (ms) min/max/avg: 0/1789/44 last: 12 ms ago
Tx Count: 1232223, Tx Interval (ms) min/max/avg: 41/41/41 last: 13 ms ago
Registered protocols:  bfd_app
Uptime:  0day 15hour 5minute 8second 430ms
Last packet: Version: 1                - Diagnostic: 0
             State bit: Up             - Demand bit: 0
             Poll bit: 0               - Final bit: 0
             Multiplier: 3             - Length: 24
             My Discr.: 1107296257     - Your Discr.: 1090519041
             Min tx interval: 50000    - Min rx interval: 50000
             Min Echo interval: 0
```

Table 1-3 describes the significant fields shown in the display.

Table 1-3 show bfd neighbors Field Descriptions

Field	Description
OurAddr	IP address of the interface for which the **show bfd neighbors** command was entered.
NeighAddr	IPv4 or IPv6 address of the BFD adjacency or neighbor.
LD/RD	Local discriminator and remote discriminator being used for the session.
RH	Remote Heard—Indicates that the remote BFD neighbor has been heard.
Holdown(mult)	Detect timer multiplier that is used for this session.
State	State of the interface—Up or Down.
Int	Interface type and slot/port.
Session state is UP and not using echo function	BFD is up and not running in echo mode.

Table 1-3 show bfd neighbors Field Descriptions (continued)

Field	Description
RX Count	Number of BFD control packets that have been received from the BFD neighbor.
TX Count	Number of BFD control packets that have been sent by the BFD neighbor.
TX Interval	Interval, in milliseconds, between sent BFD packets.
Registered protocols	Routing protocols that have been registered with BFD.
Last packet: Version:	BFD version detected and run between the BFD neighbors.
Diagnostic	Diagnostic code specifying the local system's reason for the last transition of the session from Up to some other state. State values are as follows: • 0—No Diagnostic • 1—Control Detection Time Expired • 2—Echo Function Failed • 3—Neighbor Signaled Session Down • 4—Forwarding Plane Reset • 5—Path Down • 6—Concentrated Path Down • 7—Administratively Down
Demand bit	Demand Mode bit. If set, the transmitting system wants to operate in demand mode. BFD has two modes—asynchronous and demand. The Cisco implementation of BFD supports only asynchronous mode.
Poll bit	Poll bit. If the Poll bit is set, the transmitting system is requesting verification of connectivity or of a parameter change.
Final bit	Final bit. If the Final bit is set, the transmitting system is responding to a received BFD control packet that had a Poll (P) bit set.
Multiplier	Detect time multiplier. The negotiated transmit interval, multiplied by the detect time multiplier, determines the detection time for the transmitting system in BFD asynchronous mode. The detect time multiplier is similar to the hello multiplier in Intermediate System-to-Intermediate System (IS-IS), which is used to determine the hold timer: (hello interval) * (hello multiplier) = hold timer. If a hello packet is not received within the hold-timer interval, a failure has occurred. Similarly, for BFD: (transmit interval) * (detect multiplier) = detect timer. If a BFD control packet is not received from the remote system within the detect-timer interval, a failure has occurred.
Length	Length of the BFD control packet, in bytes.
My Discr.	My Discriminator. Unique, nonzero discriminator value generated by the transmitting system used to demultiplex multiple BFD sessions between the same pair of systems.

Table 1-3 show bfd neighbors Field Descriptions (continued)

Field	Description
Your Discr.	Your Discriminator. The discriminator received from the corresponding remote system. This field reflects the received value of My Discriminator or is zero if that value is unknown.
Min tx interval	Minimum transmission interval, in microseconds, that the local system wants to use when sending BFD control packets.
Min rx interval	Minimum receipt interval, in microseconds, between received BFD control packets that the system can support.
Min Echo interval	Minimum interval, in microseconds, between received BFD control packets that the system can support. If the value is zero, the transmitting system does not support the receipt of BFD echo packets.

Related Commands

Command	Description
bfd echo	Enables BFD echo mode.

show errdisable

To display the errdisable recovery and detection run-time information, use the **show errdisable** command.

show errdisable {**detect** | **recovery**}

Syntax Description

detect	Enables errdisable detection on all causes.
recovery	Enables automatic errdisable recovery from all causes.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display errdisable detection on all cases:

```
switch# show errdisable detect
ErrDisable Reason               Timer Status
-----------------               ------------
link-flap                       enabled
udld                            enabled
bpduguard                       enabled
loopback                        enabled
storm-ctrl                      enabled
sec-violation                   enabled
psec-violation                  enabled
vpc-peerlink                    enabled
failed-port-state               enabled
event-debug                     enabled
event-debug1                    enabled
event-debug2                    enabled
event-debug3                    enabled
event-debug4                    enabled
switch#
```

This example shows how to display errdisable recovery for all the cases:

```
switch# show errdisable recovery
ErrDisable Reason               Timer Status
-----------------               ------------
link-flap                       disabled
udld                            disabled
```

```
bpduguard                      disabled
loopback                       disabled
storm-ctrl                     disabled
sec-violation                  disabled
psec-violation                 disabled
vpc-peerlink                   disabled
failed-port-state              disabled
event-debug                    disabled
event-debug1                   disabled
event-debug2                   disabled
event-debug3                   disabled
event-debug4                   disabled

        Timer interval: 300
switch#
```

Related Commands

Command	Description
bfd echo	Enables BFD echo mode.

show interface

To display the interface status and information, use the **show**.

show interface

Syntax Description

This command has some keywords. For more details, see the "Usage Guidelines" section for this command.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
6.1(1)	Changed the **show interface** command output.
5.1(1)	Changed the command output to show the port is suspended due to min-links.
4.0	This command was introduced.

Usage Guidelines

Use the **show interface** command to display the interface status and information. To display **show interface** commands with valid keywords, see the following commands in this document:

- **show interface brief**—Displays brief information of interface.
- **show interface capabilities**—Displays interface capabilities information.
- **show interface counters**—Displays interface counters.
- **show interface counters detailed**—Displays only nonzero counters.
- **show interface counters errors**—Displays interface error counters.
- **show interface counters module**—Displays interface counters on a specified module.
- **show interface counters snmp**—Displays SNMP MIB values.
- **show interface counters storm-control**—Displays interface storm-control counters.
- **show interface counters trunk**—Displays interface trunk counters.
- **show interface debounce**—Displays interface debounce time information.
- **show interface description**—Displays interface description.
- **show interface ethernet**—Displays Ethernet interface information.
- **show interface flowcontrol**—Displays interface flow control information.
- **show interface mgmt**—Displays management interface.

- **show interface port-channel**—Displays port-channel interface.
- **show interface port-channel counters**—Displays interface port-channel counters.
- **show interface status**—Displays the interface line status.
- **show interface switchport**—Displays interface switchport information.
- **show interface transceiver**—Displays interface transceiver information.
- **show interface trunk**—Displays interface trunk information.

This command does not require a license.

Examples

This example shows how to display the enhanced show output for the sub-interfaces. The output is enhanced beginning with Cisco NX-OS Release 6.1(1):

```
switch# show interface ethernet 101/1/1
Ethernet101/1/1 is up
admin state is up,
  Hardware: 100/1000 Ethernet, address: 1cdf.0f3b.8042 (bia 1cdf.0f3b.8042)
  MTU 9216 bytes, BW 1000000 Kbit, DLY 10 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, medium is broadcast
  Port mode is trunk
  full-duplex, 1000 Mb/s
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is on
  Auto-mdix is turned off
  Switchport monitor is off
  EtherType is 0x8100
  Last link flapped 2d16h
  Last clearing of "show interface" counters never
  2 interface resets
  30 seconds input rate 64 bits/sec, 0 packets/sec
  30 seconds output rate 72 bits/sec, 0 packets/sec
  Load-Interval #2: 5 minute (300 seconds)
    input rate 64 bps, 0 pps; output rate 72 bps, 0 pps
  RX
    0 unicast packets  6331 multicast packets  0 broadcast packets
    6331 input packets  519142 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  2124 multicast packets  16 broadcast packets
    2140 output packets  576661 bytes
    0 jumbo packets
    0 output error  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble  0 output discard
    0 Tx pause

switch#
```

Related commands

Command	Description
interface	Enters the interface configuration mode and configures the types and identities of interfaces.

show interface brief

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

show interface [**ethernet** *slot/port* | **port-channel** *channel-number*]

SyntaxDescription

ethernet	(Optional) Specifies the slot and port of the Ethernet interface that you want to display.
slot/port	(Optional) Slot number and port number for the Ethernet interface. The range is from 1 to 253.
port-channel	(Optional) Specifies the port-channel number of the port-channel interface that you want to display.
channel-number	(Optional) Channel number. The range is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

If you do not specify an interface, this command displays information about all Layer 2 interfaces. Use the **show interface brief** command to display brief information about the interface.

This command does not require a license.

Examples

This example shows how to display brief information about the interface:

```
switch# show interface brief

--------------------------------------------------------------------------------
Port   VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --           up     172.28.231.193                          1000     1500

--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                   Ch #
--------------------------------------------------------------------------------
Eth2/1        --     eth  routed down    Administratively down      auto(D) --
```

```
Eth2/2        --      eth  routed down    Administratively down      auto(D) --
Eth2/3        --      eth  routed down    Administratively down      auto(D) --
Eth2/4        1       eth  pvlan  down    Administratively down      auto(D) --
Eth2/5        --      eth  routed down    Administratively down      auto(D) --
Eth2/6        1       eth  access down    Link not connected         auto(D) --
Eth2/7        1       eth  access up      none                       1000(D) --
Eth2/8        --      eth  routed down    Administratively down      auto(D) --
Eth2/9        1       eth  access up      none                       1000(D) --
Eth2/10       1       eth  access down    Link not connected         auto(D) --
Eth2/11       --      eth  routed down    Administratively down      auto(D) --
Eth2/12       --      eth  routed down    Administratively down      auto(D) --
Eth2/13       --      eth  routed down    Administratively down      auto(D) --
Eth2/14       --      eth  routed down    Administratively down      auto(D) --
Eth2/15       --      eth  routed down    Administratively down      auto(D) --
Eth2/16       --      eth  routed down    Administratively down      auto(D) --
Eth2/17       --      eth  routed down    Administratively down      auto(D) --
Eth2/18       --      eth  routed down    Administratively down      auto(D) --
Eth2/19       --      eth  routed down    Administratively down      auto(D) --
Eth2/20       --      eth  routed down    Administratively down      auto(D) --
Eth2/21       --      eth  routed down    Administratively down      auto(D) --
Eth2/22       --      eth  routed down    Administratively down      auto(D) --
Eth2/23       --      eth  routed down    Administratively down      auto(D) --
Eth2/24       --      eth  routed down    Administratively down      auto(D) --
Eth2/25       --      eth  routed down    Administratively down      auto(D) --
Eth2/26       --      eth  routed down    Administratively down      auto(D) --
Eth2/27       --      eth  routed down    Administratively down      auto(D) --
Eth2/28       --      eth  routed down    Administratively down      auto(D) --
Eth2/29       --      eth  routed down    Administratively down      auto(D) --
Eth2/30       --      eth  routed down    Administratively down      auto(D) --
Eth2/31       --      eth  routed down    Administratively down      auto(D) --
Eth2/32       --      eth  routed down    Administratively down      auto(D) --
Eth2/33       --      eth  routed down    Administratively down      auto(D) --
Eth2/34       --      eth  routed down    Administratively down      auto(D) --
Eth2/35       --      eth  routed down    Administratively down      auto(D) --
Eth2/36       --      eth  routed down    Administratively down      auto(D) --
Eth2/37       --      eth  routed down    Administratively down      auto(D) --
Eth2/38       --      eth  routed down    Administratively down      auto(D) --
Eth2/39       --      eth  routed down    Administratively down      auto(D) --
Eth2/40       --      eth  routed down    Administratively down      auto(D) --
Eth2/41       --      eth  routed down    Administratively down      auto(D) --
Eth2/42       --      eth  routed down    Administratively down      auto(D) --
Eth2/43       --      eth  routed down    Administratively down      auto(D) --
Eth2/44       --      eth  routed down    Administratively down      auto(D) --
Eth2/45       --      eth  routed down    Administratively down      auto(D) --
Eth2/46       --      eth  routed down    Administratively down      auto(D) --
Eth2/47       --      eth  routed down    Administratively down      auto(D) --
Eth2/48       --      eth  routed down    Administratively down      auto(D) --

--------------------------------------------------------------------------------
Interface      Secondary VLAN(Type)                    Status     Reason
--------------------------------------------------------------------------------
Vlan1          --                                      down       none
```

Related commands

Command	Description
interface	Enters the interface configuration mode and configures the types and identities of interfaces.

show interface capabilities

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

show interface [**ethernet** *slot/port* | **port-channel** *channel-number*] **capabilities**

Syntax Description

ethernet	(Optional) Specifies the slot and port of the Ethernet interface that you want to display.
slot/port	(Optional) Slot number and port number for the Ethernet interface. The range is from 1 to 253.
port-channel	(Optional) Specifies the port-channel number of the port-channel interface that you want to display.
channel-number	(Optional) Channel number. The range is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **show interface capabilities** command to display information about the capabilities of the interface such as the speed, duplex, and rate mode. If you do not specify an interface, this command displays information about all Layer 2 interfaces.

This command does not require a license.

Examples

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

```
switch# show interface ethernet 2/7 capabilities
Ethernet2/7
  Model:                COPPER
  Type:                 1000BaseT
  Speed:                10,100,1000,auto
  Duplex:               half/full/auto
  Trunk encap. type:    802.1Q
  Channel:              yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:          rx-(off/on/desired),tx-(off/on/desired)
  Rate mode:            dedicated
  QOS scheduling:       rx-(2q4t),tx-(1p3q4t)
```

```
CoS rewrite:           yes
ToS rewrite:           yes
SPAN:                  yes
UDLD:                  yes
Link Debounce:         yes
Link Debounce Time:    yes
MDIX:                  yes
Port Group Members:    none
```

Related Commands

Command	Description
interface	Enters the interface configuration mode and configures the types and identities of interfaces.

show interface counters

To display in and out counters for all interfaces in the system, use the **show interface counters** command.

show interface [**ethernet** *slot/port* | **port-channel** *channel-number*] **counters**

Syntax Description

ethernet	(Optional) Specifies the slot and port of the Ethernet interface that you want to display.
slot/port	(Optional) Slot number and port number for the Ethernet interface. The range is from 1 to 253.
port-channel	(Optional) Specifies the port-channel number of the port-channel interface that you want to display.
channel-number	(Optional) Channel number. The range is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **show interface counters** command to display in and out counters for all or a specific interface. If you do not specify an interface, this command displays information about all Layer 2 interfaces.

This command does not require a license.

Examples

This example shows how to display the in and out counters for all interfaces:

```
switch# show interface counters

--------------------------------------------------------------------------------
Port                 InOctets       InUcastPkts      InMcastPkts      InBcastPkts
--------------------------------------------------------------------------------
mgmt0              137046816             46882           115497           267729
Eth2/1                     0                 0                0                0
Eth2/2                     0                 0                0                0
Eth2/3                     0                 0                0                0
Eth2/4                     0                 0                0                0
Eth2/5                     0                 0                0                0
```

Eth2/6	0	0	0	0
Eth2/7	295061	0	1348	0
Eth2/8	0	0	0	0
Eth2/9	4174381	0	53303	0
Eth2/10	0	0	0	0
Eth2/11	0	0	0	0
Eth2/12	0	0	0	0
Eth2/13	0	0	0	0
Eth2/14	0	0	0	0
Eth2/15	0	0	0	0
Eth2/16	0	0	0	0
Eth2/17	0	0	0	0
Eth2/18	0	0	0	0
Eth2/19	0	0	0	0
Eth2/20	0	0	0	0
Eth2/21	0	0	0	0
Eth2/22	0	0	0	0
Eth2/23	0	0	0	0
Eth2/24	0	0	0	0
Eth2/25	0	0	0	0
Eth2/26	0	0	0	0
Eth2/27	0	0	0	0
Eth2/28	0	0	0	0
Eth2/29	0	0	0	0
Eth2/30	0	0	0	0
Eth2/31	0	0	0	0
Eth2/32	0	0	0	0
Eth2/33	0	0	0	0
Eth2/34	0	0	0	0
Eth2/35	0	0	0	0
Eth2/36	0	0	0	0
Eth2/37	0	0	0	0
Eth2/38	0	0	0	0
Eth2/39	0	0	0	0
Eth2/40	0	0	0	0
Eth2/41	0	0	0	0
Eth2/42	0	0	0	0
Eth2/43	0	0	0	0
Eth2/44	0	0	0	0
Eth2/45	0	0	0	0
Eth2/46	0	0	0	0
Eth2/47	0	0	0	0
Eth2/48	0	0	0	0
Vlan1	0	0	0	--

Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
mgmt0	7555343	45951	1352	136
Eth2/1	0	0	0	0
Eth2/2	0	0	0	0
Eth2/3	0	0	0	0
Eth2/4	0	0	0	0
Eth2/5	0	0	0	0
Eth2/6	0	0	0	0
Eth2/7	4174381	0	53303	0
Eth2/8	0	0	0	0
Eth2/9	295061	0	1348	0
Eth2/10	0	0	0	0
Eth2/11	0	0	0	0
Eth2/12	0	0	0	0
Eth2/13	0	0	0	0
Eth2/14	0	0	0	0
Eth2/15	0	0	0	0

```
Eth2/16                 0                   0                   0                   0
Eth2/17                 0                   0                   0                   0
Eth2/18                 0                   0                   0                   0
Eth2/19                 0                   0                   0                   0
Eth2/20                 0                   0                   0                   0
Eth2/21                 0                   0                   0                   0
Eth2/22                 0                   0                   0                   0
Eth2/23                 0                   0                   0                   0
Eth2/24                 0                   0                   0                   0
Eth2/25                 0                   0                   0                   0
Eth2/26                 0                   0                   0                   0
Eth2/27                 0                   0                   0                   0
Eth2/28                 0                   0                   0                   0
Eth2/29                 0                   0                   0                   0
Eth2/30                 0                   0                   0                   0
Eth2/31                 0                   0                   0                   0
Eth2/32                 0                   0                   0                   0
Eth2/33                 0                   0                   0                   0
Eth2/34                 0                   0                   0                   0
Eth2/35                 0                   0                   0                   0
Eth2/36                 0                   0                   0                   0
Eth2/37                 0                   0                   0                   0
Eth2/38                 0                   0                   0                   0
Eth2/39                 0                   0                   0                   0
Eth2/40                 0                   0                   0                   0
Eth2/41                 0                   0                   0                   0
Eth2/42                 0                   0                   0                   0
Eth2/43                 0                   0                   0                   0
Eth2/44                 0                   0                   0                   0
Eth2/45                 0                   0                   0                   0
Eth2/46                 0                   0                   0                   0
Eth2/47                 0                   0                   0                   0
Eth2/48                 0                   0                   0                   0
Vlan1                   0                   0                   0                   --
```

Related Commands

Command	Description
clear counters interface	Clears the counters for the specified interfaces.

show interface counters errors

To display interface error counters, use the **show interface counters errors**.

show interface [**ethernet** *slot/port* | **port-channel** *channel-number*] **counter errors**

Syntax Description

ethernet	(Optional) Specifies the slot and port of the Ethernet interface that you want to display.
slot/port	(Optional) Slot number and port number for the Ethernet interface. The range is from 1 to 253.
port-channel	(Optional) Specifies the port-channel number of the port-channel interface that you want to display.
channel-number	(Optional) Channel number. The range is from 1 to 4096.

Command Default

None

Command Modes

Any command mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **show interface counters errors** command to display interface error counters. If you do not specify an interface, this command displays information about all Layer 2 interfaces.

This command does not require a license.

Examples

This example shows how to display the interface error counters:

```
switch# show interface counters errors

--------------------------------------------------------------------------------
Port       Align-Err     FCS-Err    Xmit-Err     Rcv-Err   UnderSize OutDiscards
--------------------------------------------------------------------------------
mgmt0             --          --          --          --          --          --
Eth2/1             0           0           0           0           0           0
Eth2/2             0           0           0           0           0           0
Eth2/3             0           0           0           0           0           0
Eth2/4             0           0           0           0           0           0
Eth2/5             0           0           0           0           0           0
Eth2/6             0           0           0           0           0           0
```

Eth2/7	0	0	0	0	0	0
Eth2/8	0	0	0	0	0	0
Eth2/9	0	0	0	0	0	0
Eth2/10	0	0	0	0	0	0
Eth2/11	0	0	0	0	0	0
Eth2/12	0	0	0	0	0	0
Eth2/13	0	0	0	0	0	0
Eth2/14	0	0	0	0	0	0
Eth2/15	0	0	0	0	0	0
Eth2/16	0	0	0	0	0	0
Eth2/17	0	0	0	0	0	0
Eth2/18	0	0	0	0	0	0
Eth2/19	0	0	0	0	0	0
Eth2/20	0	0	0	0	0	0
Eth2/21	0	0	0	0	0	0
Eth2/22	0	0	0	0	0	0
Eth2/23	0	0	0	0	0	0
Eth2/24	0	0	0	0	0	0
Eth2/25	0	0	0	0	0	0
Eth2/26	0	0	0	0	0	0
Eth2/27	0	0	0	0	0	0
Eth2/28	0	0	0	0	0	0
Eth2/29	0	0	0	0	0	0
Eth2/30	0	0	0	0	0	0
Eth2/31	0	0	0	0	0	0
Eth2/32	0	0	0	0	0	0
Eth2/33	0	0	0	0	0	0
Eth2/34	0	0	0	0	0	0
Eth2/35	0	0	0	0	0	0
Eth2/36	0	0	0	0	0	0
Eth2/37	0	0	0	0	0	0
Eth2/38	0	0	0	0	0	0
Eth2/39	0	0	0	0	0	0
Eth2/40	0	0	0	0	0	0
Eth2/41	0	0	0	0	0	0
Eth2/42	0	0	0	0	0	0
Eth2/43	0	0	0	0	0	0
Eth2/44	0	0	0	0	0	0
Eth2/45	0	0	0	0	0	0
Eth2/46	0	0	0	0	0	0
Eth2/47	0	0	0	0	0	0
Eth2/48	0	0	0	0	0	0

Port	Single-Col	Multi-Col	Late-Col	Exces-Col	Carri-Sen	Runts
mgmt0	--	--	--	--	--	--
Eth2/1	0	0	0	0	0	0
Eth2/2	0	0	0	0	0	0
Eth2/3	0	0	0	0	0	0
Eth2/4	0	0	0	0	0	0
Eth2/5	0	0	0	0	0	0
Eth2/6	0	0	0	0	0	0
Eth2/7	0	0	0	0	0	0
Eth2/8	0	0	0	0	0	0
Eth2/9	0	0	0	0	0	0
Eth2/10	0	0	0	0	0	0
Eth2/11	0	0	0	0	0	0
Eth2/12	0	0	0	0	0	0
Eth2/13	0	0	0	0	0	0
Eth2/14	0	0	0	0	0	0
Eth2/15	0	0	0	0	0	0
Eth2/16	0	0	0	0	0	0
Eth2/17	0	0	0	0	0	0

Eth2/18	0	0	0	0	0	0
Eth2/19	0	0	0	0	0	0
Eth2/20	0	0	0	0	0	0
Eth2/21	0	0	0	0	0	0
Eth2/22	0	0	0	0	0	0
Eth2/23	0	0	0	0	0	0
Eth2/24	0	0	0	0	0	0
Eth2/25	0	0	0	0	0	0
Eth2/26	0	0	0	0	0	0
Eth2/27	0	0	0	0	0	0
Eth2/28	0	0	0	0	0	0
Eth2/29	0	0	0	0	0	0
Eth2/30	0	0	0	0	0	0
Eth2/31	0	0	0	0	0	0
Eth2/32	0	0	0	0	0	0
Eth2/33	0	0	0	0	0	0
Eth2/34	0	0	0	0	0	0
Eth2/35	0	0	0	0	0	0
Eth2/36	0	0	0	0	0	0
Eth2/37	0	0	0	0	0	0
Eth2/38	0	0	0	0	0	0
Eth2/39	0	0	0	0	0	0
Eth2/40	0	0	0	0	0	0
Eth2/41	0	0	0	0	0	0
Eth2/42	0	0	0	0	0	0
Eth2/43	0	0	0	0	0	0
Eth2/44	0	0	0	0	0	0
Eth2/45	0	0	0	0	0	0
Eth2/46	0	0	0	0	0	0
Eth2/47	0	0	0	0	0	0
Eth2/48	0	0	0	0	0	0

Port	Giants	SQETest-Err	Deferred-Tx	IntMacTx-Er	IntMacRx-Er	Symbol-Err
mgmt0	--	--	--	--	--	--
Eth2/1	0	--	0	0	0	0
Eth2/2	0	--	0	0	0	0
Eth2/3	0	--	0	0	0	0
Eth2/4	0	--	0	0	0	0
Eth2/5	0	--	0	0	0	0
Eth2/6	0	--	0	0	0	0
Eth2/7	0	--	0	0	0	0
Eth2/8	0	--	0	0	0	0
Eth2/9	0	--	0	0	0	0
Eth2/10	0	--	0	0	0	0
Eth2/11	0	--	0	0	0	0
Eth2/12	0	--	0	0	0	0
Eth2/13	0	--	0	0	0	0
Eth2/14	0	--	0	0	0	0
Eth2/15	0	--	0	0	0	0
Eth2/16	0	--	0	0	0	0
Eth2/17	0	--	0	0	0	0
Eth2/18	0	--	0	0	0	0
Eth2/19	0	--	0	0	0	0
Eth2/20	0	--	0	0	0	0
Eth2/21	0	--	0	0	0	0
Eth2/22	0	--	0	0	0	0
Eth2/23	0	--	0	0	0	0
Eth2/24	0	--	0	0	0	0
Eth2/25	0	--	0	0	0	0
Eth2/26	0	--	0	0	0	0
Eth2/27	0	--	0	0	0	0
Eth2/28	0	--	0	0	0	0

Eth2/29	0	--	0	0	0	0
Eth2/30	0	--	0	0	0	0
Eth2/31	0	--	0	0	0	0
Eth2/32	0	--	0	0	0	0
Eth2/33	0	--	0	0	0	0
Eth2/34	0	--	0	0	0	0
Eth2/35	0	--	0	0	0	0
Eth2/36	0	--	0	0	0	0
Eth2/37	0	--	0	0	0	0
Eth2/38	0	--	0	0	0	0
Eth2/39	0	--	0	0	0	0
Eth2/40	0	--	0	0	0	0
Eth2/41	0	--	0	0	0	0
Eth2/42	0	--	0	0	0	0
Eth2/43	0	--	0	0	0	0
Eth2/44	0	--	0	0	0	0
Eth2/45	0	--	0	0	0	0
Eth2/46	0	--	0	0	0	0
Eth2/47	0	--	0	0	0	0
Eth2/48	0	--	0	0	0	0

Related Commands

Command	Description
clear counters interface	Clears the counters for the specified interfaces.

show interface counters storm-control

To display interface storm control discard counters, use the **show interface counters storm-control**.

show interface [**ethernet** *slot/port* | **port-channel** *channel-number*] **counters storm-control**

SyntaxDescription

ethernet	(Optional) Specifies the slot and port of the Ethernet interface that you want to display.
slot/port	(Optional) Slot number and port number for the Ethernet interface. The range is from 1 to 253.
port-channel	(Optional) Specifies the port-channel number of the port-channel interface that you want to display.
channel-number	(Optional) Channel number. The range is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **show interface counters storm-control** command to display interface storm control discard counters. If you do not specify an interface, this command displays information about all Layer 2 interfaces.

This command does not require a license.

Examples

This example shows how to display the interface storm control discard counters:

```
switch# show interface counters storm-control

--------------------------------------------------------------------------------
Port       UcastSupp %     McastSupp %     BcastSupp %     TotalSuppDiscards
--------------------------------------------------------------------------------
Eth2/1          100.00          100.00          100.00                      0
Eth2/2          100.00          100.00          100.00                      0
Eth2/3          100.00          100.00          100.00                      0
Eth2/4          100.00          100.00          100.00                      0
Eth2/5          100.00          100.00          100.00                      0
Eth2/6          100.00          100.00          100.00                      0
```

Eth2/7	100.00	100.00	100.00	0
Eth2/8	100.00	100.00	100.00	0
Eth2/9	100.00	100.00	100.00	0
Eth2/10	100.00	100.00	100.00	0
Eth2/11	100.00	100.00	100.00	0
Eth2/12	100.00	100.00	100.00	0
Eth2/13	100.00	100.00	100.00	0
Eth2/14	100.00	100.00	100.00	0
Eth2/15	100.00	100.00	100.00	0
Eth2/16	100.00	100.00	100.00	0
Eth2/17	100.00	100.00	100.00	0
Eth2/18	100.00	100.00	100.00	0
Eth2/19	100.00	100.00	100.00	0
Eth2/20	100.00	100.00	100.00	0
Eth2/21	100.00	100.00	100.00	0
Eth2/22	100.00	100.00	100.00	0
Eth2/23	100.00	100.00	100.00	0
Eth2/24	100.00	100.00	100.00	0
Eth2/25	100.00	100.00	100.00	0
Eth2/26	100.00	100.00	100.00	0
Eth2/27	100.00	100.00	100.00	0
Eth2/28	100.00	100.00	100.00	0
Eth2/29	100.00	100.00	100.00	0
Eth2/30	100.00	100.00	100.00	0
Eth2/31	100.00	100.00	100.00	0
Eth2/32	100.00	100.00	100.00	0
Eth2/33	100.00	100.00	100.00	0
Eth2/34	100.00	100.00	100.00	0
Eth2/35	100.00	100.00	100.00	0
Eth2/36	100.00	100.00	100.00	0
Eth2/37	100.00	100.00	100.00	0
Eth2/38	100.00	100.00	100.00	0
Eth2/39	100.00	100.00	100.00	0
Eth2/40	100.00	100.00	100.00	0
Eth2/41	100.00	100.00	100.00	0
Eth2/42	100.00	100.00	100.00	0
Eth2/43	100.00	100.00	100.00	0
Eth2/44	100.00	100.00	100.00	0
Eth2/45	100.00	100.00	100.00	0
Eth2/46	100.00	100.00	100.00	0
Eth2/47	100.00	100.00	100.00	0
Eth2/48	100.00	100.00	100.00	0

Related Commands

Command	Description
clear counters interface	Clears the counters for the specified interfaces.

show interface counters trunk

To display the counters for Layer 2 switch port trunk interfaces, use the **show interface counters trunk** command.

show interface {**ethernet** *slot/port*} **counters trunk**

Syntax Description

ethernet	(Optional) Specifies the slot and port of the Ethernet interface that you want to display.
slot/port	(Optional) Slot number and port number for the Ethernet interface. The range is from 1 to 253.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The device supports only IEEE 802.1Q encapsulation. This command also displays the counters for trunk port channels.

This command does not require a license.

Examples

This example shows how to display the counters for a trunk interface. This display shows the frames transmitted and received through the trunk interface, as well as the number of frames with the wrong trunk encapsulation:

```
switch# show interface ethernet 2/9 counters trunk

--------------------------------------------------------------------------
Port            TrunkFramesTx   TrunkFramesRx      WrongEncap
--------------------------------------------------------------------------
Ethernet2/9                 0               0               0
```

Related Commands

Command	Description
clear counters interface	Clears the counters for the specified interfaces.

show interface debounce

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

show interface [**ethernet** *slot/port* | **port-channel** *channel-number*] **debounce**

Syntax Description

ethernet	(Optional) Specifies the slot and port of the Ethernet interface that you want to display.
slot/port	(Optional) Slot number and port number for the Ethernet interface. The range is from 1 to 253.
port-channel	(Optional) Specifies the port-channel number of the port-channel interface that you want to display.
channel-number	(Optional) Channel number. The range is from 1 to 4096.

Command Default

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **show interface debounce** command to display debounce time information about the interface. If you do not specify an interface, this command displays information about all Layer 2 interfaces.

This command does not require a license.

Examples

This example shows how to display debounce time information about the interface:

```
switch# show interface debounce

--------------------------------------------------------------------------------
Port          Debounce time   Value(ms)
--------------------------------------------------------------------------------
Eth2/1        enable              100
Eth2/2        enable              100
Eth2/3        enable              100
Eth2/4        enable              100
Eth2/5        enable              100
Eth2/6        enable              100
Eth2/7        enable              100
```

```
Eth2/8        enable              100
Eth2/9        enable              100
Eth2/10       enable              100
Eth2/11       enable              100
Eth2/12       enable              100
Eth2/13       enable              100
Eth2/14       enable              100
Eth2/15       enable              100
Eth2/16       enable              100
Eth2/17       enable              100
Eth2/18       enable              100
Eth2/19       enable              100
Eth2/20       enable              100
Eth2/21       enable              100
Eth2/22       enable              100
Eth2/23       enable              100
Eth2/24       enable              100
Eth2/25       enable              100
Eth2/26       enable              100
Eth2/27       enable              100
Eth2/28       enable              100
Eth2/29       enable              100
Eth2/30       enable              100
Eth2/31       enable              100
Eth2/32       enable              100
Eth2/33       enable              100
Eth2/34       enable              100
Eth2/35       enable              100
Eth2/36       enable              100
Eth2/37       enable              100
Eth2/38       enable              100
Eth2/39       enable              100
Eth2/40       enable              100
Eth2/41       enable              100
Eth2/42       enable              100
Eth2/43       enable              100
Eth2/44       enable              100
Eth2/45       enable              100
Eth2/46       enable              100
Eth2/47       enable              100
Eth2/48       enable              100
```

Related Commands

Command	Description
link debounce time	Enables the debounce timer for Ethernet ports.

show interface description

To display a description about the interface, use the **show interface description** command.

show interface description

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **show interface description** command to display the interface description.

This command does not require a license.

Examples

This example shows how to display a description of the interface:

```
switch# show interface description

--------------------------------------------------------------------------------
Interface                Description
--------------------------------------------------------------------------------
mgmt0                    --

--------------------------------------------------------------------------------
Port          Type   Speed   Description
--------------------------------------------------------------------------------
Eth2/1        eth    1000    --
Eth2/2        eth    1000    --
Eth2/3        eth    1000    --
Eth2/4        eth    1000    --
Eth2/5        eth    1000    --
Eth2/6        eth    1000    --
Eth2/7        eth    1000    server2
Eth2/8        eth    1000    --
Eth2/9        eth    1000    --
Eth2/10       eth    1000    ethernet slot 2 port 10
Eth2/11       eth    1000    --
Eth2/12       eth    1000    --
Eth2/13       eth    1000    --
```

```
Eth2/14       eth    1000    --
Eth2/15       eth    1000    --
Eth2/16       eth    1000    --
Eth2/17       eth    1000    --
Eth2/18       eth    1000    --
Eth2/19       eth    1000    --
Eth2/20       eth    1000    --
Eth2/21       eth    1000    --
Eth2/22       eth    1000    --
Eth2/23       eth    1000    --
Eth2/24       eth    1000    --
Eth2/25       eth    1000    --
Eth2/26       eth    1000    --
Eth2/27       eth    1000    --
Eth2/28       eth    1000    --
Eth2/29       eth    1000    --
Eth2/30       eth    1000    --
Eth2/31       eth    1000    --
Eth2/32       eth    1000    --
Eth2/33       eth    1000    --

...<additional lines truncated>
```

Related Commands

Command	Description
description	Provides textual interface descriptions for interfaces.

show interface ethernet

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

show interface ethernet *slot/port* [**brief | cable-diagnostics-tdr | capabilities | counters** {**brief | detailed | errors | snmp | storm-control | trunk**}| **debounce | description | fcoe | flowcontrol | mac-address | status** {**err-disabled | err-vlans**}| **switchport | transceiver | trunk**]

Syntax Description

slot/port	Slot number and port number for the Ethernet interface. The range is from 1 to 253.
brief	(Optional) Displays brief information about the interface.
cable-diagnostics-tdr	(Optional) Displays information about the time domain reflectometer (TDR) test.
capabilities	(Optional) Displays interface capabilities.
counters	Displays the counters.
brief	Displays information about the counters in brief.
detailed	Displays only nonzero counters.
errors	Displays error counters in the interface.
snmp	Displays SNMP MIB values.
storm-control	Displays storm-control counters.
trunk	Displays trunk counters.
debounce	(Optional) Displays the debounce time of the interface.
description	(Optional) Displays the interface description.
fcoe	(Optional) Displays the Fibre Channel over Ethernet (FCoE) information of the interface.
flowcontrol	(Optional) Displays the flow-control information.
mac-address	(Optional) Displays the MAC address.
status	(Optional) Displays the link status of the interface.
err-disabled	Displays the error-disabled state of the interface.
err-vlans	Displays VLAN errors in the interface.
switchport	(Optional) Displays switch-port information.
transceiver	(Optional) Displays the transceiver information.
trunk	(Optional) Displays interface trunk information.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.1(1)	Added the **brief**, **cable-diagnostics-tdr**, **capabilities**, **debounce**, **description**, **detailed**, **errors**, **err-disabled**, **err-vlans**, **fcoe**, **flowcontrol**, **mac-address**, **snmp**, **storm-control**, **status**, **switchport**, **transceiver**, and **trunk** keywords.
4.0	This command was introduced.

Usage Guidelines

Use the **show interface ethernet** command to display information about the Ethernet interface.

This command does not require a license.

Examples

This example shows how to display information about the Ethernet interface:

