



Layer 2/3 Commands

- [channel-group](#), on page 2
- [channel-protocol](#), on page 5
- [clear lacp](#), on page 6
- [clear pagp](#), on page 6
- [clear spanning-tree counters](#), on page 7
- [clear spanning-tree detected-protocols](#), on page 8
- [debug etherchannel](#), on page 8
- [debug lacp](#), on page 9
- [debug pagp](#), on page 10
- [debug platform pm](#), on page 11
- [debug platform uddl](#), on page 12
- [debug spanning-tree](#) , on page 13
- [interface port-channel](#), on page 14
- [lacp max-bundle](#), on page 15
- [lacp port-priority](#), on page 16
- [lacp rate](#), on page 17
- [lacp system-priority](#), on page 18
- [pagp learn-method](#), on page 19
- [pagp port-priority](#), on page 20
- [port-channel](#), on page 21
- [port-channel auto](#), on page 21
- [port-channel load-balance](#), on page 22
- [port-channel load-balance extended](#), on page 23
- [port-channel min-links](#), on page 24
- [rep admin vlan](#), on page 25
- [rep block port](#), on page 25
- [rep lsl-age-timer](#), on page 27
- [rep lsl-retries](#), on page 27
- [rep preempt delay](#), on page 28
- [rep preempt segment](#), on page 29
- [rep segment](#), on page 29
- [rep stcn](#), on page 31
- [show etherchannel](#), on page 31

- [show interfaces rep detail](#), on page 34
- [show lacp](#), on page 35
- [show pagp](#), on page 39
- [show platform software fed etherchannel](#), on page 40
- [show platform pm](#), on page 41
- [show rep topology](#), on page 42
- [show uddl](#), on page 43
- [switchport](#), on page 46
- [switchport access vlan](#), on page 47
- [switchport mode](#), on page 49
- [switchport nonegotiate](#), on page 51
- [switchport voice vlan](#), on page 52
- [uddl](#), on page 55
- [uddl port](#), on page 56
- [uddl reset](#), on page 57

channel-group

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

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

Syntax Description

| | |
|-----------------------------|--|
| auto | Enables auto-LAG feature on individual port interface. By default, the auto-LAG feature is enabled on the port. |
| <i>channel-group-number</i> | Channel group number. The range is 1 to 128. |
| mode | Specifies the EtherChannel mode. |
| active | Unconditionally enables Link Aggregation Control Protocol (LACP). |
| auto | Enables the Port Aggregation Protocol (PAgP) only if a PAgP device is detected. |

| | |
|-------------------|---|
| non-silent | (Optional) Configures the interface for nonsilent operation when connected to a partner that is PAgP-capable. Use in PAgP mode with the auto or desirable keyword when traffic is expected from the other device. |
| desirable | Unconditionally enables PAgP. |
| on | Enables the on mode. |
| passive | Enables LACP only if a LACP device is detected. |

Command Default
No channel groups are assigned.
No mode is configured.

Command Modes
Interface configuration

| Command History | Release | Modification |
|------------------------|--------------------|------------------------------|
| | Cisco IOS XE 3.2SE | This command was introduced. |

Usage Guidelines
For Layer 2 EtherChannels, the **channel-group** command automatically creates the port-channel interface when the channel group gets its first physical port. You do not have to use the **interface port-channel** command in global configuration mode to manually create a port-channel interface. If you create the port-channel interface first, the *channel-group-number* can be the same as the *port-channel-number*, or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.

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

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

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

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

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

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



Caution

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

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

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

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

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

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

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



Caution

Do not assign bridge groups on the physical EtherChannel ports because it creates loops.

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

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

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

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

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

```
Device# configure terminal
Device(config)# interface range GigabitEthernet 2/0/4 - 5
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
```

```

Device(config-if-range)# channel-group 5 mode passive
Device(config-if-range)# exit
Device(config)# interface GigabitEthernet 3/0/3
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 10
Device(config-if)# channel-group 5 mode passive
Device(config-if)# exit

```

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

channel-protocol

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

```

channel-protocol {lACP | PAGP}
no channel-protocol

```

Syntax Description

lACP Configures an EtherChannel with the Link Aggregation Control Protocol (LACP).

PAGP Configures an EtherChannel with the Port Aggregation Protocol (PAGP).

Command Default

No protocol is assigned to the EtherChannel.

Command Modes

Interface configuration

Command History

| Release | Modification |
|--------------------|------------------------------|
| Cisco IOS XE 3.2SE | This command was introduced. |

Usage Guidelines

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

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

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

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

You cannot configure PAGP on cross-stack configurations.

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

```
Device(config-if)# channel-protocol lACP
```

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

clear lacp

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

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

| | |
|---------------------------|---|
| Syntax Description | <i>channel-group-number</i> (Optional) Channel group number. The range is 1 to 128. |
| | counters Clears traffic counters. |

Command Default None

Command Modes Privileged EXEC

| Command History | Release | Modification |
|------------------------|--------------------|------------------------------|
| | Cisco IOS XE 3.2SE | This command was introduced. |

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

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

```
Device# clear lacp counters
```

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

```
Device# clear lacp 4 counters
```

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

clear pagp

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

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

| | |
|---------------------------|---|
| Syntax Description | <i>channel-group-number</i> (Optional) Channel group number. The range is 1 to 128. |
| | counters Clears traffic counters. |

Command Default None

| | | |
|-------------------------|--|------------------------------|
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE 3.2SE | This command was introduced. |
| Usage Guidelines | <p>You can clear all counters by using the clear pagp counters command, or you can clear only the counters for the specified channel group by using the clear pagp channel-group-number counters command.</p> <p>This example shows how to clear all channel-group information:</p> <pre>Device# clear pagp counters</pre> <p>This example shows how to clear PAgP traffic counters for group 10:</p> <pre>Device# clear pagp 10 counters</pre> <p>You can verify that the information was deleted by entering the show pagp privileged EXEC command.</p> | |

clear spanning-tree counters

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

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

| | | |
|---------------------------|--|--|
| Syntax Description | interface <i>interface-id</i> | (Optional) Clears all spanning-tree counters on the specified interface. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 128. |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE 3.2SE | This command was introduced. |
| Usage Guidelines | <p>If the <i>interface-id</i> value is not specified, spanning-tree counters are cleared for all interfaces.</p> <p>This example shows how to clear spanning-tree counters for all interfaces:</p> <pre>Device# clear spanning-tree counters</pre> | |

clear spanning-tree detected-protocols

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

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

| | | |
|---------------------------|--------------------------------------|--|
| Syntax Description | interface <i>interface-id</i> | (Optional) Restarts the protocol migration process on the specified interface. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 128. |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE 3.2SE | This command was introduced. |

Usage Guidelines

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

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

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

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

debug etherchannel

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

```
debug etherchannel [{all | detail | error | event | idb}]  
no debug etherchannel [{all | detail | error | event | idb}]
```


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

Command Default Debugging is disabled.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|------------------------|--------------------|------------------------------|
| | Cisco IOS XE 3.2SE | This command was introduced. |

Usage Guidelines The **undebg etherchannel** command is the same as the **no debug etherchannel** command.



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

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

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

This example shows how to display all EtherChannel debug messages:

```
Device# debug etherchannel all
```

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

```
Device# debug etherchannel event
```

debug lacp

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

```
debug lacp [{all | event | fsm | misc | packet}]
no debug lacp [{all | event | fsm | misc | packet}]
```

| | | |
|---------------------------|--------------|--|
| Syntax Description | all | (Optional) Displays all LACP debug messages. |
| | event | (Optional) Displays LACP event debug messages. |

fsm (Optional) Displays messages about changes within the LACP finite state machine.

misc (Optional) Displays miscellaneous LACP debug messages.

packet (Optional) Displays the receiving and transmitting LACP control packets.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------|------------------------------|
| | Cisco IOS XE 3.2SE | This command was introduced. |

Usage Guidelines The **undebg etherchannel** command is the same as the **no debug etherchannel** command.

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

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

This example shows how to display all LACP debug messages:

```
Device# debug LACP all
```

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

```
Device# debug LACP event
```

debug pagp

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

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

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

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

Command Default Debugging is disabled.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------|------------------------------|
| | Cisco IOS XE 3.2SE | This command was introduced. |

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

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

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

This example shows how to display all PAgP debug messages:

```
Device# debug pagp all
```

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

```
Device# debug pagp event
```

debug platform pm

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

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

| Syntax Description | | |
|--------------------|--|---|
| all | | Displays all port manager debug messages. |
| counters | | Displays counters for remote procedure call (RPC) debug messages. |
| errdisable | | Displays error-disabled-related events debug messages. |
| fec | | Displays forwarding equivalence class (FEC) platform-related events debug messages. |
| if-numbers | | Displays interface-number translation event debug messages. |
| l2-control | | Displays Layer 2 control infra debug messages. |
| link-status | | Displays interface link-detection event debug messages. |
| platform | | Displays port manager function event debug messages. |

| | |
|-------------------|--|
| pm-spi | Displays port manager stateful packet inspection (SPI) event debug messages. |
| pm-vectors | Displays port manager vector-related event debug messages. |
| detail | (Optional) Displays vector-function details. |
| ses | Displays service expansion shelf (SES) related event debug messages. |
| vlan | Displays VLAN creation and deletion event debug messages. |

Command Default Debugging is disabled.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|------------------------|--------------------|------------------------------|
| | Cisco IOS XE 3.2SE | This command was introduced. |

Usage Guidelines The **undebug platform pm** command is the same as the **no debug platform pm** command.