```
switch# show interface ethernet 2/5
Ethernet2/5 is down (Administratively down)
  Hardware: 10/100/1000 Ethernet, address: 0018.bad8.3ffd (bia 0019.076c.4db0)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  auto-duplex, auto-speed
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned on
  Switchport monitor is off
  Last clearing of "show interface" counters never
  1 minute input rate 0 bits/sec, 0 packets/sec
  1 minute output rate 0 bits/sec, 0 packets/sec
  L3 in Switched:
    ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
  L3 out Switched:
    ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
  Rx
    0 input packets 0 unicast packets 0 multicast packets
    0 broadcast packets 0 jumbo packets 0 storm suppression packets
    0 bytes
  Tx
    0 output packets 0 multicast packets
    0 broadcast packets 0 jumbo packets
    0 bytes
    0 input error 0 short frame 0 watchdog
    0 no buffer 0 runt 0 CRC 0 ecc
    0 overrun  0 underrun 0 ignored 0 bad etype drop
    0 bad proto drop 0 if down drop 0 input with dribble
    0 input discard
    0 output error 0 collision 0 deferred
    0 late collision 0 lost carrier 0 no carrier
    0 babble
    0 Rx pause 0 Tx pause
  0 interface resets
```

Related Commands

Command	Description
interface	Enters the interface configuration mode and configures the types and identities of interfaces.

show interface flowcontrol

To display the flow-control configuration for all or a specified interface, use the **show interface flowcontrol** command.

show interface flowcontrol [**fex** | **port-channel** *channel-number*] **flowcontrol**

Syntax Description

fex	(Optional) Displays the Fabric Extender interface that you want to display. the range is from 100 to 199.
port-channel *channel-number*	(Optional) Displays the port-channel number of the port-channel interface that you want to display. The range is from 1 to 4096.
flowcontrol	(Optional) Displays the interface flowcontrol information.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin 2
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.
5.1	The **fex** keyword was added.

Usage Guidelines

Use the **show interface flowcontrol** command to display information about the interface flow control. If you do not specify an interface, this command displays information about all Layer 2 interfaces.

This command does not require a license.

Examples

This example shows how to display the interface flow-control information:

```
switch# show interface flowcontrol

--------------------------------------------------------------------------------
Port       Send FlowControl  Receive FlowControl  RxPause TxPause
           admin    oper     admin    oper
--------------------------------------------------------------------------------
Eth2/1     off      off      off      off         0       0
Eth2/2     off      off      off      off         0       0
Eth2/3     off      off      off      off         0       0
Eth2/4     off      off      off      off         0       0
Eth2/5     off      off      off      off         0       0
Eth2/6     off      off      off      off         0       0
Eth2/7     off      off      off      off         0       0
```

```
Eth2/8      off       off       off       off          0         0
Eth2/9      off       off       off       off          0         0
Eth2/10     off       off       off       off          0         0
Eth2/11     off       off       off       off          0         0
Eth2/12     off       off       off       off          0         0
Eth2/13     off       off       off       off          0         0
Eth2/14     off       off       off       off          0         0
Eth2/15     off       off       off       off          0         0
Eth2/16     off       off       off       off          0         0
Eth2/17     off       off       off       off          0         0
Eth2/18     off       off       off       off          0         0
Eth2/19     off       off       off       off          0         0
Eth2/20     off       off       off       off          0         0
Eth2/21     off       off       off       off          0         0
Eth2/22     off       off       off       off          0         0
Eth2/23     off       off       off       off          0         0
Eth2/24     off       off       off       off          0         0
Eth2/25     off       off       off       off          0         0
Eth2/26     off       off       off       off          0         0
Eth2/27     off       off       off       off          0         0
Eth2/28     off       off       off       off          0         0
Eth2/29     off       off       off       off          0         0
Eth2/30     off       off       off       off          0         0
Eth2/31     off       off       off       off          0         0
Eth2/32     off       off       off       off          0         0
Eth2/33     off       off       off       off          0         0
Eth2/34     off       off       off       off          0         0
Eth2/35     off       off       off       off          0         0
Eth2/36     off       off       off       off          0         0
Eth2/37     off       off       off       off          0         0
Eth2/38     off       off       off       off          0         0
Eth2/39     off       off       off       off          0         0
Eth2/40     off       off       off       off          0         0
Eth2/41     off       off       off       off          0         0
Eth2/42     off       off       off       off          0         0
Eth2/43     off       off       off       off          0         0
Eth2/44     off       off       off       off          0         0
Eth2/45     off       off       off       off          0         0
Eth2/46     off       off       off       off          0         0
Eth2/47     off       off       off       off          0         0
Eth2/48     off       off       off       off          0         0
```

Related Commands

Command	Description
flowcontrol	Enables or disables the ability of the Ethernet port to send and receive flow-control pause frames.

show interface mgmt

To display the management interface information, use the **show interface mgmt** command.

show interface mgmt *number* [**brief** | **counters** [**detailed** | **errors** [**snmp**]] | **description** | **status**]

Syntax Description

number	Information about the management interface number. The valid value is 0.
brief	(Optional) Displays brief information about the management interface.
counters	(Optional) Displays the counters for the management interface.
detailed	(Optional) Displays detailed information about the counters for the management interface.
errors	(Optional) Displays the errors for the management interface.
snmp	(Optional) Displays the SNMP errors for the management interface.
description	(Optional) Displays the description of the management interface.
status	(Optional) Displays the status of the management interface.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **show interface mgmt** *number* command to display information about the management interface.

This command does not require a license.

Examples

This example shows how to display the management interface information:

```
switch# show interface mgmt0
mgmt0 is up
  Hardware: GigabitEthernet, address: 0019.076c.1a78 (bia 0019.076c.1a78)
  Internet Address is 172.28.231.193/23
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  full-duplex, 1000 Mb/s
```

```
Auto-Negotiation is turned on
1 minute input rate 6446522 bits/sec, 78642 packets/sec
1 minute output rate 1965455 bits/sec, 20644 packets/sec
Rx
  78681 input packets 15607 unicast packets 20178 multicast packets
  42896 broadcast packets 24189392 bytes
Tx
  20647 output packets 20377 unicast packets 246 multicast packets
  24 broadcast packets 7370904 bytes
```

Related Commands

Command	Description
interface	Enters the interface configuration mode and configures the types and identities of interfaces.

show interface port-channel

To display descriptive information about port channels, use the **show interface port-channel** command.

show interface port-channel *channel-number* [**brief** | **description** | **flowcontrol** | **status** | **switchport** | **trunk**]

Syntax Description

channel-number	Number of the port-channel group. The range is from 1 to 4096.
brief	(Optional) Specifies the summary information for specified port channels.
description	(Optional) Specifies the description of specified port channels.
flowcontrol	(Optional) Specifies information about the flow-control status control for specified port channels and the statistics on received and transmitted flow-control pause packets.
status	(Optional) Specifies information about the status for specified port channels.
switchport	(Optional) Specifies information for specified Layer 2 port channels including access and trunk modes.
trunk	(Optional) Specifies information for specified Layer 2 port channels on the trunk mode.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.2(1)	Display of configured static MAC address for Layer 3 port channels was added.
4.0	This command was introduced.

Usage Guidelines

To display more statistics for the specified port channels, use the **show interface port-channel counters** command.

This command does not require a license.

Examples

This example shows how to display information for a specific port channel. This example displays statistical information gathered on the port channel at 1-minute intervals:

```
switch# show interface port-channel 101
port-channel101 is up
admin state is up,
  Hardware: Port-Channel, address: 0026.9825.58e4 (bia 0026.9825.58e4)
  MTU 9216 bytes, BW 20000000 Kbit, DLY 10 usec
  reliability 255/255, txload 16/255, rxload 16/255
  Encapsulation ARPA, medium is broadcast
  Port mode is fex-fabric
  full-duplex, 10 Gb/s
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned off
  Switchport monitor is off
  EtherType is 0x8100
  Members in this channel: Eth7/1, Eth8/1
  Last clearing of "show interface" counters never
  1 interface resets
  30 seconds input rate 1264864848 bits/sec, 1736043 packets/sec
  30 seconds output rate 1264870712 bits/sec, 1736074 packets/sec
  Load-Interval #2: 5 minute (300 seconds)
    input rate 1.25 Gbps, 1.72 Mpps; output rate 1.25 Gbps, 1.72 Mpps
  RX
    733914 unicast packets  382406768498 multicast packets  11476533567 broadcast packets
    393884035979 input packets  36031214919080 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
    62339596 Rx pause
  TX
    1019601 unicast packets  382406766702 multicast packets  11476533707 broadcast packets
    393884320010 output packets  36030918130654 bytes
    0 jumbo packets
    0 output error  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble  0 output discard
    0 Tx pause
```

This example shows how to display a brief description for a specific port channel, including the mode for the port channel, the status, speed, and protocol:

```
switch# show interface port-channel 5 brief

--------------------------------------------------------------------------------
Port-channel VLAN  Type Mode   Status  Reason                    Speed  Protocol
Interface
--------------------------------------------------------------------------------
                  eth  access down    No operational members      auto(D)  lacp
```

This example shows how to display the description for a specific port channel:

```
switch# show interface port-channel 5 description

--------------------------------------------------------------------------------
Interface               Description
--------------------------------------------------------------------------------
port-channel5           test
```

This example shows how to display the flow-control information for a specific port channel:

```
switch# show interface port-channel 50 flowcontrol

--------------------------------------------------------------------------------
Port       Send FlowControl  Receive FlowControl  RxPause TxPause
```

```
           admin    oper     admin    oper
--------------------------------------------------------------------------------
Po50       off      off      off      off         0       0
```

The **oper** display for the **show interface port-channel flowcontrol** command shows as on if one member of the port channel is set to on for flow control and all the of the members and the entire port channel is set to on for flow control.

This example shows how to display the status of a specific port channel:

```
switch# show interface port-channel 5 status

--------------------------------------------------------------------------------
Port           Name               Status   Vlan      Duplex  Speed   Type
--------------------------------------------------------------------------------
               test                down     1         auto    auto    --
```

This example shows how to display information for a specific Layer 2 port channel:

```
switch# show interface port-channel 50 switchport
Name: port-channel50
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: trunk
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-3967,4048-4093
  Administrative private-vlan primary host-association: none
  Administrative private-vlan secondary host-association: none
  Administrative private-vlan primary mapping: none
  Administrative private-vlan secondary mapping: none
  Administrative private-vlan trunk native VLAN: none
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: none
  Administrative private-vlan trunk private VLANs: none
  Operational private-vlan: none
```

This command displays information for Layer 2 port channels in both the access and trunk modes.

When you use this command for a routed port channel, the device returns the following message:

```
Name: port-channel20
  Switchport: Disabled
```

This example shows how to display information for a specific Layer 2 port channel that is in trunk mode:

```
switch# show interface port-channel 5 trunk

switch# show interface port-channel 50 trunk
port-channel50 is down (No operational members)
    Hardware is Ethernet, address is 0000.0000.0000
    MTU 1500 bytes, BW 100000 Kbit, DLY 10 usec
    Port mode is access
    Speed is auto-speed
    Duplex mode is auto
    Beacon is turned off
    Receive flow-control is off, Send flow-control is off
    Rate mode is dedicated
  Members in this channel: Eth2/10
    Native Vlan: 1
    Allowed Vlans: 1-3967,4048-4093
```

This command displays information for only Layer 2 port channels in the trunk modes; you cannot display information about Layer 2 port channels in the access mode with this command.

Related Commands

Command	Description
show interface port-channel counters	Displays the statistics for channel groups.
show port-channel summary	Displays summary information for all channel groups.

show interface port-channel counters

To display information about port-channel statistics, use the **show interface port-channel counters** command.

show interface port-channel *channel-number* **counters** [**brief** | **detailed** [**all** | **snmp**] | **errors** [**snmp**] | **trunk**]

Syntax Description

channel-number	Number of the port-channel group. The range is from1 to 4096.
brief	(Optional) Specifies the rate MB/s and total frames for specified port channels.
detailed	(Optional) Specifies the nonzero counters for specified port channels.
all	(Optional) Specifies the counters for specified port channels.
snmp	(Optional) Specifies the SNMP MIB values for specified port channels.
errors	(Optional) Specifies the interface error counters for specified port channels.
trunk	(Optional) Specifies the interface trunk counters for specified port channels.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This command displays statistics for all port channels including the Link Aggregation Control Protocol (LACP)-enabled port channels and those port channels that are not associated with an aggregation protocol.

This command does not require a license.

Examples

This example shows how to display the counters for a specific port channel. This example display shows the transmitted and received unicast and multicast packets:

```
switch# show interface port-channel 2 counters
```

```
Port            InOctets   InUcastPkts   InMcastPkts   InBcastPkts
Po2                 6007             1            31             1

Port           OutOctets  OutUcastPkts  OutMcastPkts  OutBcastPkts
Po2                 4428             1            25             1
```

This example shows how to display the brief counters for a specific port channel. This display shows the transmitted and received rate and total frames:

```
switch# show interface port-channel 20 counters brief

--------------------------------------------------------------------------------
Interface              Input (rate is 1 min avg)  Output (rate is 1 min avg)
                       -------------------------  --------------------------
                       Rate     Total             Rate     Total
                       MB/s     Frames            MB/s     Frames
--------------------------------------------------------------------------------
port-channel20         0        0                 0        0
```

This example shows how to display all the detailed counters for a specific port channel:

```
switch# show interface port-channel 20 counters detailed all
port-channel20
  64 bit counters:
   0.                      rxHCTotalPkts = 0
   1.                       txHCTotalPks = 0
   2.                    rxHCUnicastPkts = 0
   3.                    txHCUnicastPkts = 0
   4.                  rxHCMulticastPkts = 0
   5.                  txHCMulticastPkts = 0
   6.                  rxHCBroadcastPkts = 0
   7.                  txHCBroadcastPkts = 0
   8.                         rxHCOctets = 0
   9.                         txHCOctets = 0
  10.                 rxTxHCPkts64Octets = 0
  11.           rxTxHCpkts65to127Octets = 0
  12.          rxTxHCpkts128to255Octets = 0
  13.          rxTxHCpkts256to511Octets = 0
  14.         rxTxHCpkts512to1023Octets = 0
  15.        rxTxHCpkts1024to1518Octets = 0
  16.        rxTxHCpkts1519to1548Octets = 0
  17.                    rxHCTrunkFrames = 0
  18.                    txHCTrunkFrames = 0
  19.                     rxHCDropEvents = 0

  All Port Counters:
   0.                           InPackets = 0
   1.                            InOctets = 0
   2.                         InUcastPkts = 0
   3.                         InMcastPkts = 0
   4.                         InBcastPkts = 0
   5.                         InJumboPkts = 0
   6.                   StormSuppressPkts = 0
   7.                          OutPackets = 0
   8.                           OutOctets = 0
   9.                        OutUcastPkts = 0
  10.                        OutMcastPkts = 0
  11.                        OutBcastPkts = 0
  12.                        OutJumboPkts = 0
  13.                    rxHCPkts64Octets = 0
  14.              rxHCPkts65to127Octets = 0
  15.             rxHCPkts128to255Octets = 0
  16.             rxHCPkts256to511Octets = 0
  17.            rxHCpkts512to1023Octets = 0
```

```
18.           rxHCpkts1024to1518Octets = 0
19.           rxHCpkts1519to1548Octets = 0
20.                   txHCPkts64Octets = 0
21.              txHCPkts65to127Octets = 0
22.             txHCPkts128to255Octets = 0
23.             txHCPkts256to511Octets = 0
24.            txHCpkts512to1023Octets = 0
25.           txHCpkts1024to1518Octets = 0
26.           txHCpkts1519to1548Octets = 0
27.                        ShortFrames = 0
28.                         Collisions = 0
29.                          SingleCol = 0
30.                          MultiCol = 0
31.                           LateCol = 0
32.                       ExcessiveCol = 0
33.                        LostCarrier = 0
34.                          NoCarrier = 0
35.                              Runts = 0
36.                             Giants = 0
37.                           InErrors = 0
38.                          OutErrors = 0
39.                       InputDiscards = 0
40.                       BadEtypeDrops = 0
41.                         IfDownDrops = 0
42.                     InUnknownProtos = 0
43.                               txCRC = 0
44.                               rxCRC = 0
45.                              Symbol = 0
46.                           txDropped = 0
47.                        TrunkFramesTx = 0
48.                        TrunkFramesRx = 0
49.                           WrongEncap = 0
50.                             Babbles = 0
51.                           Watchdogs = 0
52.                                 ECC = 0
53.                            Overruns = 0
54.                           Underruns = 0
55.                            Dribbles = 0
56.                            Deferred = 0
57.                             Jabbers = 0
58.                            NoBuffer = 0
59.                             Ignored = 0
60.                          bpduOutLost = 0
61.                          cos0OutLost = 0
62.                          cos1OutLost = 0
63.                          cos2OutLost = 0
64.                          cos3OutLost = 0
65.                          cos4OutLost = 0
66.                          cos5OutLost = 0
67.                          cos6OutLost = 0
68.                          cos7OutLost = 0
69.                              RxPause = 0
70.                              TxPause = 0
71.                               Resets = 0
72.                              SQETest = 0
73.                    InLayer3Routed = 0
74.                InLayer3RoutedOctets = 0
75.                     OutLayer3Routed = 0
76.                OutLayer3RoutedOctets = 0
77.                     OutLayer3Unicast = 0
78.              OutLayer3UnicastOctets = 0
79.                  OutLayer3Multicast = 0
80.           OutLayer3MulticastOctets = 0
81.                    InLayer3Unicast = 0
```

```
  82.              InLayer3UnicastOctets = 0
  83.                  InLayer3Multicast = 0
  84.             InLayer3MulticastOctets = 0
  85.               InLayer3AverageOctets = 0
  86.              InLayer3AveragePackets = 0
  87.              OutLayer3AverageOctets = 0
  88.             OutLayer3AveragePackets = 0
```

This example shows how to display the error counters for a specific port channel:

```
switch# show interface port-channel 5 counters errors

--------------------------------------------------------------------------------
Port       Align-Err     FCS-Err    Xmit-Err     Rcv-Err   UnderSize OutDiscards
--------------------------------------------------------------------------------
Po5                0           0           0           0           0           0
--------------------------------------------------------------------------------
Port      Single-Col   Multi-Col    Late-Col   Exces-Col   Carri-Sen       Runts
--------------------------------------------------------------------------------
Po5                0           0           0           0           0           0