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

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

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

```
Device# debug platform pm vlans
```

debug platform udd

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

```
debug platform udd [{error | event}] [switch switch-number]
no debug platform udd [{error | event}] [switch switch-number]
```

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

Command Default Debugging is disabled.

| | | |
|-------------------------|---|------------------------------|
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE 3.2SE | This command was introduced. |
| Usage Guidelines | <p>The undebbug platform uidd command is the same as the no debug platform uidd command.</p> <p>When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the active switch by using the session switch-number EXEC command. Then enter the debug command at the command-line prompt of the stack member.</p> | |

debug spanning-tree

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

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

| | | |
|---------------------------|---------------------|---|
| Syntax Description | all | Displays all spanning-tree debug messages. |
| | backbonefast | Displays BackboneFast-event debug messages. |
| | bpdu | Displays spanning-tree bridge protocol data unit (BPDU) debug messages. |
| | bpdu-opt | Displays optimized BPDU handling debug messages. |
| | config | Displays spanning-tree configuration change debug messages. |
| | etherchannel | Displays EtherChannel-support debug messages. |
| | events | Displays spanning-tree topology event debug messages. |
| | exceptions | Displays spanning-tree exception debug messages. |
| | general | Displays general spanning-tree activity debug messages. |
| | ha | Displays high-availability spanning-tree debug messages. |
| | mstp | Debugs Multiple Spanning Tree Protocol (MSTP) events. |
| | pvst+ | Displays per-VLAN spanning-tree plus (PVST+) event debug messages. |
| | root | Displays spanning-tree root-event debug messages. |

| | |
|------------------------|---|
| snmp | Displays spanning-tree Simple Network Management Protocol (SNMP) handling debug messages. |
| switch | Displays device shim command debug messages. This shim is the software module that is the interface between the generic Spanning Tree Protocol (STP) code and the platform-specific code of various device platforms. |
| synchronization | Displays the spanning-tree synchronization event debug messages. |
| uplinkfast | Displays UplinkFast-event debug messages. |

Command Default Debugging is disabled.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|------------------------|--------------------|------------------------------|
| | Cisco IOS XE 3.2SE | This command was introduced. |

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

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

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

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

```
Device# debug spanning-tree all
```

interface port-channel

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

```
interface port-channel port-channel-number
no interface port-channel
```

Syntax Description *port-channel-number* Channel group number. The range is 1 to 128.

Command Default No port channel logical interfaces are defined.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|--------------------|------------------------------|
| | Cisco IOS XE 3.2SE | This command was introduced. |

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

Only one port channel in a channel group is allowed.

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

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

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

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

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

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

lACP max-bundle

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

```
lACP max-bundle max_bundle_number
no lACP max-bundle
```

| Syntax Description | <i>max_bundle_number</i> The maximum number of active LACP ports in the port channel. The range is 1 to 8. The default is 8. | | | | |
|---------------------------|--|---------|--------------|--------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Interface configuration | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.3SE</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE 3.3SE | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE 3.3SE | This command was introduced. | | | | |

Usage Guidelines

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

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

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

This example shows how to specify a maximum of five active LACP ports in port channel 2:

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

lACP port-priority

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

```
lACP port-priority priority
no lACP port-priority
```

Syntax Description

priority Port priority for LACP. The range is 1 to 65535.

Command Default

The default is 32768.

Command Modes

Interface configuration

Command History

| Release | Modification |
|--------------------|------------------------------|
| Cisco IOS XE 3.2SE | This command was introduced. |

Usage Guidelines

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

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

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



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

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

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

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

```
Device# interface gigabitEthernet2/0/1
Device(config-if)# lACP port-priority 1000
```

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

lACP rate

To set the rate at which Link Aggregation Control Protocol (LACP) control packets are ingress to an LACP-supported interface, use the **lACP rate** command in interface configuration mode. To return to the default settings, use the **no** form of this command

```
lACP rate {normal | fast}
no lACP rate
```

Syntax Description

normal Specifies that LACP control packets are ingress at the normal rate, every 30 seconds after the link is bundled.

fast Specifies that LACP control packets are ingress at the fast rate, once every 1 second.

Command Default

The default ingress rate for control packets is 30 seconds after the link is bundled.

Command Modes

Interface configuration (config-if)

Command History

| Release | Modification |
|----------------------------|------------------------------|
| Cisco IOS XE Denali 16.2.1 | This command was introduced. |

Usage Guidelines

Use this command to modify the duration of LACP timeout. The LACP timeout value on Cisco switch is three times the LACP rate configured on the interface. Using the **lACP rate** command, you can select the LACP timeout value for a switch to be either 90 seconds or 3 seconds.

This command is supported only on LACP-enabled interfaces.

This example shows how to specify the fast (1 second) ingress rate on interface GigabitEthernet 0/0:

```
Device(config)# interface gigabitEthernet 0/0
Device(config-if)# lACP rate fast
```

lACP system-priority

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

```
lACP system-priority priority
no lACP system-priority
```

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

| | |
|------------------------|-----------------------|
| Command Default | The default is 32768. |
|------------------------|-----------------------|

| | |
|----------------------|----------------------|
| Command Modes | Global configuration |
|----------------------|----------------------|

| Command History | Release | Modification |
|------------------------|--------------------|------------------------------|
| | Cisco IOS XE 3.2SE | This command was introduced. |

Usage Guidelines

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

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

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

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

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

This example shows how to set the LACP system priority:

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

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

pagp learn-method

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

```
pagp learn-method {aggregation-port | physical-port}
no pagp learn-method
```

| | | |
|---------------------------|---|--|
| Syntax Description | aggregation-port | Specifies address learning on the logical port channel. The device sends packets to the source using any port in the EtherChannel. This setting is the default. With aggregation-port learning, it is not important on which physical port the packet arrives. |
| | physical-port | Specifies address learning on the physical port within the EtherChannel. The device sends packets to the source using the same port in the EtherChannel from which it learned the source address. The other end of the channel uses the same port in the channel for a particular destination MAC or IP address. |
| Command Default | The default is aggregation-port (logical port channel). | |
| Command Modes | Interface configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE 3.2SE | This command was introduced. |

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

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

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

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

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

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

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

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

pagp port-priority

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

pagp port-priority *priority*
no pagp port-priority

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

| | |
|------------------------|---------------------|
| Command Default | The default is 128. |
|------------------------|---------------------|

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

| Command History | Release | Modification |
|------------------------|--------------------|------------------------------|
| | Cisco IOS XE 3.2SE | This command was introduced. |

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

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

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

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

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

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

port-channel

To convert the auto created EtherChannel into a manual channel and adding configuration on the EtherChannel, use the **port-channel** command in privileged EXEC mode.

```
port-channel {channel-group-number persistent | persistent }
```

| | | |
|---------------------------|---|---|
| Syntax Description | <i>channel-group-number</i> | Channel group number. The range is 1 to 128. |
| | persistent | Converts the auto created EtherChannel into a manual channel and allows you to add configuration on the EtherChannel. |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE 3.7.2E | This command was introduced. |
| Usage Guidelines | You can use the show etherchannel summary privileged EXEC command to display the EtherChannel information. | |

Examples

This example shows how to convert the auto created EtherChannel into a manual channel:

```
Device# port-channel 1 persistent
```

port-channel auto

To enable the auto-LAG feature on a switch globally, use the **port-channel auto** command in global configuration mode. To disable the auto-LAG feature on the switch globally, use **no** form of this command.

```
port-channel auto  
no port-channel auto
```

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no arguments or keywords. | |
| Command Default | By default, the auto-LAG feature is disabled globally and is enabled on all port interfaces. | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE 3.7.2E | This command was introduced. |

Usage Guidelines

You can use the **show etherchannel auto** privileged EXEC command to verify if the EtherChannel was created automatically.

Examples

This example shows how to enable the auto-LAG feature on the switch:

```
Device(config)# port-channel auto
```

port-channel load-balance

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

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

Syntax Description

| | |
|------------------------------|---|
| dst-ip | Specifies load distribution based on the destination host IP address. |
| dst-mac | Specifies load distribution based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel. |
| dst-mixed-ip-port | Specifies load distribution based on the destination IPv4 or IPv6 address and the TCP/UDP (Layer 4) port number. |
| dst-port | Specifies load distribution based on the destination TCP/UDP (Layer 4) port number for both IPv4 and IPv6. |
| extended | Sets extended load balance methods among the ports in the EtherChannel. See the port-channel load-balance extended command. |
| src-dst-ip | Specifies load distribution based on the source and destination host IP address. |
| src-dst-mac | Specifies load distribution based on the source and destination host MAC address. |
| src-dst-mixed-ip-port | Specifies load distribution based on the source and destination host IP address and TCP/UDP (layer 4) port number. |
| src-dst-port | Specifies load distribution based on the source and destination TCP/UDP (Layer 4) port number. |
| src-ip | Specifies load distribution based on the source host IP address. |
| src-mac | Specifies load distribution based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port. |
| src-mixed-ip-port | Specifies load distribution based on the source host IP address and TCP/UDP (Layer 4) port number. |
| src-port | Specifies load distribution based on the TCP/UDP (Layer 4) port number. |

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

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|--------------------|------------------------------|
| | Cisco IOS XE 3.2SE | This command was introduced. |