--------------------------------------------------------------------------------
Port          Giants SQETest-Err Deferred-Tx IntMacTx-Er IntMacRx-Er  Symbol-Err
--------------------------------------------------------------------------------
                   0          --           0           0           0           0
```

This example shows how to display information about the trunk interfaces for a specific port channel:

```
switch# show interface port-channel 5 counters trunk

--------------------------------------------------------------------------------
Port            TrunkFramesTx   TrunkFramesRx      WrongEncap
--------------------------------------------------------------------------------
port-channel5               0               0               0
```

Related Commands

Command	Description
clear counters	Clears the statistics for all interfaces that belong to a specific channel group.

show interface status

To display the interface line status, use the **show interface status** command.

show interface status [**down** | **err-disabled** | **err-vlans** | **error policy** [**detail**] | **inactive** | **module** *number* | **up**]

Syntax Description

down	(Optional) Displays the interface down state.
err-disabled	(Optional) Displays the interface error-disabled state.
err-vlans	(Optional) Displays the VLANs with errors.
error policy	(Optional) Displays the interfaces and VLANs that generated an error during policy programming.
detail	(Optional) Displays details of the interface that generated the error.
inactive	(Optional) Displays the interface inactive state.
module *number*	(Optional) Displays the module number. The range is from 1 to 18.
up	(Optional) Displays the interface up state.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
6.2(2)	Added the **error policy** keyword to the syntax description.
4.1(2)	The **err-vlans** parameter was added.
4.0	This command was introduced.

Usage Guidelines

Use the **show interface status** to display the interface line status.

This command does not require a license.

Examples

This example shows how to display the interface status error policy details:

```
switch# configure terminal
switch# show interface status error policy detail

--------------------------------------------------------------------------------
```

```
No. Interface   Error Type      Time Stamp                Reason            VLAN
--------------------------------------------------------------------------------
switch#
```

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

```
switch# show interface status module 2

--------------------------------------------------------------------------------
Port           Name               Status   Vlan      Duplex  Speed   Type
--------------------------------------------------------------------------------
Eth2/1         --                 down     routed    auto    auto    1000BaseT
Eth2/2         --                 down     routed    auto    auto    1000BaseT
Eth2/3         --                 down     routed    auto    auto    1000BaseT
Eth2/4         --                 down     1         auto    auto    1000BaseT
Eth2/5         --                 down     routed    auto    auto    1000BaseT
Eth2/6         --                 down     1         auto    auto    1000BaseT
Eth2/7         server2            up       1         full    1000    1000BaseT
Eth2/8         --                 down     routed    auto    auto    1000BaseT
Eth2/9         --                 up       1         full    1000    1000BaseT
Eth2/10        ethernet slot 2 po down     1         auto    auto    1000BaseT
Eth2/11        --                 down     routed    auto    auto    1000BaseT
Eth2/12        --                 down     routed    auto    auto    1000BaseT
Eth2/13        --                 down     routed    auto    auto    1000BaseT
Eth2/14        --                 down     routed    auto    auto    1000BaseT
Eth2/15        --                 down     routed    auto    auto    1000BaseT
Eth2/16        --                 down     routed    auto    auto    1000BaseT
Eth2/17        --                 down     routed    auto    auto    1000BaseT
Eth2/18        --                 down     routed    auto    auto    1000BaseT
Eth2/19        --                 down     routed    auto    auto    1000BaseT
Eth2/20        --                 down     routed    auto    auto    1000BaseT
Eth2/21        --                 down     routed    auto    auto    1000BaseT
Eth2/22        --                 down     routed    auto    auto    1000BaseT
Eth2/23        --                 down     routed    auto    auto    1000BaseT
Eth2/24        --                 down     routed    auto    auto    1000BaseT
Eth2/25        --                 down     routed    auto    auto    1000BaseT
Eth2/26        --                 down     routed    auto    auto    1000BaseT
Eth2/27        --                 down     routed    auto    auto    1000BaseT
Eth2/28        --                 down     routed    auto    auto    1000BaseT
Eth2/29        --                 down     routed    auto    auto    1000BaseT
Eth2/30        --                 down     routed    auto    auto    1000BaseT
Eth2/31        --                 down     routed    auto    auto    1000BaseT
Eth2/32        --                 down     routed    auto    auto    1000BaseT
Eth2/33        --                 down     routed    auto    auto    1000BaseT
Eth2/34        --                 down     routed    auto    auto    1000BaseT
Eth2/35        --                 down     routed    auto    auto    1000BaseT
Eth2/36        --                 down     routed    auto    auto    1000BaseT
Eth2/37        --                 down     routed    auto    auto    1000BaseT
Eth2/38        --                 down     routed    auto    auto    1000BaseT
Eth2/39        --                 down     routed    auto    auto    1000BaseT
Eth2/40        --                 down     routed    auto    auto    1000BaseT
Eth2/41        --                 down     routed    auto    auto    1000BaseT
Eth2/42        --                 down     routed    auto    auto    1000BaseT
Eth2/43        --                 down     routed    auto    auto    1000BaseT
Eth2/44        --                 down     routed    auto    auto    1000BaseT
Eth2/45        --                 down     routed    auto    auto    1000BaseT
Eth2/46        --                 down     routed    auto    auto    1000BaseT
Eth2/47        --                 down     routed    auto    auto    1000BaseT
Eth2/48        --                 down     routed    auto    auto    1000BaseT
```

Related Commands

Command	Description
interface	Enters the interface configuration mode and configures the types and identities of interfaces.

show interface switchport

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

show interface [**ethernet** *type/slot* | **port-channel** *channel-number*] **switchport**

Syntax Description

ethernet *type/slot*	(Optional) Type and number of the interface that you want to display.
port-channel *channel-number*	(Optional) Specifies the port-channel number of the port-channel interface that you want to display. The range is from 1to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.2(1)	Information about private VLAN promiscuous trunk ports was added.
4.0	This command was introduced.

Usage Guidelines

If you do not specify an interface, this command displays information about all Layer 2 interfaces, including access, trunk, port-channel interfaces, and all private VLAN ports.

Use the **show interface counters** command to display statistics for the specified Layer 2 interface.

This command does not require a license.

Examples

This example shows how to display information for all Layer 2 interfaces:

```
switch# show interface switchport
Name: Ethernet2/5
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: access
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-3967,4048-4093
  Administrative private-vlan primary host-association: none
  Administrative private-vlan secondary host-association: none
  Administrative private-vlan primary mapping: none
  Administrative private-vlan secondary mapping: none
  Administrative private-vlan trunk native VLAN: none
```

```
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: none
  Administrative private-vlan trunk private VLANs: none
  Operational private-vlan: none

Name: Ethernet2/9
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: trunk
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-3967,4048-4093
  Administrative private-vlan primary host-association: none
  Administrative private-vlan secondary host-association: none
  Administrative private-vlan primary mapping: none
  Administrative private-vlan secondary mapping: none
  Administrative private-vlan trunk native VLAN: none
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: none
  Administrative private-vlan trunk private VLANs: none
  Operational private-vlan: none

Name: port-channel5
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: access
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-3967,4048-4093
  Administrative private-vlan primary host-association: none
  Administrative private-vlan secondary host-association: none
  Administrative private-vlan primary mapping: none
  Administrative private-vlan secondary mapping: none
  Administrative private-vlan trunk native VLAN: none
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: none
  Administrative private-vlan trunk private VLANs: none
  Operational private-vlan: none
```

Beginning with Cisco NX-OS Release 4.2(1), you can display information on private VLAN promiscuous trunk ports on Cisco Nexus 7000 Series devices. This example shows how to display information for those interfaces:

```
switch# show interface switchport
Name: Ethernet7/4
  Switchport: Enabled
  Administrative Mode: private-vlan trunk promiscuous
  Operational Mode: down
  Administrative Trunking Encapsulation: negotiate
  Negotiation of Trunking: on
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Administrative Native VLAN tagging: enabled
  Voice VLAN: none
  Administrative private-vlan host-association: none
  Administrative private-vlan mapping: none
  Administrative private-vlan secondary mapping: none
  Administrative private-vlan trunk Native VLAN tagging: enabled
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: 1, 4, 3000-4000
  Administrative private-vlan trunk private VLAN mappings:
      2 (VLAN0002)  3 (VLAN0003)           4 (VLAN0004)  5 (VLAN00005)
     10 (VLAN0010)  20 (CLAN0020)          30 (VLAN0030)  40 (Inactive)
  Operational private-vlan: none
```

Related Commands

Command	Description
switchport mode	Sets the specified interfaces as either Layer 2 access or trunk interfaces.

show interface transceiver

To display information about all the transceiver interfaces, use the **show interface transceiver** command.

show interface transceiver [**calibrations** | **details**]

Syntax Description

calibrations	(Optional) Displays calibration information for transceivers.
detail	(Optional) Displays detailed information for transceivers.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display calibration information for transceiver interfaces:

```
switch(config)# show interface transceiver calibrations

Ethernet9/25
    sfp is present
    name is CISCO-EXCELIGHT
    part number is SPP5101LR-C1
    revision is A
    serial number is ECL121601PB
    nominal bitrate is 10300 MBits/sec
    Link length supported for 9/125um fiber is 10 km(s)
    cisco id is --
    cisco extended id number is 4


                SFP External 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
```

This example shows how to display detailed information for transceiver interfaces:

```
switch(config)# show interface transceiver detailed

Ethernet10/9
    sfp is present
    name is CISCO
    part number is SPP5101SR-C1
    revision is A
    serial number is ECL1120017J
    nominal bitrate is 10300 MBits/sec
    Link length supported for 50/125um fiber is 82 m(s)
    Link length supported for 62.5/125um fiber is 26 m(s)
    cisco id is --
    cisco extended id number is 4

            SFP Detail Diagnostics Information (external calibration)
  ----------------------------------------------------------------------------
                                    Alarms                  Warnings
                                 High        Low         High          Low
  ----------------------------------------------------------------------------
  Temperature   25.54 C        75.00 C     -5.00 C     70.00 C        0.00 C
  Voltage        3.22 V         3.63 V      2.97 V      3.46 V        3.13 V
  Current        4.49 mA       10.00 mA     0.00 mA     9.00 mA       0.00 mA
  Tx Power       -3.50 dBm       2.99 dBm  -11.30 dBm   -1.00 dBm     -7.30 dBm
  Rx Power       -2.92 dBm       2.99 dBm  -13.97 dBm   -1.00 dBm     -9.91 dBm
  Transmit Fault Count = 0
  ----------------------------------------------------------------------------
```

Related Commands

Command	Description
show interface	Displays information about the specified interfaces.

show interface trunk

To display information about all the trunk interfaces, use the **show interface trunk** command.

show interface [**ethernet** *slot/port* | **port-channel** *channel-number*] **trunk** [**module** *number* | **vlan** *vlan-id*]

Syntax Description

ethernet *slot/port*	(Optional) Type and number of the interface that you want to display.
port-channel *channel-number*	(Optional) Specifies the port-channel number of the port-channel interface that you want to display.
module *number*	(Optional) Specifies the module number. The range is from 1 to 18.
vlan *vlan-id*	(Optional) Specifies the VLAN number. The range is from 1 to 2499 and from 2628 to 4093.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

If you do not specify an interface, a module number, or a VLAN number, the system displays information for all trunk interfaces.

This command displays information about all Layer 2 trunk interfaces and trunk port-channel interfaces.

Use the **show interface counters** command to display statistics for the specified Layer 2 interface.

This command does not require a license.

Examples

This example shows how to display information for all Layer 2 trunk interfaces:

```
switch(config)# show interface trunk

--------------------------------------------------------------------------------
Port       Native  Status        Port
           Vlan                  Channel
--------------------------------------------------------------------------------
Eth2/9     1       trunking      --
Eth2/10    1       trnk-bndl     Po50
Po50       1       not-trunking  --
```

```
--------------------------------------------------------------------------------
Port       Vlans Allowed on Trunk
--------------------------------------------------------------------------------
Eth2/9     1-3967,4048-4093
Eth2/10    1-3967,4048-4093
Po50       1-3967,4048-4093

--------------------------------------------------------------------------------
Port       STP Forwarding
--------------------------------------------------------------------------------
Eth2/9     none
Eth2/10    none
Po50       none
```

Related Commands

Command	Description
switchport mode trunk	Sets the specified interfaces as Layer 2 trunk interfaces.

show interface tunnel

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

show interface tunnel *number*

Syntax Description

number	Number of the tunnel interface that you want to display information for. The range is from 0 to 65503.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.2(1)	Display of configured static MAC address was added.
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information about tunnel interfaces:

```
switch(config)# show interface tunnel 5

Tunnel5 is down (Administratively down)
    MTU 1476 bytes, BW 9 Kbit
    Transport protocol is in VRF "default"
    Tunnel protocol/transport GRE/IP
    Last clearing of "show interface" counters never
    Tx
    0 packets output, 1 minute output rate 0 packets/sec
    Rx
    0 packets input, 1 minute input rate 0 packets/sec
```

Related Commands

Command	Description
show interface	Displays information about the specified interfaces.

show ip dhcp snooping statistics

To display statistics related to the Dynamic Host Configuration Protocol (DHCP), use the **show ip dhcp snooping statistics** command.

show ip dhcp snooping statistics

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC mode

Command History

Release	Modification
5.1(1)	Added the command output (added two counters)
4.0	This command was introduced.

Usage Guidelines

To enable this feature, use the **feature dhcp** command.

Examples

This example shows how to display statistics related to DHCP:

```
switch# show ip dhcp snooping statistics
Packets processed 0
Packets received through cfsoe 0
Packets forwarded 0
Packets forwarded on cfsoe 0
Total packets dropped 0
Packets dropped from untrusted ports 0
Packets dropped due to MAC address check failure 0
Packets dropped due to Option 82 insertion failure 0
Packets dropped due to o/p intf unknown 0
Packets dropped which were unknown 0
Packets dropped due to dhcp relay not enabled 0
Packets dropped due to no binding entry 0
Packets dropped due to interface error/no interface 0
Packets dropped due to max hops exceeded 0
switch#
```

Related Commands

Command	Description
show ip dhcp snooping statistics	Display statistics related to the Dynamic Host Configuration Protocol.

show lacp counters

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

show lacp counters [**interface port-channel** *channel-number*]

Syntax Description

interface port-channel	(Optional) Specifies the interface port channel.
channel-number	(Optional) Number of the LACP channel group. The range is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

If you do not specify the *channel-number*, all channel groups are displayed.

This command does not require a license.

Examples

This example shows how to display the LACP statistics for a specific channel group:

```
switch# show lacp counters interface port-channel 1

LACPDUs          Marker      Marker Response    LACPDUs
Port               Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
--------------------------------------------------------------------------------
port-channel1
Ethernet1/1         554    536       0      0        0      0         0
Ethernet1/2         527    514       0      0        0      0         0
Ethernet1/3         535    520       0      0        0      0         0
Ethernet1/4         515    502       0      0        0      0         0
Ethernet1/5         518    505       0      0        0      0         0
Ethernet1/6         540    529       0      0        0      0         0
Ethernet1/7         541    530       0      0        0      0         0
Ethernet1/8         547    532       0      0        0      0         0
Ethernet1/9         544    532       0      0        0      0         0
Ethernet1/10        513    501       0      0        0      0         0
Ethernet1/11        497    485       0      0        0      0         0
Ethernet1/12        493    486       0      0        0      0         0
Ethernet1/13        492    485       0      0        0      0         0
```

```
Ethernet1/14        482     481       0         0          0         0          0
Ethernet1/15        481     476       0         0          0         0          0
Ethernet1/16        482     477       0         0          0         0          0
```

Related Commands

Command	Description
clear lacp counters	Clears the statistics for all LACP interfaces or those interfaces that belong to a specific LACP channel group.

show lacp interface

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

show lacp interface ethernet *slot/port*

Syntax Description

slot/port	Slot number and port number for the interface you want to display. The range is from 1 to 253.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The LACP_Activity field displays whether the link is configured in the active or passive port-channel mode.

The Port Identifier field displays the port priority as part of the information. The part of the information in this field is the port number. The following example shows how to identify the port priority and the port number:

Port Identifier=0x8000,0x101

The port priority value is 0x8000, and the port number value is 0x101 in this example.

This command does not require a license.

Examples

This example shows how to display the LACP statistics for a specific channel group:

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

switch(config-if-range)# show lacp interface eth1/1
Interface Ethernet1/1 is up
  Channel group is 1 port channel is Po1
  PDUs sent: 556
  PDUs rcvd: 538
  Markers sent: 0
  Markers rcvd: 0
  Marker response sent: 0
  Marker response rcvd: 0
```

```
  Unknown packets rcvd: 0
  Illegal packets rcvd: 0
Lag Id: [ [(8000, 0-11-11-22-22-74, 0, 8000, 101), (8000, 0-11-11-22-22-75, 0, 8
000, 401)] ]
Operational as aggregated link since Wed Jun 11 20:37:59 2008

Local Port: Eth1/1   MAC Address= 0-11-11-22-22-74
  System Identifier=0x8000,0-11-11-22-22-74
  Port Identifier=0x8000,0x101
  Operational key=0
  LACP_Activity=active
  LACP_Timeout=Long Timeout (30s)
  Synchronization=IN_SYNC
  Collecting=true
  Distributing=true
  Partner information refresh timeout=Long Timeout (90s)
Actor Admin State=
Actor Oper State=
Neighbor: 4/1
  MAC Address= 0-11-11-22-22-75
  System Identifier=0x8000,0-11-11-22-22-75
  Port Identifier=0x8000,0x401
  Operational key=0
  LACP_Activity=active
  LACP_Timeout=Long Timeout (30s)
  Synchronization=IN_SYNC
  Collecting=true
  Distributing=true
Partner Admin State=
Partner Oper State=
```

Related Commands

Command	Description
show port-channel summary	Displays information about all port-channel groups.

show lacp neighbor

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

show lacp neighbor [**interface port-channel** *channel-number*]

Syntax Description

interface port-channel	(Optional) Specifies the interface port channel.
channel-number	(Optional) Port-channel number for the LACP neighbor that you want to display. The range is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

If you do not specify the *channel-number*, all channel groups are displayed.

This command does not require a license.