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

Examples

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

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

port-channel load-balance extended

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

```
port-channel load-balance extended [{dst-ip | dst-mac | dst-port | ipv6-label | l3-proto | src-ip | src-mac | src-port}]
no port-channel load-balance extended
```

| Syntax Description | |
|--------------------|--|
| dst-ip | (Optional) Specifies load distribution based on the destination host IP address. |
| dst-mac | (Optional) Specifies load distribution based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel. |
| dst-port | (Optional) Specifies load distribution based on the destination TCP/UDP (Layer 4) port number for both IPv4 and IPv6. |
| ipv6-label | (Optional) Specifies load distribution based on the source MAC address and IPv6 flow label. |
| l3-proto | (Optional) Specifies load distribution based on the source MAC address and Layer 3 protocols. |
| src-ip | (Optional) Specifies load distribution based on the source host IP address. |
| src-mac | (Optional) Specifies load distribution based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port. |
| src-port | (Optional) Specifies load distribution based on the TCP/UDP (Layer 4) port number. |

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

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|--------------------|------------------------------|
| | Cisco IOS XE 3.2SE | This command was introduced. |

Usage Guidelines For information about when to use these forwarding methods, see the *Layer 2/3 Configuration Guide (Catalyst 3850 Switches)* for this release.

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

Examples

This example shows how to set the extended load-distribution method:

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

port-channel min-links

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

```
port-channel min-links min_links_number
no port-channel min-links
```

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

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

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

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

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

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

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

This example shows how to specify a minimum of three active LACP ports before port channel 2 becomes active:


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

rep admin vlan

To configure a Resilient Ethernet Protocol (REP) administrative VLAN for REP to transmit hardware flood layer (HFL) messages, use the **rep admin vlan** command in global configuration mode. To return to the default configuration with VLAN 1 as the administrative VLAN, use the **no** form of this command.

```
rep admin vlan vlan-id
no rep admin vlan
```

Syntax Description

vlan-id The 48-bit static MAC address.

Command Default

The default value of the administrative VLAN is VLAN 1.

Command Modes

Global configuration (config)

Command History

Release

Cisco IOS XE Denali 16.2.2

Modification

This command was introduced

Usage Guidelines

The range of the REP administrative VLAN is from 2 to 4094.

If you do not configure an administrative VLAN, the default VLAN is VLAN 1. The default VLAN 1 is always configured. There can be only one administrative VLAN on a router and on a segment.

You can verify your settings by entering the **show interfaces rep detail** privileged EXEC command.

The following example shows how to configure VLAN 100 as the REP administrative VLAN:

```
Device(config)# rep admin vlan 100
```

rep block port

To configure a REP VLAN load balancing on the REP primary edge port, use the **rep block port** command in interface configuration mode. To return to the default configuration with VLAN 1 as the administrative VLAN, use the **no** form of this command.

```
rep block port {id port-id | neighbor-offset | preferred} vlan {vlan-list | all}
no rep block port {id port-id | neighbor-offset | preferred}
```

Syntax Description

id *port-id*

Specifies the VLAN blocking alternate port by entering the unique port ID, which is automatically generated when REP is enabled. The REP port ID is a 16-character hexadecimal value. You can display the port ID for an interface by entering the **show interface interface-id rep detail** command in privileged EXEC mode.

| | |
|------------------------|--|
| <i>neighbor-offset</i> | Identifies the VLAN blocking alternate port by entering the offset number of a neighbor. The range is from -256 to +256; a value of 0 is invalid. |
| preferred | Selects the regular segment port previously identified as the preferred alternate port for VLAN load balancing. |
| vlan | Identifies the VLANs to be blocked. |
| <i>vlan-list</i> | VLAN ID or range of VLAN IDs to be displayed. Enter a VLAN ID from 1 to 4094 or a range or sequence of VLANs (such as 1-3, 22, 41-44) to be blocked. |
| all | Blocks all the VLANs. |

Command Default

The default behavior after you enter the **rep preempt segment** command in privileged EXEC (for manual preemption) is to block all VLANs at the primary edge port. This behavior remains until you configure the **rep block port** command.

If the primary edge port cannot determine which port is to be the alternate port, the default action is no preemption and no VLAN load balancing.

Command Modes

Interface configuration (config-if)

Command History

| Release | Modification |
|----------------------------|-----------------------------|
| Cisco IOS XE Denali 16.2.2 | This command was introduced |

Usage Guidelines

You must enter this command on the REP primary edge port.

When you select an alternate port by entering an offset number, this number identifies the downstream neighbor port of an edge port. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors. Do not enter an offset value of 1 because that is the offset number of the primary edge port itself.

If you have configured a preempt delay time by entering the **rep preempt delay seconds** command in interface configuration mode and a link failure and recovery occurs, VLAN load balancing begins after the configured preemption time period elapses without another link failure. The alternate port specified in the load-balancing configuration blocks the configured VLANs and unblocks all other segment ports. If the primary edge port cannot determine the alternate port for VLAN balancing, the default action is no preemption.

Each port in a segment has a unique port ID. To determine the port ID of a port, enter the **show interfaces interface-id rep detail** command in privileged EXEC mode.