Examples

This example shows how to display the information about the LACP neighbors for a specific port channel:

```
switch# show lacp neighbor interface port-channel 1
Flags:  S - Device is sending Slow LACPDUs F - Device is sending Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode
port-channel1 neighbors
Partner's information
          Partner               Partner                   Partner
Port      System ID             Port Number     Age       Flags
Eth1/1    32768,0-11-11-22-22-750x401           44817     SA

          LACP Partner          Partner                   Partner
          Port Priority         Oper Key                  Port State
          32768                 0x0                       0x3d

Partner's information
          Partner               Partner                   Partner
```

```
Port      System ID             Port Number     Age         Flags
Eth1/2    32768,0-11-11-22-22-750x402           44817       SA

          LACP Partner          Partner                     Partner
          Port Priority         Oper Key                    Port State
          32768                 0x0                         0x3d
```

Related Commands

Command	Description
show port-channel summary	Displays information about all port-channel groups.

show lacp port-channel

To display information about Link Aggregation Control Protocol (LACP) port channels, use the **show lacp port-channel** command.

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

Syntax Description

interface port-channel	(Optional) Specifies the interface port channel.
channel-number	(Optional) Port-channel number for the LACP neighbor that you want to display. The range is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

If you do not specify the *channel-number*, all channel groups are displayed.

This command does not require a license.

Examples

This example shows how to display the information about LACP port channels:

```
switch# show lacp port-channel

port-channel1
  Local System Identifier=0x8000,0-11-11-22-22-74
  Admin key=0x0
  Operational key=0x0
  Partner System Identifier=0x8000,0-11-11-22-22-75
  Operational key=0x0
  Max delay=0
  Aggregate or individual=1
port-channel2
  Local System Identifier=0x8000,0-11-11-22-22-74
  Admin key=0x1
  Operational key=0x1
  Partner System Identifier=0x8000,0-11-11-22-22-75
  Operational key=0x1
  Max delay=0
```

```
Aggregate or individual=1
```

Related Commands

Command	Description
show port-channel summary	Displays information about all port-channel groups.

show lacp system-identifier

To display the Link Aggregation Control Protocol (LACP) system identifier for the device, use the **show lacp system-identifier** command.

show lacp system-identifier

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The LACP system ID is the combination of the configurable LACP system priority value and the MAC address.

Each system that runs LACP has an LACP system priority value. You can accept the default value of 32768 for this parameter, or 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 uses the system priority during negotiation with other devices. A higher system priority value means a lower priority.

The system ID is different for each virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to display the information about the LACP port channel for a specific port channel:

```
switch# show lacp system-identifier
8000,AC-12-34-56-78-90
```

Related Commands

Command	Description
lacp system-priority	Sets the system priority for LACP.

show ospfv3

To display general information about the Open Shortest Path First version 3 (OSPFv3) routing process, use the **show ospfv3** command.

show ospfv3 [process-id]

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Interface configuration mode

SupportedUserRoles None

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines OSPFv3 must be running on all participating devices. You must configure the he baseline parameters for Bidirectional Forwarding Detection (BFD) sessions on the interfaces over which you want to run BFD sessions to BFD neighbors must be configured.

Examples This example shows how to display the general information about to discover the OSPFv3 routing process:

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-router)# ospfv3 bfd disable
switch(config-if)# exit
switch(config)# show bfd neighbors details
switch(config)# show ospfv3

Routing Process 3 with ID 172.1.2.1 VRF default
Routing Process Instance Number 1
Stateful High Availability enabled
Graceful-restart is configured
Grace period: 60 state: Inactive
Last graceful restart exit status: None
Supports only single TOS(TOS0) routes
Supports opaque LSA
Administrative distance 110
Reference Bandwidth is 40000 Mbps
SPF throttling delay time of 200.000 msecs,
SPF throttling hold time of 1000.000 msecs,
SPF throttling maximum wait time of 5000.000 msecs
LSA throttling start time of 0.000 msecs,
```

```
LSA throttling hold interval of 5000.000 msecs,
LSA throttling maximum wait time of 5000.000 msecs
Minimum LSA arrival 1000.000 msec
LSA group pacing timer 10 secs
Maximum paths to destination 8
Number of external LSAs 0, checksum sum 0
Number of areas is 0, 0 normal, 0 stub, 0 nssa
Number of active areas is 0, 0 normal, 0 stub, 0 nssa
Install discard route for summarized external routes.
Install discard route for summarized internal routes.
BFD is enabled

Routing Process 200 with ID 172.1.2.1 VRF default
Routing Process Instance Number 2
Stateful High Availability enabled
Graceful-restart is configured
Grace period: 60 state: Inactive
Last graceful restart exit status: None
Supports only single TOS(TOS0) routes
Supports opaque LSA
Administrative distance 110
Reference Bandwidth is 40000 Mbps
SPF throttling delay time of 200.000 msecs,
SPF throttling hold time of 1000.000 msecs,
SPF throttling maximum wait time of 5000.000 msecs
LSA throttling start time of 0.000 msecs,
LSA throttling hold interval of 5000.000 msecs,
LSA throttling maximum wait time of 5000.000 msecs
 Minimum LSA arrival 1000.000 msec
 LSA group pacing timer 10 secs
 Maximum paths to destination 8
 Number of external LSAs 0, checksum sum 0
 Number of areas is 0, 0 normal, 0 stub, 0 nssa
 Number of active areas is 0, 0 normal, 0 stub, 0 nssa
 Install discard route for summarized external routes.
 Install discard route for summarized internal routes.
switch(config)#
```

Related Commands

Command	Description
ospfv3 bfd	Enables BFD on a per-interface basis for one or more interfaces associated with the OSPFv3 routing process.

show port-channel compatibility-parameters

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

show port-channel compatibility-parameters

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Any command mode

SupportedUserRoles network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines When you add an interface to a channel group, the software checks certain interface attributes to ensure that the interface is compatible with the channel group. For example, you cannot add a Layer 3 interface to a Layer 2 channel group. The software also checks the operational attributes for an interface before allowing that interface to participate in the port-channel aggregation.

This command displays the list of compatibility checks that the system uses.

Using the **channel-group** command, you can force ports with incompatible parameters to join the port channel as long as the following parameters are the same:

- (Link) speed capability
- Speed configuration
- Duplex capability
- Duplex configuration
- Flow-control capability
- Flow-control configuration

Note See the **channel-group** command for information about forcing ports to join a port channel.

This command does not require a license.

Examples

This example shows how to display the list of compatibility checks that the system makes to ensure that an interface is compatible with a channel group:

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

Members must have the same port mode configured, either E or AUTO. If they
are configured in AUTO port mode, they have to negotiate E 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.

* MTU

Members have to have the same MTU configured. This only applies to ethernet
port-channel.

* MEDIUM

Members have to have the same medium type configured. This only applies to
ethernet port-channel.

* Span mode

Members must have the same span mode.

* sub interfaces

Members must not have sub-interfaces.

* Duplex Mode

Members must have same Duplex Mode configured.

* Ethernet Layer

Members must have same Ethernet Layer (switchport/no-switchport) configured.

* Span Port

Members cannot be SPAN ports.

* Storm Control

Members must have same storm-control configured.

* Flow Control

Members must have same flowctrl configured.

* Capabilities

Members must have common capabilities.

* port

Members port VLAN info.

* port
```

```
Members port does not exist.

* switching port

Members must be switching port, Layer 2.

* port access VLAN

Members must have the same port access VLAN.

* port native VLAN

Members must have the same port native VLAN.

* port allowed VLAN list

Members must have the same port allowed VLAN list.
```

Related Commands

Command	Description
channel-group	Adds or removes interfaces to port-channel groups and assigns the port-channel mode to the interface.

show port-channel database

To display information about the port channels, use the **show port-channel database** command.

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

Syntax Description

interface port-channel	(Optional) Specifies the interface port channel.
channel-number	(Optional) Port-channel number for the Link Aggregation Control Protocol (LACP) neighbor that you want to display. The range is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

If you do not specify the *channel-number*, all channel groups are displayed. This command displays Link Aggregation Control Protocol (LACP)-enabled ports channels and port channels without an associated aggregation protocol.

This command does not require a license.

Examples

This example shows how to display information about all port channels:

```
switch# show port-channel database
port-channel5
    Administrative channel mode is active
    Operational channel mode is active
    Last membership update is successful
    1 ports in total, 0 ports up
    Age of the port-channel is 1d:16h:18m:50s
    Time since last bundle is 1d:16h:18m:56s
    Last bundled member is
    Ports:   Ethernet2/5            [down]

port-channel20
    Administrative channel mode is active
    Operational channel mode is active
```

```
    Last membership update is successful
    1 ports in total, 0 ports up
    Age of the port-channel is 1d:16h:18m:50s
    Time since last bundle is 1d:16h:18m:56s
    Last bundled member is
    Ports:   Ethernet2/20           [down]
```

This example shows how to display information about a specific port channel:

```
switch# show port-channel database interface port-channel 20
port-channel20
    Administrative channel mode is active
    Operational channel mode is active
    Last membership update is successful
    1 ports in total, 0 ports up
    Age of the port-channel is 1d:16h:23m:14s
    Time since last bundle is 1d:16h:23m:20s
    Last bundled member is
    Ports:   Ethernet2/20           [down]
```

Related Commands

Command	Description
show port-channel summary	Displays a summary of information about all port channels.

show port-channel load-balance

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

show port-channel load-balance [**forwarding-path interface port-channel** *channel-number*]

Syntax Description

forwarding-path interface port-channel	(Optional) Identifies the port in the port channel that forwards the packet.
channel-number	Port-channel number for the load-balancing forwarding path that you want to display. The is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information about the current port-channel load balancing for the system:

```
switch# show port-channel load-balance

Port Channel Load-Balancing Configuration:
System: source-dest-ip-vlan

Port Channel Load-Balancing Addresses Used Per-Protocol:
Non-IP: source-dest-mac
IP: source-dest-ip-vlan
```

Related Commands

Command	Description
port-channel load-balance ethernet	Configures load balancing using port channels.

show port-channel rbh-distribution

To display information about the Result Bundle Hash (RBH) for port channels, use the **show port-channel rbh-distribution** command.

show port-channel rbh-distribution [**interface port-channel** *channel-number*]

Syntax Description

interface port-channel	(Optional) Specifies the interface port channel.
channel-number	(Optional) Port-channel number for the LACP neighbor that you want to display. The range is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The RBH value ranges from 0 to 7 and is shared among port members in a port channel.

This command does not require a license.

Examples

This example shows how to display RBH distribution for a specific port channel:

```
switch# show port-channel rbh-distribution interface port-channel 4

ChanId    Member port    RBH values         Num of buckets
--------  -------------  -----------------  ----------------
 4         Eth3/13        4,5,6,7            4
 4         Eth3/14        0,1,2,3            4
```

Related Commands

Command	Description
port-channel summary	Displays summary information about port channels.

show port-channel summary

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

show port-channel summary

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
5.1(1)	Added a new port channel status ‘M’ to the command output.
4.0	This command was introduced.

Usage Guidelines

If the Link Aggregation Control Protocol (LACP) is not enabled, the output shows “NONE” in the Protocol column of the display.

A channel-group interface can be in the following operational states:

- Down—The interface is down because it is administratively shut down or some other reason not related to port channels.
- Individual—The interface is part of a port channel but is unable to aggregate into a port channel because of protocol exchange problems:
  - This interface continues to forward traffic as an individual link.
  - STP is aware of this interface.
- Suspended—The operational parameters of the interface are not compatible with the port channel. This interface is not forwarding traffic, although the physical MAC link state is still up.
- Switched—The interface is switched.
- Up (port channel)—The port channel is up.
- Up in port channel (members)—The port member of the port channel is up.
- Hot standby (LACP only)—The interface is eligible to join the port group if one of the interfaces currently participating in the LACP channel goes down.
  - This interface does not forward data traffic; it forwards only protocol data units (PDUs).

  - This interface does not run STP.
- Module-removed—The module has been removed.
- Routed—The interface is routed.

This command does not require a license.

Examples

This example shows how to display summary information for the port channels:

```
switch(config-if)# 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)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
     Channel
--------------------------------------------------------------------------------
2     Po2(SU)     Edge     LACP      Eth4/9(D)    Eth4/10(D)   Eth4/11(P)
                                     Eth4/12(P)
3     Po3(SU)     Edge     LACP      Eth4/27(P)   Eth4/28(P)   Eth4/29(P)
                                     Eth4/30(P)
10    Po10(SU)    Edge     LACP      Eth4/1(P)    Eth4/2(P)    Eth4/3(P)
                                     Eth4/4(P)    Eth4/13(P)   Eth4/14(P)
                                     Eth4/15(P)   Eth4/16(P)   Eth4/17(P)
                                     Eth4/18(P)   Eth4/19(P)   Eth4/20(P)
                                     Eth4/21(P)   Eth4/22(P)   Eth4/23(P)
                                     Eth4/24(P)
```

Related Commands

Command	Description
show port-channel usage	Displays the port-channel numbers used and available.
show port-channel traffic	Displays transmitted and received unicast, multicast, and broadcast percentages for the port channels.

show port-channel traffic

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

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

Syntax Description

interface port-channel	(Optional) Specifies the interface port channel.
channel-number	(Optional) Port-channel number for the LACP neighbor that you want to display. The range is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This command displays the percentage of transmitted and received unicast, multicast, and broadcast traffic about the port channel.

If you do not specify the *channel-number*, information for all port channels is displayed.

This command does not require a license.

Examples

This example shows how to display the traffic statistics for all port channels:

```
switch(config)# show port-channel traffic
ChanId      Port Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ --------- ------- ------- ------- ------- ------- -------
     5    Eth2/5    0.0%    0.0%    0.0%    0.0%    0.0%    0.0%
------ --------- ------- ------- ------- ------- ------- -------
    20   Eth2/20    0.0%    0.0%    0.0%    0.0%    0.0%    0.0%
```

This example shows how to display the traffic statistics for a specific port channel:

```
switch(config)# show port-channel traffic interface port-channel 5
ChanId      Port Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ --------- ------- ------- ------- ------- ------- -------
     5    Eth2/5    0.0%    0.0%    0.0%    0.0%    0.0%    0.0%
```

Related Commands

Command	Description
port-channel summary	Displays summary information about port channels.

show port-channel usage

To display the port-channel numbers used and available, use the **show port-channel usage** command.

show port-channel usage

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This command displays port-channel numbers used and available in the virtual device context (VDC) that you are monitoring.

The number of port-channel numbers available across all VDCs for the entire system is from 1 to 4096.

This command does not require a license.

Examples

This example shows how to display the usage for all port channels:

```
switch# show port-channel usage
Totally 2 port-channel numbers used
====================================
Used  :   5 , 20
Unused:   1 - 4 , 6 - 19 , 21 - 4096
```

Related Commands

Command	Description
port-channel summary	Displays summary information about port channels.

show port-profile

To display information about port profiles, use the **show port-profil**e command.

show port-profile [**brief** | **expand-interface** [**name** *name*] | **name** *name* | **usage**]

Syntax Description

brief	(Optional) Displays brief information about the port profiles.
expand-interface name	(Optional) Displays the configured attributes at an interface per port profile. An optional name can be specified to show the expanded interface output for that specific port profile.
name *name*	(Optional) Displays information for the specified port profile.
usage	(Optional) Displays a list of interfaces to which each profile is attached.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **show port-profile** command to display information about the configured port profiles on the device. It displays all configured port profiles.

Port profiles are not aware of default values, so the default value configuration appears in the port profiles. For example, MTU 1500 is a default value and does not appear in the running-configuration of an interface. However, because port profiles are unaware of default values, MTU 1500 appears in the port-profile display.

This command does not require a license.

Examples

This example shows how to display information about port profiles:

```
switch(config)# show port-profile
 try1
 type: Ethernet
 description:
 status: enabled
 max-ports: 512
 inherit:
```

```
 config attributes:
  channel-group 5
 evaluated config attributes:
  channel-group 5
 assigned interfaces:
  Ethernet1/1

 try2
 type: Ethernet
 description:
 status: disabled
 max-ports: 512
 inherit:
 config attributes:
 evaluated config attributes:
 assigned interfaces:
```

This example shows how to display brief port profile information:

```
switch(config)# show port-profile brief
-------------------------------------------------------------
Port                Profile  Conf   Eval   Assigned  Child
Profile              State   Items  Items  Intfs     Profs
-------------------------------------------------------------
try1                1        1      1      1         0
try2                0        0      0      0         0
```

This example shows how to display expanded port profile interface information:

```
switch(config)# show port-profile expand-interface
 try1
 Ethernet1/1
  channel-group 5

 try2
```

This example shows how to display specific port profile information:

```
switch(config)# show port-profile name try1
 try1
 type: Ethernet
 description:
 status: enabled
 max-ports: 512
 inherit:
 config attributes:
  channel-group 5
 evaluated config attributes:
  channel-group 5
 assigned interfaces:
  Ethernet1/1


switch(config)# show port-profile usage
 try1
 Ethernet1/1
```

This example shows how to display port profiles and values that you have entered in interface configuration mode using the **show running-config** command:

```
switch(config)# show running-config interface ethernet 8/5
interface ethernet8/5
 inherit  try1
 mtu 3000
```

Related Commands

Command	Description
port-profile	Configures, names, and allows you to enter port-profile configuration mode.
inherit port-profile	Assigns port profile to specified interfaces and allows one port profile to inherit configuration parameters from another port profile.

show running-config interface

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

show running-config interface [**all** | {**ethernet** {*slot/port*} [**all**]} | **expand-port-profile** | {**loopback** {*number*} [**all**]} | {**mgmt0** [**all**]} | {**port-channel** {*channel-number*} [**membership**]} | {**tunnel** {*number*} [**all**]} | {**vlan** {*vlan-id*} [**all**]}

Syntax Description

all	(Optional) Displays the configuration with defaults.
ethernet *slot/port*	Displays the number of the module and port number. The range is from 1 to 253.
expand-port-profile	(Optional) Displays port profiles.
loopback *number*	Displays the number of the loopback interface. The range is from 1 to 4096.
mgmt0	(Optional) Displays the management interface.
port-channel *channel-number*	Displays the number of the port-channel group. The range is from 0 to 1023.
membership	(Optional) Specifies the membership of the specified port channel.
tunnel *number*	Displays the number of the tunnel interface. The range is from 0 to 65535.
vlan *vlan-id*	Displays the number of the VLAN. The range is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.
4.2(1)	The **expand-port-profile** parameter was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information about the running configuration for a specific Ethernet interface:

```
switch(config)# show running-config interface ethernet 2/7
```

```
version 4.0(3)

interface Ethernet2/7
  description Ethernet port 3 on module 1
  mtu 8000
  delay 20
  udld enable
  no shutdown
```

This example shows how to display information about the running configuration for a specific range of Ethernet interfaces:

```
switch(config)# show running-config interface ethernet 2/7 - 9
version 4.0(3)

interface Ethernet2/7
  description Ethernet port 3 on module 1
  mtu 8000
  delay 20
  udld enable
  no shutdown

interface Ethernet2/8
  no shutdown

interface Ethernet2/9
  no shutdown
```

This example shows how to display information about the running configuration for a specific loopback interface:

```
switch(config)# interface loopback 345
switch(config-if)# show running-config interface loopback 345
version 4.0(3)
interface loopback345
```

This example shows how to display the running configuration for a specific port channel:

```
switch(config)# show running-config interface port-channel 10
version 4.0(1)

interface port-channel10
  switchport
  switchport mode trunk
```

This example shows how to display information about the running configuration for VLAN interface 50:

```
switch(config)# show running-config interface vlan 50
version 4.0(3)

interface Vlan50
```

Related Commands

Command	Description
interface	Enters the interface configuration mode and configures the types and identities of interfaces.
interface vlan	Creates a VLAN interface and enters interface configuration mode.
show interface ethernet	Displays information about the Ethernet interface.