The following example shows how to configure REP VLAN load balancing.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep block port id 0009001818D68700 vlan 1-100
```

rep lsl-age-timer

To configure the REP link status layer (LSL) age-out timer value, use the **rep lsl-age-timer** command in interface configuration mode. To restore the default age-out timer value, use the **no** form of this command.

```
rep lsl-age-timer milliseconds
no rep lsl-age-timer milliseconds
```

| | | |
|---------------------------|---|-----------------------------|
| Syntax Description | <i>milliseconds</i> REP LSL age-out timer value in milliseconds (ms). The range is from 120 ms to 10000 ms in multiples of 40 ms. | |
| Command Default | The default LSL age-out timer value is 5 ms. | |
| Command Modes | Interface configuration (config-if) | |
| Command History | Release | Modification |
| | Cisco IOS XE Denali 16.2.2 | This command was introduced |

Usage Guidelines The **rep lsl-age-timer** command is used to configure the REP LSL age-out timer value. While configuring REP configurable timers, we recommend that you configure the REP LSL number of retries first and then configure the REP LSL age-out timer value.

The following example shows how to configure REP LSL age-out timer value.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 1 edge primary
Device(config-if)# rep lsl-age-timer 2000
```

rep lsl-retries

To configure the REP link status layer (LSL) number of retries, use the **rep lsl-retries** command in interface configuration mode. To restore the default number of retries, use the **no** form of this command.

```
rep lsl-retries number-of-retries
no rep lsl-retries number-of-retries
```

| | | |
|---------------------------|---|-----------------------------|
| Syntax Description | <i>number-of-retries</i> Number of LSL retries. The range of retries is from 3 to 10. | |
| Command Default | The default number of LSL retries is 5. | |
| Command Modes | Interface configuration (config-if) | |
| Command History | Release | Modification |
| | Cisco IOS XE Denali 16.2.2 | This command was introduced |

Usage Guidelines

The **rep lsl-retries** command is used to configure the number of retries before the REP link is disabled. While configuring REP configurable timers, we recommend that you configure the REP LSL number of retries first and then configure the REP LSL age-out timer value.

The following example shows how to configure REP LSL retries.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 2 edge primary
```

rep preempt delay

To configure a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered, use the **rep preempt delay** command in interface configuration mode. To remove the configured delay, use the **no** form of this command.

rep preempt delay *seconds*
no rep preempt delay

Syntax Description

seconds Number of seconds to delay REP preemption. The range is from 15 to 300 seconds. The default is manual preemption without delay.

Command Default

REP preemption delay is not set. The default is manual preemption without delay.

Command Modes

Interface configuration (config-if)

Command History

| Release | Modification |
|----------------------------|-----------------------------|
| Cisco IOS XE Denali 16.2.2 | This command was introduced |

Usage Guidelines

You must enter this command on the REP primary edge port.

You must enter this command and configure a preempt time delay if you want VLAN load balancing to automatically trigger after a link failure and recovery.

If VLAN load balancing is configured, after a segment port failure and recovery, the REP primary edge port starts a delay timer before VLAN load balancing occurs. Note that the timer restarts after each link failure. When the timer expires, the REP primary edge alerts the alternate port to perform VLAN load balancing (configured by using the **rep block port** interface configuration command) and prepares the segment for the new topology. The configured VLAN list is blocked at the alternate port, and all other VLANs are blocked at the primary edge port.

You can verify your settings by entering the **show interfaces rep** privileged EXEC command.

The following example shows how to configure a REP preemption time delay of 100 seconds on the primary edge port.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep preempt delay 100
```

rep preempt segment

To manually start REP VLAN load balancing on a segment, use the **rep preempt segment** command in privileged EXEC mode.

```
rep preempt segment segment-id
```

Syntax Description

segment-id ID of the REP segment. The range is from 1 to 1024.

Command Default

Manual preemption is the default behavior.

Command Modes

Privileged EXEC (#)

Command History

| Release | Modification |
|----------------------------|-----------------------------|
| Cisco IOS XE Denali 16.2.2 | This command was introduced |

Usage Guidelines

Enter this command on the segment, which has the primary edge port on the router.

Ensure that all the other segment configuration is completed before setting preemption for VLAN load balancing. When you enter the **rep preempt segment** *segment-id* command, a confirmation message appears before the command is executed because preemption for VLAN load balancing can disrupt the network.

If you do not enter the **rep preempt delay** *seconds* command in interface configuration mode on the primary edge port to configure a preemption time delay, the default configuration is to manually trigger VLAN load balancing on the segment. Use the **show rep topology** privileged EXEC command to see which port in the segment is the primary edge port.

If you do not configure VLAN load balancing, entering this command results in the default behavior—the primary edge port blocks all VLANs.