Command	Description
show port-channel summary	Displays a summary of port-channel information.
show running-config	Displays the running configuration on the device.

show running-config interface mgmt

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

show running-config interface mgmt {*number*}

Syntax Description

number	Management interface number that you want to display. The value is from 0 to 0.

Defaults

None

Command Modes

Any command mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **show running-config interface mgmt** command to display the running configuration for a management interface.

This command does not require a license.

Examples

This example shows how to display information about the running configuration for management interface 0:

```
switch# show running-config interface mgmt 0
version 4.0(3)

interface mgmt0
  ip address 172.28.231.193/23
```

Related Commands

Command	Description
show interface mgmt	Displays the management interface information.

show running-config vpc

To display the running configuration information for virtual port channels (vPCs), use the **show running-config vpc** command.

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

Syntax Description

all	(Optional) Displays the running configuration for all vPCs.

Defaults

None

Command Modes

Any command mode.

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the running configuration for a vPC:

```
switch (config)# show running-config vpc
version 4.1(2)
feature vpc
vpc domain 2
  role priority 1
  system-priority 32667
  peer-keepalive destination 10.10.76.52 source 10.10.76.51 udp-port 3200 vrf ma
engagement interval 1000 timeout 5


interface port-channel10
  vpc 20

interface port-channel101
  vpc 101

interface port-channel200
  vpc peer-link

interface port-channel201
  vpc 201
```

Related Commands

Command	Description
show vpc brief	Displays information about vPCs. If the feature is not enabled, this command returns an error.

show startup-config interface

To display interface configuration information in the startup configuration, use the **show startup-config interface** command.

show startup-config interface [**ethernet** *slot/port* | **expand-port-profile** | **loopback** *number* | **mgmt** | **port-channel** {*channel-number*} [**membership**] | **tunnel** *number* | {**vlan** *vlan-id*}]

Syntax Description

ethernet *slot/port*	(Optional) Displays the number of the module and port number.
expand-port-profile	(Optional) Displays the port profiles.
loopback *number*	(Optional) Displays the number of the loopback interface. The range is from 1 to 4096.
mgmt	(Optional) Displays the management interface.
port-channel *channel-number*	(Optional) Displays the number of the port-channel group. The range is from 0 to 1023.
membership	(Optional) Displays the membership of the specified port channel.
tunnel *number*	(Optional) Displays the number of the tunnel interface. The range is from 0 to 65535.
vlan *vlan-id*	(Optional) Displays the number of the VLAN. The range is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.
4.2(1)	The **expand-port-profile** parameter was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the information in the startup configuration for the interface Ethernet 7/1:

```
switch(config)# show startup-config interface ethernet 7/1
version 4.1(2)

interface Ethernet7/1
```

```
ip pim sparse-mode
```

Related Commands

Command	Description
show interface	Displays information about the specified interface.

show startup-config vpc

To display virtual port-channel (vPC) configuration information in the startup configuration, use the **show startup-config vpc** command.

show startup-config vpc [**all**]

Syntax Description

all	(Optional) Displays the startup-configuration information for all vPCs.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the vPC information in the startup configuration:

```
switch(config)# show startup-config vpc
version 4.1(2)
feature vpc
vpc domain 1


interface port-channel10
  vpc peer-link

interface port-channel120
  vpc 100
```

Related Commands

Command	Description
show vpc brief	Displays information about vPCs.

show udld

To display information about the Unidirectional Link Detection (UDLD) configuration, use the **show udld** command.

show udld [**ethernet** *slot/port* | **global** | **neighbors**]

Syntax Description

ethernet *slot/port*	(Optional) Displays the Ethernet slot and port number you want to display. The range is from 1 to 253.
global	(Optional) Displays the UDLD global status and configuration on all interfaces.
neighbors	(Optional) Displays the UDLD neighbor interfaces.

Defaults

None

Command Modes

Any command mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **show udld** command to display information about the UDLD configuration for an interface. UDLD must be enabled on the device before you can display this command; enter the **feature udld** command to enable UDLD globally on the device.

This command does not require a license.

Examples

This example shows how to display information about the UDLD configuration for Ethernet port 2/7:

```
switch# show udld ethernet 2/7

Interface Ethernet2/7
---------------------------------
Port enable administrative configuration setting: disabled
Port enable operational state: disabled
Current bidirectional state: unknown
Current operational state:  udld-init - Multiple neighbor not detected
Message interval: 7
Timeout interval: 5
```

Related Commands

Command	Description
udld	Configures the ports to use a UDLD mode.
feature udld	Enables UDLD globally on device.

show vdc

To display virtual device contexts (VDCs), use the **show vdc** command.

show vdc

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display VDCs:

```
switch# show vdc
Switchwide mode is m1 f1 m1xl f2 m2xl

vdc_id  vdc_name                        state               mac
  type        lc
------  --------                        -----               ----------
  ---------   ------
1       switch                          active              00:22:55:79:a4:c1
  Ethernet    m1 f1 m1xl m2xl
2       2                               active              00:22:55:79:a4:c2
  Ethernet    m1 f1 m1xl m2xl

switch#
```

Related commands

Command	Description
show lacp	Displays LACP information.

show vpc brief

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

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

Syntax Description

vpc *number*	(Optional) Displays brief information about the specified vPC. The range is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
6.1(2)E1	Added an example with the **fabricpath load balance** command and the **no port-channel limit** command.
6.1(2)	Changed the command output.
4.2(1)	Added the **vpc** keyword and *number* argument.
4.1(3)	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 the 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 on enabling vPCs.

Beginning with Cisco Release 4.2(1), you can display the track object, if you have configured a tracked object for running vPCs on a single module under the vpc-domain configuration mode.

This command does not require a license.

Examples

This example shows how to display brief information about the vPCs:

```
switch(config)# show vpc brief
switch-peer1(config)# show vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 1
vPC+ switch id                    : 2
```

```
Peer status                         : peer adjacency formed ok
vPC keep-alive status               : peer is alive
vPC fabricpath status               : peer is reachable through fabricpath
Configuration consistency status    : success
Per-vlan consistency status         : success
Type-2 inconsistency reason         : Consistency Check Not Performed
vPC role                            : primary
Number of vPCs configured           : 8
Peer Gateway                        : Disabled
Dual-active excluded VLANs          : -
Graceful Consistency Check          : Enabled
Auto-recovery status                : Disabled
Fabricpath load balancing           : Enabled
Port Channel Limit                  : limit to 244

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--More-
```

This example shows how to displays brief information about the vPCs when the **fabricpath load balance** command and the **no port-channel limit** command are configured:

```
switch(config-vpc-domain)# show vpc
Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id : 1
vPC+ switch id : 1
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
vPC fabricpath status : peer is not reachable through fabricpath
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role : secondary
Number of vPCs configured : 1
Peer Gateway : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Disabled
Fabricpath load balancing : Enabled
Operational Layer3 Peer : Disabled
Port Channel Limit : no limit
vPC Peer-link status
---------------------------------------------------------------------
id Port Status Active vlans
-- ---- ------ --------------------------------------------------

1 Po100 up 1-10
vPC status
----------------------------------------------------------------------------
id Port Status Consistency Reason Active vlans vPC+ Attribute
-- ---- ------ ----------- ------ ------------ --------------
1 Po1 up success success 1-10 DF: Partial, FP
MAC: 1.1.4513
```

This example shows how to display brief information about the vPCs when **no port-channel limit** is added:

```
switch-peer1(config-vpc-domain)# no port-channel limit
switch-peer1(config-vpc-domain)# show vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link
```

```
vPC domain id                     : 1
vPC+ switch id                    : 2
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
vPC fabricpath status             : peer is reachable through fabricpath
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 inconsistency reason       : Consistency Check Not Performed
vPC role                          : primary
Number of vPCs configured         : 8
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Disabled
Fabricpath load balancing         : Enabled
Port Channel Limit                : no limit

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--More--
```

This example also shows how to display brief information about the vPCs. In this example, the port channel failed the consistency check, and the device displays the reason for the failure:

```
switch(config)# show vpc brief

Legend:
                (*) - local vpc is down, forwarding via vPC peer-link

vPC domain id                   : 10
Peer status                     : peer adjacency formed ok
vPC keep-alive status           : peer is alive
Configuration consistency status: failed
Configuration consistency reason: vPC type-1 configuration incompatible - STP interface
port type inconsistent
vPC role                        : secondary
Number of vPC configured        : 1

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po10   up     1-100

vPC status
----------------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------------------------- ------------
20   Po20   up     failed      vPC type-1 configuration   -
                                incompatible - STP
                                interface port type
                                inconsistent
```

This example shows how to display information about the tracked objects in the vPCs, which is available beginning in Cisco NX-OS Release 4.2(1):

```
switch(config)# show vpc brief

Legend:
                (*) - local vpc is down, forwarding via vPC peer-link
```

```
vPC domain id                     : 1
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
vPC role                          : secondary
Number of vPC configured          : 3
Track object                      : 12


vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po10   up     1-100
```

Related Commands

Command	Description
feature vpc	Enables vPCs on the device.
show port channel summary	Displays information about port channels.

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 port-channel** *channel-number* | **vlan** | **vpc** *number*}

Syntax Description

global	(Optional) Displays the configuration of all Type 1 global parameters on both sides of the vPC peer link.
interface port-channel	(Optional) Displays the configuration of all Type 1 interface parameters on both sides of the vPC peer link.
channel- number	(Optional) Channel number. The range is from 1 to 4096.
vlan	(Optional) Displays the configuration of all Type 1 interface parameters on both sides of the vPC peer link for the specified VLAN.
vpc *number*	(Optional) Displays the configuration of all Type 1 interface parameters on both sides of the vPC peer link for the specified vPC. The range is from 1 to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.1(3)	This command was introduced.
4.2(1)	Added the display of local suspended VLANs. **Note** The command does not display the vPC peer device's suspended VLANs.
4.2(1)	Added the *vpc* argument.
5.2(1)	Added the **vlan** keyword.

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 does 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 the **feature vpc** command for information on enabling vPCs.

This command does not require a license.

Examples

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

```
switch (config)# show vpc consistency-parameters global

Legend:
        Type 1 : vPC will be suspended in case of mismatch

Name            Type Local Value              Peer Value
-------------   ---- ------------------------ -------------------------
STP Mode        1    Rapid-PVST               Rapid-PVST
STP Disabled    1    None                     None
STP MST         1    ""                       ""
Region Name
STP MST         1    0                        0
Region
Revision
```

```
STP MST         1
Region
Instance to
VLAN Mapping
STP Loopguard   1    Disabled                Disabled
STP Bridge      1    Enabled                 Enabled
Assurance
STP Port Type   1    Normal                  Normal
Allowed VLAN    -    1-100                   1-100
Local suspended -    1-50                    -
VLANs
```

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

```
switch (config)# show vpc consistency-parameters interface port-channel 20

Legend:
        Type 1 : vPC will be suspended in case of mismatch

Name            Type Local Value              Peer Value
-------------   ---- ---------------------- -------------------------
STP Port Type   1    Default                  Default
STP Port        1    None                     None
Guard
mode            1    on                       on
Speed           1    10 Gb/s                  10 Gb/s
Duplex          1    full                     full
Port Mode       1    trunk                    trunk
Native Vlan     1    1                        1
MTU             1    1500                     1500
Allowed VLAN    -    1-100                    1-100
bitset
```

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.

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.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.2(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 on enabling vPCs.

This command does not require a license.

Examples

This example shows how to display vPC orphan ports:

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

Note:
--------::Going through port database. Please be patient.::--------

VLAN            Orphan Ports
-------         --------------------------
1               Po600
2               Po600
3               Po600
4               Po600
5               Po600
6               Po600
7               Po600
8               Po600
9               Po600
10              Po600
```

```
11              Po600
12              Po600
13              Po600
14              Po600
15              Po600
```

Related Commands

Command	Description
feature vpc	Enables vPCs on the device.
show vpc brief	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.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.1(3)	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 virtual routing and forwarding (VRF) instance 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 on enabling vPCs.

This command does not require a license.

Examples

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

```
n7k-2(config-vpc-domain)# show vpc peer-keepalive

vPC keep-alive status           : peer is alive
--Send status                   : Success
--Last send at                  : 2008.05.17 18:23:53 986 ms
--Sent on interface             : Eth7/16
--Receive status                : Success
--Last receive at               : 2008.05.17 18:23:54 99 ms
--Received on interface         : Eth7/16
```

```
--Last update from peer         : (0) seconds, (486) msec

vPC Keep-alive parameters
--Destination                   : 172.23.145.213
--Keepalive interval            : 1000 msec
--Keepalive timeout             : 5 seconds
--Keepalive hold timeout        : 3 seconds
--Keepalive vrf                 : pkal
--Keepalive udp port            : 3200
--Keepalive tos                 : 192
```

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

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

The **show vpc role** command displays the following information about the vPC status:

- Status of peer adjacency
- vPC role of the VDC that you are working on
- 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.

This command does not require a license.

Examples

This example shows how to display the vPC role information of the device that you are working on:

```
switch (config)# show vpc role

Primary:

vPC Role status
----------------------------------------------------
vPC role                        : primary
Dual Active Detection Status    : 0
```

```
vPC system-mac                  : 00:23:04:ee:be:01
vPC system-priority             : 32667
vPC local system-mac            : 00:22:55:79:ea:c1
vPC local role-priority         : 32667


Secondary:

vPC Role status
----------------------------------------------------
vPC role                        : secondary
Dual Active Detection Status    : 0
vPC system-mac                  : 00:23:04:ee:be:01
vPC system-priority             : 32667
vPC local system-mac            : 00:22:55:79:de:41
vPC local role-priority         : 32667
```

When you reload the primary vPC peer device, the secondary vPC peer device assumes the role of the primary device. The following example shows how the vPC role displays on the new primary device:

```
switch (config)# show vpc role

vPC Role status
----------------------------------------------------
vPC role                        : secondary, operational primary
Dual Active Detection Status    : 0
vPC system-mac                  : 00:23:04:ee:be:64
vPC system-priority             : 32667
vPC local system-mac            : 00:22:55:79:de:41
vPC local role-priority         : 32667
```

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.

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[

peer-keepalive	Displays statistics about the peer-keepalive message.
peer-link	Displays statistics about the peer link.
vpc *number*	Displays statistics about the specified vPC. The range is from 1 to 4096.

Defaults None

Command Modes Any command mode

SupportedUserRoles network-admin

vdc-admin

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines The **peer-link** parameter displays the same information as the **show interface port-channel** *channel number* command for the vPC peer-link port channel.

The **vpc** *number* parameter displays the same information as the **show interface port-channel** *channel number* command for the specified vPC port channel.

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

This command does not require a license.

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

```
switch# show vpc statistics peer-keepalive

vPC keep-alive status           : peer is alive

VPC keep-alive statistics
--------------------------------------------------
peer-keepalive tx count:          1036
peer-keepalive rx count:          1028
average interval for peer rx:     995
Count of peer state changes:      1
```

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 bring the port administratively down, use the **shutdown** command. To bring the port administratively up, use the **no shutdown** command.

shutdown [**force**]

no shutdown [**force**]

Syntax Description

force	(Optional) Forces the interface state to change. When you shut down a management interface, a warning question is displayed regarding active Telnet sessions. You can bypass the question with the **force** option. The **force** option is also useful when you run an automated configuration playback. The **force** option is only available for Ethernet interfaces or the management port.

Defaults

None

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **shutdown** command to bring the port administratively down. Use the **no shutdown** command to bring the port administratively up.

This command does not require a license.

Examples

This example shows how to bring the port administratively down:

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

This example shows how to bring the port administratively up:

```
switch(config-if)# no shutdown
```

Related Commands

Command	Description
interface ethernet	Configures the types and identities of Ethernet interfaces.

speed

To set the speed for Ethernet ports or management interfaces or set the port to autonegotiate its speed with other ports on the link, use the **speed** command.

speed {**10** | **100** | **1000** | **10000** | **auto** [**10** [**100** [**1000**]]]}

Syntax Description

10	Sets the speed at 10 Mbps.
100	Sets the speed at 100 Mbps.
1000	Sets the speed at 1 Gbps.
10000	Sets the speed at 10 Gbps.
auto	Sets the interface to autonegotiation.

Defaults

None

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Before you begin, make sure that the remote port has a speed setting that supports your changes for the local port. If you want to set the local port to use a specific speed, you must set the remote port for the same speed or set the local port to autonegotiate the speed.

The interface speed and duplex mode are interrelated, so you should configure both of their parameters at the same time.

The interface speed that you specify can affect the duplex mode used for an interface, so you should set the speed before setting the duplex mode. If you set the speed for autonegotiation, the duplex mode is automatically set to be autonegotiated. If you specify 10- or 100-Mbps speed, the port is automatically configured to use half-duplex mode, but you can specify full-duplex mode instead. If you specify a speed of 1000 Mbps (1 Gbps) or faster, full duplex is automatically used. For more details about configuring this command, see the *Cisco NX-OS Interfaces Configuration Guide*.

This command does not require a license.

Examples

This example shows how to set the speed of Ethernet port 1 on the 48-port 10/100/1000 module in slot 3 to 1000 Mbps and full-duplex mode:

```
switch# config t
```

```
switch(config)# interface ethernet 3/1
switch(config-if)# speed 1000
switch(config-if)# duplex full
```

Related Commands

Command	Description
duplex	Specifies the duplex mode as full, half, or autonegotiate.
show interface	Displays the interface status, which includes the speed parameters.

state enabled

To enable the specified port profile, use the **state enabled** command. To return to the default value, use the **no** form of this command.

state enabled

no state enabled

Syntax Description

This command has no keywords or arguments.

Defaults

Disabled

Command Modes

Port-profile configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **state enabled** command to enable the specified port profile. See the **port-profile** command for information about the port-profile feature.

To apply the port-profile configurations to the interfaces, you must enable the specific port profile. You can configure and inherit a port profile onto a range of interfaces prior to enabling the port profile; you would then enable that port profile for the configurations to take effect on the specified interfaces. The maximum number of interfaces that can inherit a single profile is 512.

If you inherit one or more port profiles onto an original port profile, only the last inherited port profile must be enabled; the system assumes that the underlying port profiles are enabled.

This command does not require a license.

Examples

This example shows how to enable the port-profile feature:

```
switch(config)# port-profile type ethernet test
switch(config-ppm)# state enabled
```

Related Commands

Command	Description
show port-profile	Displays information about the port profiles.

switchport

To set the interface as a Layer 2 switching port, use the **switchport** command. To return the interface to the default Layer 3 routed interface status and cause all Layer 2 configuration to be erased, use the **no** form of this command.

switchport

no switchport

Syntax Description

This command has no keywords or arguments.

Defaults

Interfaces are Layer 3 by default.

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	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 additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

The default switchport mode is the access mode. Use the **switchport mode** command to do the following:

- Set the interface to the Layer 2 access mode
- Return the interface to the Layer 2 trunk mode
- Use the interface with private VLANs.

Enter the **no switchport** command to shut down the port and then reenable it. This action may generate messages on the device to which the port is connected.

When you use the **no switchport** command, all the Layer 2 configuration is deleted from that interface, and the interface has the default VLAN configuration.

The port goes down and reinitializes when you change the interface mode.

This command does not require a license.

Examples

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

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

Related Commands

Command	Description
show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport access vlan

To set the access VLAN when the interface is in access mode, use the **switchport access vlan** command. To reset the access-mode VLAN to the appropriate default VLAN for the device, use the **no** form of this command.

switchport access vlan *vlan-id*

no switchport access vlan

Syntax Description

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

Defaults

VLAN1

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	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 access vlan** command. This action is required only if you have not entered the **switchport** command for the interface.

Enter the **no switchport access vlan** command to shut down the port and then reenable it. This action may generate messages on the device to which the port is connected.

Use the **no** form of the **switchport access vlan** command to reset the access-mode VLAN to the appropriate default VLAN for the device.

This command does not require a license.

Examples

This example shows how to cause a port interface that has already been configured as a switched interface to operate as an access port in VLAN 2 instead of the platform's default VLAN in the interface-configuration mode:

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

Related Commands

Command	Description
show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport autostate exclude

To exclude an access port or trunk from the VLAN interface link-up calculation on the Cisco NX-OS device, use the **switchport autostate exclude** command. To revert to the default settings, use the **no** form of this command.

switchport autostate exclude

no switchport autostate exclude

Syntax Description

This command has no keywords or arguments.

Defaults

All ports are included in the VLAN interface link-up calculation.

Command Modes

Interface configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

The **switchport autostate exclude** command marks the port to be excluded from the interface VLAN up calculation when there are multiple ports in the VLAN.

The **show interface** *interface* **switchport** command displays the autostate mode if the mode has been set. If the mode has not been set, the autostate mode is not displayed.

This command does not require a license.

Examples

This example shows how to exclude a port from the VLAN interface link-up calculation on the Cisco NX-OS device:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# switchport
switch(config-if)# switchport autostate exclude
```

This example shows how to include all ports in the VLAN interface link-up calculation on the Cisco NX-OS device:

```
switch(config-if)# no switchport autostate exclude
```

Related Commands

Command	Description
switchport	Configures the interface as a Layer 2 switching port.
show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport dot1q ethertype

To set the EtherType used for Q-in-Q encapsulation on an interface, use the **switchport dot1q ethertype** command. To reset the EtherType to its default value, Use the **no** form of this command.

switchport dot1q ethertype *ethertype*

no switchport dot1q ethertype [*ethertype*]

Syntax Description

ethertype	Value to set for the EtherType. The range is from 0x600 to 0xffff. • 0x8100 is the default EtherType for 802.1q frames • 0x88A8 is the EtherType for 802.1ad double tagged frames • 0x9100 is the EtherType for QinQ frames

Defaults

0x8100 is the default EtherType for 802.1q frames

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must enter the **switchport** command without any keywords to configure the Ethernet interface as a Layer 2 interface before you can enter the **switchport mode** command. This action is required only if you have not entered the **switchport** command for the interface.

You must set the EtherType only on the egress trunk interface that carries double tagged frames (the trunk interface that connects the service providers). If you change the EtherType on one side of the trunk, you must set the same value on the other end of the trunk (symmetrical configuration).

Caution The EtherType value you set affects all the tagged packets going out on the interface (not just Q-in-Q packets).

This command does not require a license.

Examples

This example shows how to create a 802.1Q tunnel on an interface:

```
switch(config-if)# switchport dot1q ethertype 0x9100
```

Related Commands

Command	Description
show interface switchport	Displays information about all the switch port interfaces.

switchport host

To configure a port that is not connected to any other devices as a Layer 2 access port with optimized packet forwarding, use the **switchport host** command. To disable a port that is not connected to any other devices as a Layer 2 access, use the **no** form of this command.

switchport host

no switchport host

Syntax Description

This command has no keywords or arguments.

Defaults

Interfaces are Layer 3 by default.

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	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 host** command. This action is required only if you have not entered the **switchport** command for the interface.

Entering the **switchport host** command on an interface:

- Makes the Layer 2 interface an access port.
- Makes the Layer 2 interface an STP edge port, which decreases the time that it takes to start up packet forwarding.
- Disables port channeling on this interface.

You should enter the **switchport host** command only on ports that are connected to a single host. When you use this command with an interface connected to other than a single host, the device returns an error message.

To optimize the port configuration, entering the **switchport host** command sets the switch port mode to access and disables channel grouping. Only an end station can accept this configuration.

This command toggles the port if it is in the UP state.

This command does not require a license.

Examples

This example shows how to optimize an access port configuration for a host connection:

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

Related Commands

Command	Description
show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport mode

To set the Layer 2 interface type, use the **switchport mode** command. To return the interface to the Layer 2 access mode, use the **no** form of this command.

switchport mode {**access** | **dot1q-tunnel** | **fabricpath** | **fex-fabric** | **private-vlan** {**host** | **promiscuous** | **trunk** [**promiscuous** | **secondary**]}| **trunk**}

no switchport mode

Syntax Description

access	Specifies the interface as a nontrunking, nontagged single-VLAN Layer 2 interface. An access port carries traffic in one VLAN only.
dot1q-tunnel	Creates a 802.1Q tunnel on the interface.
fabricpath	Specifies the port mode as FabricPath.
fex-fabric	Sets the interface type to be an uplink port for a Fabric Extender.
private-vlan	Sets the port mode as a private-VLAN (PVLAN) host.
host	Sets the port mode as the PVLAN host.
promiscuous	(Optional) Sets the port mode as PVLAN promiscuous.
secondary	(Optional) Sets the port mode trunk as isolated.
trunk	Specifies the trunking VLAN interface in Layer 2. A trunk port can carry traffic in one or more VLANs (based on the trunk allowed VLAN list configuration) on the same physical link.

Defaults

access ports

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
5.2(1)	Added the **dot1q-tunnel**, **fabricpath**, **fex-fabric**, **private-vlan**, **host**, **promiscuous**, and **secondary** keywords.
4.0	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 mode** command. This action is required only if you have not entered the **switchport** command for the interface.

If you enter **access** mode, the interface goes into nontrunking mode; if you enter **trunk** mode, the interface goes into trunking mode.

To correctly deliver the traffic on a trunk port with several VLANs, the switch uses the IEEE 802.1Q encapsulation, or tagging, method. If an access port receives a packet with an 802.1Q tag in the header, that port drops the packet without learning its MAC source address.

Note A port can function as either an access port, a trunk port, or a private VLAN port; a port cannot function as all three simultaneously.

The port goes down and reinitializes when you change the interface mode.

This command does not require a license.

Examples

This example shows how to set the interface to trunking mode:

```
switch(config-if)# switchport mode trunk
```

Related Commands

Command	Description
show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport mode dot1q-tunnel

To creates an 802.1Q tunnel on an interface, use the **switchport mode dot1q-tunnel** command. To disable the 802.1Q tunnel on the interface, use the **no** form of this command.

switchport mode dot1q-tunnel

no switchport mode dot1q-tunnel

Syntax Description

This command has no arguments or keywords.

Defaults

No 802.1Q tunnel

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must enter the **switchport** command without any keywords to configure the Ethernet interface as a Layer 2 interface before you can enter the **switchport mode** command. This action is required only if you have not entered the **switchport** command for the interface.

The port goes down and reinitializes (port flap) when the interface mode is changed. BPDU filtering is enabled and the Cisco Discovery Protocol (CDP) is disabled on tunnel interfaces.

This command does not require a license.

Examples

This example shows how to create a 802.1Q tunnel on an interface:

```
switch(config-if)# switchport mode dot1q-tunnel
```

Related Commands

Command	Description
switchport mode fex-fabric	Sets the interface type to be an uplink port for a Fabric Extender.

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

vlan-list	Allowed VLANs that transmit through this interface in tagged format when in trunking mode; the range of valid values is from 1 to 4094.
add	Adds the defined list of VLANs to those currently set instead of replacing the list.
all	Allows all appropriate VLANs to transmit through this interface in tagged format when in trunking mode.
except	Allows all VLANs to transmit through this interface in tagged format when in trunking mode except the specified values.
none	Blocks all VLANs transmitting through this interface in tagged format when in trunking mode.
remove	Removes the defined list of VLANs from those currently set instead of replacing the list.

Defaults

All VLANs

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	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.

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
show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport trunk native vlan

To change the native VLAN ID when the interface is in trunking mode, use the **switchport trunk native vlan** command. To return the native VLAN ID to VLAN 1, use the **no** form of this command.

switchport trunk native vlan *vlan-id*

no switchport trunk native vlan

Syntax Description

vlan-id	Native VLAN for the trunk in 802.1Q trunking mode. The range is from 1 to 4094, except the internally reserved VLANs are 3968 to 4047 and 4094.

Defaults

VLAN1

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	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 native vlan** command. This action is required only if you have not entered the **switchport** command for the interface.

Note See the **vlandot1q tag native** command for more information about configuring the native VLAN for 802,1Q trunk ports.

Use the **no** form of the **native vlan** command to reset the native mode VLAN to the default VLAN1 for the device.

This command does not require a license.

Examples

This example shows how to configure the native VLAN for an interface in trunk mode:

```
switch(config-if)# switchport trunk native vlan 5
```

Related Commands

Command	Description
show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

system default switchport

To change the default interface mode for the system from Layer 3 routing to Layer 2 switching, use the **system default switchport** command. To return the system to Layer 3 routing default interface mode, use the **no** form of this command.

system default switchport [**fabricpath | shutdown**]

no system default switchport [**fabricpath | shutdown**]

Syntax Description

fabricpath	(Optional) Configures the default port mode as FabricPath.
shutdown	(Optional) Configures the administrative state as down.

Defaults

None

Command Modes

Global configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
5.2(1)	Added the **fabricpath** keyword.
4.0	This command was introduced.

Usage Guidelines

The **system default switchport** command makes all the interfaces Layer 2 access ports.

This command does not require a license.

Examples

This example shows how to configure the system so that all the interfaces are in Layer 2 access mode:

```
switch(config-if)# system default switchport
```

Related Commands

Command	Description
show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

system default interface congestion mode

To configure the default interface congestion mode, use the **system default interface congestion mode** command. To disable this feature, use the **no** form of this command.

system default interface congestion mode {**core** | **edge**}

no system default interface congestion mode {**core** | **edge**}

Syntax Description

core	Specifies the core port type.
edge	Specifies the edge port type.

Defaults

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.1(1)	This command was introduced.

Usage Guidelines

None

Examples

This example shows how to configure the default interface congestion mode for the core port type:

```
switch# config terminal
switch(config)# system default interface congestion mode core
switch(config)#
```

This example shows how to disable the default interface congestion mode for the edge port type:

```
switch# config terminal
switch(config)# no system default interface congestion mode edge
switch(config)#
```

Related Commands

Command	Description
show system default switchport	Displays default values for switch port attributes.
show interface brief	Displays FC port modes.

system default interface congestion timeout

To configure the default value for a congestion timeout, use the **system default interface congestion timeout** command. To disable this feature, use the **no** form of this command.

system default interface congestion timeout *milliseconds* **mode** {**core | edge**}

no system default interface congestion timeout *milliseconds* **mode** {**core | edge**}

Syntax Description

milliseconds	Number of milliseconds. The range is from 100 to 1000 milliseconds.
mode	Specifies the mode.
core	Specifies the core port type.
	Specifies the edge port type.

Defaults

500 milliseconds

Command Modes

Global configuration mode

Command History

Release	Modification
6.1(1)	This command was introduced.

Usage Guidelines

Setting a smaller timeout on the edge ports such as 100 or 200 milliseconds helps to reduce the congestion on the edge port by making the packets on that port timeout sooner when they see the pause condition.

Note You should use the default configuration for core ports and a value that does not exceed 500 ms (100 to 200 ms preferable) for fabric edge ports.

Examples

This example shows how to configure the default value for a congestion timeout for the core type:

```
switch# config terminal
switch(config)# system default interface congestion timeout 100 mode core
switch(config)#
```

This example shows how to disable the default value for a congestion timeout for the edge type:

```
switch# config terminal
switch(config)# no system default interface congestion timeout 100 mode edge
switch(config)#
```

Related Commands

Command	Description
show system default switchport	Displays default values for switch port attributes.
show interface brief	Displays FC port modes.

system default interface pause timeout

To configure the default timeout value for a pause frame, use the **system default interface pause timeout** command. To disable this feature, use the **no** form of this command.

system default interface pause timeout *milliseconds* **mode** {**core** | **edge**}

no system default interface pause timeout *milliseconds* **mode** {**core** | **edge**}

Syntax Description

milliseconds	Number of milliseconds. The range is from 100 to 500 milliseconds.
mode	Specifies the mode.
core	Specifies the port type.
edge	Specifies the edge port type.

Defaults

500 milliseconds

Command Modes

Global configuration mode

Command History

Release	Modification
6.1(1)	This command was introduced.

Usage Guidelines

When the port is in the PAUSE state for the configured period, pause frame timeout can be enabled on that port, which results in all frames that come to that port getting dropped in the egress. This action frees up the buffer space in the ISL link (which carries traffic for this port) and helps to reduce congestion on other unrelated flows, use the same link.

Examples

This example shows how to configure the timeout value pause frame for the core port type:

```
switch# config terminal
switch(config)# system default interface pause timeout 100 mode core
switch(config)#
```

This example shows how to disable the timeout value pause for the edge port type:

```
switch# config terminal
switch(config)# no system default interface pause timeout 100 mode edge
switch(config)#
```

Related Commands

Command	Description
show system default switchport	Displays default values for switch port attributes.
show interface brief	Displays FC port modes.

system default interface pause mode

To configure the default timeout value for a pause frame, use the **system default interface pause mode** command. To disable this feature, use the **no** form of this command.

system default interface pause mode {**core** | **edge**}

no system default interface pause mode {**core** | **edge**}

Syntax Description

core	Specifies the core port type.
edge	Specifies the edge port type.

Defaults

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.1(1)	This command was introduced.

Usage Guidelines

None

Examples

This example shows how to configure the default timeout value for a pause frame for the core port type:

```
switch# config terminal
switch(config)# system default interface pause mode core
switch(config)#
```

This example shows how to disable the timeout default value for a pause frame for the edge port type:

```
switch# config terminal
switch(config)# no system default interface pause mode edge
switch(config)#
```

Related Commands

Command	Description
show system default switchport	Displays default values for switch port attributes.
show interface brief	Displays FC port modes.

system jumbomtu

To configure the system jumbo maximum transmission unit (MTU) size for Layer 2 interfaces, use the **system jumbomtu** command.

system jumbomtu *size*

Syntax Description

size	Even number between 1500 and 9216.

Defaults

The system jumbo MTU default size is 9216 bytes and the interface default MTU is 1500 bytes.

Command Modes

Global configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **system jumbomtu** command to specify the MTU size for Layer 2 interfaces. The range is from 1500 to 9216.

The physical level uses an unchangeable bandwidth of 1 GB.

This command does not require a license.

Examples

This example shows how to configure the system jumbo MTU as 8000 bytes and how to change the MTU specification for an interface that was configured with the previous jumbo MTU size:

```
switch# config t
switch(config)# system jumbomtu 8000
switch(config)# show running-config
switch(config)# interface ethernet 2/2
switch(config-if)# switchport
switch(config-if)# mtu 4608
```

Related Commands

Command	Description
show running-config	Displays the current operating configuration, which includes the system jumbo MTU size.

system-mac

To overwrite the MAC address that the device creates for the virtual port-channel (vPC) domain when you create a vPC domain, use the **system-mac** command. To return to the default vPC system MAC address, use the **no** form of this command.

system-mac *mac-address*

no system-mac

Syntax Description[

mac-address	MAC address that you want for the vPC domain using the format xxxx.xxxx.xxxx.

Defaults None

Defaults vpc-domain command mode

SupportedUserRoles network-admin

vdc-admin

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines You must enable the vPC feature before you can create a vPC system MAC address.

Use the **system-mac** command to overwrite the MAC address created by the system once you create a vPC domain. By default, the system creates a MAC address for the vPC when you create a vPC domain based on the domain ID. Cisco reserved a range of MAC addresses from the IEEE for this purpose and these addresses are used to complete the last 10 bits of the vPC domain MAC address. The range of default MAC addresses is as follows:

- Number of reserved MAC addresses—1024
- Starting—002304eebe00
- Ending—002304eec1ff

This command does not require a license.

Examples This example shows how to create a vPC system MAC address:

```
switch# config t
switch(config)# vpc domain 5
switch(config-vpc-domain)# system-mac 22cd.34ab.ca32
```

Related Commands

Command	Description
show vpc role	Displays the system MAC address for the vPC domain.

system module-type

To control which type of modules are allowed in this chassis, use the **system module-type** command. To return to the default settings, use the **no** form of this command.

system module-type *module-type*

no system module-type *module-type*

Syntax Description[

module-type	f1—Enables f1 type modules in the chassis.
	f2—Enables f2 type modules in the chassis.
	m1—Enables m1 type modules in the chassis.
	m1x1—Enables m1x1 type modules in the chassis.
	m2x1—Enables m2x2 type modules in the chassis.

Defaults None

Command Modes Global configuration mode.

SupportedUserRoles network-admin
vdc-admin

Command History

Release	Modification
6.1(3)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to control the type of modules that are allowed in this chassis:

```
switch# config t
switch(config)# system module-type f1 m1xl f2 m2xl fc f2e
Modules of unsupported types will not be allowed to power on after this. Continue(y/n)?
[yes]
switch(config)#
```

Related Commands

Command	Description
show vpc role	Displays the system MAC address for the vPC domain.

system-priority

To overwrite the system priority that the device creates for the virtual port-channel (vPC) domain when you create a vPC domain, use the **system-priority** command. To return to the default vPC system priority, use the **no** form of this command.

system-priority *priority*

no system-priority *priority*

Syntax Description[

priority	System priority. The range is from 1 to 65535.