You configure VLAN load balancing by entering the **rep block port** command in interface configuration mode on the REP primary edge port before you manually start preemption.

The following example shows how to manually trigger REP preemption on segment 100.

```
Device# rep preempt segment 100
```

rep segment

To enable REP on the interface and to assign a segment ID to the interface, use the **rep segment** command in interface configuration mode. To disable REP on the interface, use the **no** form of this command.

```
rep segment segment-id [edge [no-neighbor] [primary]] [preferred]
no rep segment
```

Syntax Description

segment-id Segment for which REP is enabled. Assign a segment ID to the interface. The range is from 1 to 1024.

| | |
|--------------------|---|
| edge | (Optional) Configures the port as an edge port. Each segment has only two edge ports. |
| no-neighbor | (Optional) Specifies the segment edge as one with no external REP neighbor. |
| primary | (Optional) Specifies that the port is the primary edge port where you can configure VLAN load balancing. A segment has only one primary edge port. |
| preferred | (Optional) Specifies that the port is the preferred alternate port or the preferred port for VLAN load balancing. |
| Note | Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port. |

Command Default REP is disabled on the interface.

Command Modes Interface configuration (config-if)

| Command History | Release | Modification |
|------------------------|----------------------------|-----------------------------|
| | Cisco IOS XE Denali 16.2.2 | This command was introduced |

Usage Guidelines REP ports must be a Layer 2 IEEE 802.1Q port or 802.1AD port. You must configure two edge ports on each REP segment, a primary edge port and a port to act as a secondary edge port.

If REP is enabled on two ports on a router, both ports must be either regular segment ports or edge ports. REP ports follow these rules:

- If only one port on a router is configured in a segment, the port should be an edge port.
- If two ports on a router belong to the same segment, both ports must be regular segment ports.
- If two ports on a router belong to the same segment and one is configured as an edge port and one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.

REP interfaces come up in a blocked state and remain in a blocked state until notified that it is safe to unblock. Be aware of this to avoid sudden connection losses.

When REP is enabled on an interface, the default is for the port to be a regular segment port.

The following example shows how to enable REP on a regular (nonedge) segment port.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 100
```

The following example shows how to enable REP on a port and identify the port as the REP primary edge port.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 100 edge primary
```

The following example shows how to enable REP on a port and identify the port as the REP secondary edge port.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 100 edge
```

The following example shows how to enable REP as an edge no-neighbor port.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 1 edge no-neighbor primary
```

rep stcn

To configure a REP edge port to send segment topology change notifications (STCNs) to another interface or to other segments, use the **rep stcn** command in interface configuration mode. To disable the sending of STCNs to the interface or to the segment, use the **no** form of this command.

```
rep stcn {interface interface-id | segment segment-id-list}
no rep stcn {interface | segment}
```

Syntax Description

interface *interface-id* Specifies a physical interface or port channel to receive STCNs.

segment *segment-id-list* Specifies one REP segment or a list of segments to receive STCNs. The segment range is from 1 to 1024. You can also configure a sequence of segments (for example 3 to 5, 77, 100).

Command Default

Transmission of STCNs to other interfaces or segments is disabled.

Command Modes

Interface configuration (config-if)

Command History

| Release | Modification |
|----------------------------|-----------------------------|
| Cisco IOS XE Denali 16.2.2 | This command was introduced |

Usage Guidelines

Enter this command on a segment edge port to send STCNs to one or more segments or to an interface. You can verify your settings by entering the **show interfaces rep detail** privileged EXEC command.

The following example shows how to configure a REP edge port to send STCNs to segments 25 to 50.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep stcn segment 25-50
```

show etherchannel

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

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

Syntax Description

channel-group-number (Optional) Channel group number. The range is 1 to 128.

| | |
|---------------------|--|
| auto | (Optional) Displays that Etherchannel is created automatically. |
| detail | (Optional) Displays detailed EtherChannel information. |
| load-balance | (Optional) Displays the load-balance or frame-distribution scheme among ports in the port channel. |
| port | (Optional) Displays EtherChannel port information. |
| port-channel | (Optional) Displays port-channel information. |
| protocol | (Optional) Displays the protocol that is being used in the channel. |
| summary | (Optional) Displays a one-line summary per channel group. |

Command Default

None

Command Modes

User EXEC

Command History

| Release | Modification |
|--------------------|------------------------------|
| Cisco IOS XE 3.2SE | This command was introduced. |

Usage Guidelines

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

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

```
device# show etherchannel auto
Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator
       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port
       A - formed by Auto LAG

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

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
 1      Po1(SUA)        LACP       Gi1/0/45(P) Gi2/0/21(P) Gi3/0/21(P)
```

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

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

                Ports in the group:
                -----
Port: Gi1/0/1
```



```

-----
Port state      = Up Mstr In-Bndl
Channel group = 1          Mode = Active          Gcchange = -
Port-channel   =          Po1GC = -             Pseudo port-channel = Po1
Port index     =          0Load = 0x00          Protocol = LACP

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

Local information:

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

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

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

Port-channel: Po1 (Primary Aggregator)

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

Ports in the Port-channel:

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

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