Defaults

32667

Command Modes

vpc-domain command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

You must enable the vPC feature before you can create a vPC system priority.

Note We recommend that you manually configure the vPC system priority when you are running LACP to ensure that the vPC peer devices are the primary devices on LACP.

This command does not require a license.

Examples

This example shows how to create a vPC system priority:

```
switch# config t
switch(config)# vpc domain 5
switch(config-vpc-domain)# system-priority 4000
```

Related Commands

Command	Description
show vpc role	Displays the system priority for the vPC domain.

track

To configure the system to monitor the track-list object that contains all the virtual port-channel (vPC) links to the core and to the vPC peer link when you are using only a single module for all links, use the **track** command. To return to the default, use the **no** form of this command.

track *track-object-id*

no track *track-object-id*

Syntax Description

track-object-id	Track-list object that you already configured.

Defaults

No tracking

Command Modes

vpc configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Beginning with Release 4.2, if you must configure all the vPC peer links and core-facing interfaces on a single N7K-M132XP-12 module, you should configure a track object and a track list that is associated with the Layer 3 link to the core and on all vPC peer links on both vPC peer devices. You can use this configuration to avoid dropping traffic if that particular module goes down because when all the tracked objects on the track list go down, the system does the following:

- Stops the vPC primary peer device sending peer-keepalive messages, which forces the vPC secondary peer device to take over.
- Brings down all the downstream vPCs on that vPC peer device, which forces all the traffic to be rerouted in the access switch to the other vPC peer device.

Once you configure this feature and if the module fails, the system automatically suspends all the vPC links on the primary vPC peer device and stops the peer-keepalive messages. This action forces the vPC secondary device to take over the primary role and all the vPC traffic to go to this new vPC primary device until the system stabilizes.

Create a track list that contains all the links to the core and all the vPC peer links as its object. Enable tracking for the specified vPC domain for this track list. Apply this same configuration to the other PC peer device.

This command does not require a license.

Examples

This example shows how to put the previously configured track-list object into the vPC domain on the vPC peer device:

```
switch# config t
switch(config)# vpc domain 5
switch(config-vpc-domain)# track object 5
```

Related Commands

Command	Description
show vpc brief	Displays information about a vPC tracked object.
feature vpc	Enables vPCs on the device.

tunnel destination

To configure the destination endpoint for a tunnel, use the **tunnel destination** command. To remove the tunnel destination, use the **no** form of this command.

tunnel destination {*ip-address* | *host-name*}

no tunnel destination {*ip-address* | *host-name*}

Syntax Description

ip-address	IP address for the tunnel destination.
host-name	Hostname for the tunnel destination.

Defaults

None

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **tunnel destinatio**n command to configure the destination address for an IP tunnel.

You should not have two tunnels using the same encapsulation mode with the same source and destination address.

This command requires the Enterprise license.

Examples

This example shows how to configure the tunnel destination:

```
switch(config-if)# tunnel destination 192.0.2.120
```

Related Commands

Command	Description
tunnel source	Sets the source of the IP tunnel.
interface tunnel	Creates the IP tunnel.
show interface tunnel	Displays information about the traffic about the specified tunnel interface.

tunnel mode

To configure the tunnel encapsulation mode for a tunnel, use the **tunnel mode** command. To restore the default value, use the **no** form of this command.

tunnel mode gre {**ip** | **ipv6**}

no tunnel mode gre {**ip** | **ipv6**}

Syntax Description

ip	Configures this tunnel encapsulation mode as IPv4.
ip v6	Configures this tunnel encapsulation mode as IPv6.

Defaults

None

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **tunnel mode** command to configure the tunnel encapsulation mode for a tunnel.

This command requires the Enterprise license.

Examples

This example shows how to configure the tunnel mode:

```
switch(config-if)# tunnel mode gre ip
```

Related Commands

Command	Description
tunnel destination	Sets the destination of the IP tunnel.
interface tunnel	Creates the IP tunnel.
show interface tunnel	Displays information about the traffic about the specified tunnel interface.

tunnel path-mtu-discovery

To enable Path MTU Discovery (PMTUD) on a tunnel interface, use the **tunnel path-mtu-discovery** command. To disable PMTUD on a tunnel interface, use the **no** form of this command.

tunnel path-mtu-discovery [**age-timer** {*aging-mins* | **infinite**} | **min-mtu** *mtu-bytes*]

no tunnel path-mtu-discovery [**age-timer** {*aging-mins* | **infinite**} | **min-mtu** *mtu-bytes*]

Syntax Description

age-timer	(Optional) Sets a timer to run for a specified interval, in minutes, after which the tunnel interface resets the maximum transmission unit (MTU) of the path to the default tunnel MTU minus 24 bytes for GRE tunnels or minus 20 bytes for IP-in-IP tunnels.
aging-mins	Number of minutes. The range is from 10 to 30. The default is 10.
infinite	Disables the age timer.
min-mtu *mtu-bytes*	(Optional) Specifies the minimum Path MTU across GRE tunnels. The range is from 92 to 65535 bytes. The default is 92.

Defaults

Disabled

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

When PMTUD (RFC 1191) is enabled on a tunnel interface, the router performs PMTUD processing for the tunnel IP packets. The router always performs PMTUD processing on the original data IP packets that enter the tunnel. When PMTUD is enabled, no packet fragmentation occurs on the encapsulated packets that travel through the tunnel. Without packet fragmentation, there is a better throughput of TCP connections. PMTUD maximizes the use of available bandwidth in the network between the endpoints of a tunnel interface.

After PMTUD is enabled, the Don't Fragment (DF) bit of the IP packet header that is forwarded into the tunnel is copied to the IP header of the external IP packets. The external IP packet is the encapsulating IP packet. Adding the DF bit allows the PMTUD mechanism to work on the tunnel path of the tunnel. The tunnel endpoint listens for Internet Control Message Protocol (ICMP) unreachable too-big messages and modifies the IP MTU of the tunnel interface, if required.

When the aging timer is configured, the tunnel code resets the tunnel MTU after the aging timer expires. After the tunnel MTU is reset, a set of full-size packets with the DF bit set is required to trigger the tunnel PMTUD and lower the tunnel MTU. At least two packets are dropped each time that the tunnel MTU changes.

When PMTUD is disabled, the DF bit of an external (encapsulated) IP packet is set to zero even if the encapsulated packet has a DF bit set to one.

The **min-mtu** keyword sets a low limit through the MTU that can be learned through the PMTUD process. Any ICMP signal received that specifies an MTU less than the minimum MTU configured is ignored. You can use this feature to prevent a denial- of-service attack from any node that can send an ICMP message to the router that specifies a very small MTU.

Note PMTUD on a tunnel interface requires that the tunnel endpoint is able to receive ICMP messages generated by routers in the path of the tunnel. You should check that ICMP messages can be received before you use PMTUD over firewall connections.

This command requires the Enterprise license.

Examples

This example shows how to configure PMTUD:

```
switch(config-if)# tunnel path-mtu-discovery
```

Related Commands

Command	Description
tunnel destination	Sets the destination of the IP tunnel.
interface tunnel	Creates the IP tunnel.
show interface tunnel	Displays information about the traffic about the specified tunnel interface.

tunnel source

To configure the source endpoint for a tunnel, use the **tunnel source** command. To remove the tunnel source, use the **no** form of this command.

tunnel source {*ip-address* | *interface-type number*}

no tunnel source [*ip-address* | *interface-type number*]

Syntax Description

ip-address	IP address for the tunnel source.
interface-type number	Interface for the tunnel source.

Defaults

None

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **tunnel source** command to configure the source address for an IP tunnel.

You should not have two tunnels using the same encapsulation mode with the same source and destination address.

This command requires the Enterprise license.

Examples

This example shows how to set the tunnel source:

```
switch(config-if)# tunnel source 192.0.2.120
```

Related Commands

Command	Description
tunnel destination	Sets the destination of the IP tunnel.
interface tunnel	Creates the IP tunnel.
show interface tunnel	Displays information about the traffic about the specified tunnel interface.

tunnel use-vrf

To specify which virtual routing and forwarding (VRF) instance to use to look up a tunnel destination IP address, use the **tunnel use-vrf** command. To return to the default, use the **no** form of this command.

tunnel use-vrf *vrf-name*

no tunnel use-vrf *vrf-name*

Syntax Description

vrf-name	Name of the VRF in which to look up the tunnel destination IP address.

Defaults

Default VRF

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

You should have the tunnel interface and tunnel destination IP address in the same VRF. You should have the same value for the *vrf-name* parameter in both the **vrf member** and **tunnel use-vrf** command.

This command requires the Enterprise license.

Examples

This example shows how to specify the VRF in which to look up the tunnel destination IP address:

```
switch(config-if)# tunnel use-vrf blue
```

Related Commands

Command	Description
show interface tunnel	Displays information about the traffic about the specified tunnel interface.
show vrf interface tunnel	Displays information about the VRF tunnel interface.

tunnel ttl

To configure the time-to-live value for a tunnel, use the **tunnel ttl** command. To restore the default value, use the **no** form of this command.

tunnel ttl *value*

no tunnel ttl [*value*]

Syntax Description

value	Time-to-live value for the tunnel. The range is from 1 to 255.

Defaults

None

Command Modes

Interface configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **tunnel ttl** command to configure the time-to-live value for an IP tunnel.

This command requires the Enterprise license.

Examples

This example shows how to configure the time-to-live value for a tunnel interface:

```
switch(config-if)# tunnel ttl 30
```

Related Commands

Command	Description
tunnel destination	Sets the destination of the IP tunnel.
interface tunnel	Creates the IP tunnel.
show interface tunnel	Displays information about the traffic about the specified tunnel interface.

udld

To configure the interfaces to use a Unidirectional Link Detection (UDLD) mode, use the **udld** command.

udld {**enable** | **disable**}

Syntax Description

disable	Disables the UDLD mode for fiber interfaces.
enable	Enables the normal UDLD mode for nonfiber interfaces.

Defaults

By default, UDLD is disabled for the 48-port, 10/100/1000-Ethernet module ports.

By default, UDLD is enabled for the 32-port, 10-Gigabit Ethernet module ports.

Command Modes

Interface configuration mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Before you can enable a UDLD mode for specified interfaces, you must make sure that UDLD is already enabled globally on the device. Use the **feature udld** command to enable UDLD globally.

Use the **udld** command to enable or disable UDLD separately on specified interfaces. This action enables UDLD in normal mode. Enter the **udld aggressive** command to enable the aggressive mode on UDLD-enabled interfaces.

This command does not require a license.

Examples

This example shows how to enable the normal UDLD mode for Ethernet port 3/1:

```
switch# config t
switch(config)# feature udld
switch(config)# interface ethernet 3/1
switch(config-if)# udld enable
```

This example shows how to disable UDLD for Ethernet port 3/1:

```
switch# config t
switch(config)# interface ethernet 3/1
switch(config-if-range)# udld disable
```

Related commands

Command	Description
feature udld	Enables UDLD globally on the device.
show udld	Displays information about the UDLD configuration.

udld aggressive

To configure the interfaces for aggressive Unidirectional Link Detection (UDLD) mode, use the **udld aggressive** command.

udld aggressive

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Interface configuration mode

Global configuration mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Before you can enable the aggressive UDLD mode for an interface, you must make sure that UDLD is already enabled globally on the device and on the specified interfaces.

Use the **udld aggressive** command to configure the ports to use a UDLD mode:

- To enable fiber interfaces for the aggressive mode, enter the **udld aggressive** command in the global command mode and all the fiber interfaces will be in aggressive UDLD mode,
- To enable the copper interfaces for the aggressive, you must enter the **udld aggressive** command in the interface mode, specifying each interface you want in aggressive UDLD mode.

To use the aggressive UDLD mode, you must configure the interfaces on both ends of the link for the aggressive UDLD mode.

This command does not require a license.

Examples

This example shows how to enable fiber interfaces for the aggressive UDLD mode:

```
switch# config t
switch(config)# udld aggressive
```

This example shows how to enable the aggressive UDLD mode for the copper Ethernet interface 3/1:

```
switch# config t
switch(config)# interface ethernet 3/1
switch(config-if)# udld aggressive
```

Related Commands

Command	Description
feature udld	Enables UDLD globally for the device.
show udld	Displays information about the UDLD configuration.

udld message-time

To set the Unidirectional Link Detection (UDLD) message interval timer, use the **udld message-time** command.

udld message-time *seconds*

Syntax Description

seconds	Number of seconds that you want between sending UDLD messages. The range is from 7 to 90 seconds.

Defaults

15 seconds

Command Modes

Global configuration mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Before you can set the UDLD message timer, you must make sure that UDLD is already enabled globally on the device. Use the **feature udld** command to globally enable UDLD.

This command does not require a license.

Examples

This example shows how to configure UDLD interval to 30 seconds:

```
switch# config t
switch(config)# udld message-time 30
```

Related Commands

Command	Description
feature udld	Enables UDLD globally for the device.
show udld	Displays information about the UDLD configuration.

udld reset

To reset the interfaces that Unidirectional Link Detection (UDLD) has shut down and return them to the UP condition, use the **udld reset** command.

udld reset

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to reset those interfaces that UDLD has shut down:

```
switch# config t
switch(config)# udld reset
```

Related Commands

Command	Description
feature udld	Enables UDLD globally for the device.
show udld	Displays information about the UDLD configuration.

vlan dot1q tag native

To enable dot1q (IEEE 802.1Q) tagging for the native VLAN in a trunk, use the **vlan dot1q tag native** command. To return to the default where no packets are tagged in the native VLAN in a trunk, use the **no** form of this command.

vlan dot1q tag native

no vlan dot1q tag native

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Typically, you configure 802.1Q trunks with a native VLAN ID, which strips tagging from all packets on that VLAN and allows all untagged traffic and control traffic to transit the switch. Packets that enter the switch with 802.1Q tags that match the native VLAN ID value are similarly stripped of tagging. If you choose to maintain the tagging on the native VLAN and drop untagged traffic, enter the **vlan dot1q tag native** command.

Use the **vlan dot1q tag native** command to configure the switch to tag the traffic received on the native VLAN and to admit only the 802.1Q-tagged frame, dropping any untagged traffic, including untagged traffic in the native VLAN. Control traffic continues to be accepted untagged on the native VLAN on a trunked port, even when the **vlan dot1q tag native** command is enabled.

Use this command to enable the tagging behavior on all native VLANs on all trunked ports on the switch.

Note If you enable 802.1Q tagging on one switch and disable it on another switch, all traffic is dropped; you must identically configure 802.1Q tagging on each switch.

This command does not require a license.

Examples

This example shows how to enable dot1q tagging for all VLANs on all trunk ports on the switch:

```
switch(config)# vlan dot1q tag native
```

Related Commands

Command	Description
show vlan dot1q tag native	Displays native VLAN-tagging information.

vpc

To move other port channels into the virtual port channel (vPC), use the **vpc** command. To remove a port channel from the vPC, use the **no** form of this command.

vpc *number*

no vpc *number*

Syntax Description

number	Number for the vPC. The range is from 1 to 4096.

Defaults

None

Command Modes

Interface command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

You must enable the vPC feature before you can create a vPC.

Once you have created the vPC domain ID and the vPC peer link, you create port channels to attach the downstream device to each vPC peer device. That is, you create one 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.

Note The vPC number that you assign to the port channel connecting to the downstream device from the vPC peer device must be identical on both vPC peer devices.

This command does not require a license.

Examples

This example shows how to move a port channel into the vPC:

```
switch# config t
switch (config)# interface port-channel 10
switch (config-if)# vpc 100
```

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.

vpc domain

To create a virtual port-channel (vPC) domain, use the **vpc domain** command. To remove a vPC domain, use the **no** form of this command.

vpc domain *domain-id*

no vpc domain *domain-id*

Syntax Description

domain-id	Domain ID for the vPC. The range of numbers is from 1 to 1000. You must use unique vPC IDs for each vPC within a single virtual device context (VDC).

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

You must enable the vPC feature before you can create a vPC domain.

You put all vPC interfaces, including the vPC peer link, on both of the vPC peer devices into the identical vPC domain. You must have unique vPC domain numbers within each VDC. In Cisco NX-OS Release 4.1(3), you can have only one vPC per VDC. Once you create a vPC domain, the system automatically creates a vPC system MAC address that is unique to that vPC.

You also use this command to enter the vpc-domain command mode in order to configure vPC parameters.

This command does not require a license.

Examples

This example shows how to create a vPC domain:

```
switch# config t
switch(config)# vpc domain 5
switch(config-vpc-domain)#
```

This example shows how to enter the vpc-domain command mode to configure an existing vPC domain:

```
switch# config t
switch(config)# vpc domain 5
```

```
switch(config-vpc-domain)#
```

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.

vpc orphan-ports suspend

To shut down the virtual port channel (vPC) port when the peer link is down, use the **vpc orphan-ports suspend** command. To revert to default settings, use the **no** form of this command.

vpc orphan-ports suspend

no vpc orphan-ports suspend

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration mode (config-if)

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

You can use the **vpc orphan-ports suspend** command only on physical ports.

Note You can configure vPC orphan port suspension only on physical ports, not on port channel member ports.

This command does not require a license.

Examples

This example shows how to shut down the vPC port when the peer link is down:

```
switch# configure terminal
switch(config)# interface ethernet 5/2
switch(config-if)# vpc orphan-ports suspend
switch(config-if)#
```

Related Commands

Command	Description
vpc domain	Creates a vPC domain.

vpc peer-link

To create a virtual port-channel (vPC) peer link, use the **vpc peer-link** command. To remove a vPC 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.

Defaults

None

Command Modes

Interface command mode

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

You must enable the vPC feature before you can create a vPC peer link.

You configure a port channel using 10-Gigabit Ethernet ports on the N7K-M132XP-12 module. We recommend that you use the 10-Gigabit Ethernet ports for the channel in dedicated mode and configure at least two of these ports on two different modules into the port channel for redundancy.

Use the **vpc peer-link** command to make that port channel a vPC peer link. The system returns an error message if you attempt to configure a 1-Gigabit Ethernet interface as a vPC peer link.

After you configure the vPC peer device and the vPC peer link is established, the system creates a new MAC address for the vPC and decides which vPC device is the primary device and which is the secondary device.

This command does not require a license.

Examples

This example shows how to create a vPC peer link:

```
switch# config t
switch(config)# interface port-channel 20
switch(config-if)# vpc peer-link
switch(config-vpc-domain)#
```

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.