```

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

```

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

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

```

```

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

```

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

```

Device> show etherchannel 1 port-channel
Port-channels in the group:
-----
Port-channel: Po1 (Primary Aggregator)

```

```

-----
Age of the Port-channel = 01d:20h:24m:50s
Logical slot/port = 10/1 Number of ports = 2
Logical slot/port = 10/1 Number of ports = 2
Port state = Port-channel Ag-Inuse
Protocol = LACP

Ports in the Port-channel:

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

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

```

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

```

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

```

show interfaces rep detail

To display detailed REP configuration and status for all the interfaces or the specified interface, including the administrative VLAN, use the **show interfaces rep detail** command in privileged EXEC mode.

show interfaces [*interface-id*] **rep detail**

| | |
|---------------------------|--|
| Syntax Description | <i>interface-id</i> (Optional) Physical interface used to display the port ID. |
|---------------------------|--|

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|----------------------------|-----------------------------|
| | Cisco IOS XE Denali 16.2.2 | This command was introduced |

| | |
|-------------------------|---|
| Usage Guidelines | Enter this command on a segment edge port to send STCNs to one or more segments or to an interface. You can verify your settings by entering the show interfaces rep detail privileged EXEC command. |
|-------------------------|---|

The following example shows how to display the REP configuration and status for a specified interface.

```

Device# show interfaces TenGigabitEthernet4/1 rep detail

TenGigabitEthernet4/1 REP enabled
Segment-id: 3 (Primary Edge)
PortID: 03010015FA66FF80

```

```

Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 02040015FA66FF804050
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 999, tx: 652
HFL PDU rx: 0, tx: 0
BPA TLV rx: 500, tx: 4
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 6, tx: 5
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 135, tx: 136

```

show lacp

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

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

| Syntax Description | |
|-----------------------------|---|
| <i>channel-group-number</i> | (Optional) Channel group number. The range is 1 to 128. |
| counters | Displays traffic information. |
| internal | Displays internal information. |
| neighbor | Displays neighbor information. |
| sys-id | Displays the system identifier that is being used by LACP. The system identifier consists of the LACP system priority and the device MAC address. |

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

| Command Modes | |
|---------------|-----------|
| | User EXEC |

| Command History | Release | Modification |
|-----------------|--------------------|------------------------------|
| | Cisco IOS XE 3.2SE | This command was introduced. |

Usage Guidelines

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

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

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

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

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

Table 1: show lacp counters Field Descriptions

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

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

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

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

The following table describes the fields in the display:

Table 2: show lacp internal Field Descriptions

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

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

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

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

Channel group 3 neighbors

Partner's information:

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

Partner's information:

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

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

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

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

show pagp

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

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

Syntax Description

channel-group-number (Optional) Channel group number. The range is 1 to 128.

counters Displays traffic information.

dual-active Displays the dual-active status.

internal Displays internal information.

neighbor Displays neighbor information.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release

Cisco IOS XE 3.2SE

Modification

This command was introduced.

Usage Guidelines

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

Examples

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

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

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

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

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

<output truncated>

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

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

Channel group 1

Port      Flags State  Timers  Hello  Partner  PAgP    Learning  Group
Gi1/0/1   SC    U6/S7  H       30s    1        128     Any       16
Gi1/0/2   SC    U6/S7  H       30s    1        128     Any       16
```

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

```
Device> show pagp 1 neighbor

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

Channel group 1 neighbors

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

show platform software fed etherchannel

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

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

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

Command Default None

Command Modes Privileged EXEC

| Command History | Release | Modification |
|------------------------|----------------------------|------------------------------|
| | Cisco IOS XE Denali 16.1.1 | This command was introduced. |

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

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

show platform pm

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

show platform pm {**etherchannel** *channel-group-number* **group-mask** | **interface-numbers** | **port-data** *interface-id* | **port-state** | **spi-info** | **spi-req-q**}

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

Command Default None

Command Modes Privileged EXEC

| Command History | Release | Modification |
|------------------------|--------------------|------------------------------|
| | Cisco IOS XE 3.2SE | This command was introduced. |

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

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

show rep topology

To display REP topology information for a segment or for all segments, including the primary and secondary edge ports in the segment, use the **show rep topology** command in privileged EXEC mode.

show rep topology [**segment** *segment-id*] [**archive**] [**detail**]

| Syntax Description | | |
|----------------------------------|----------------------------|--|
| segment <i>segment-id</i> | | (Optional) Specifies the segment for which to display REP topology information. The ID range is from 1 to 1024. |
| archive | | (Optional) Displays the previous topology of the segment. This keyword is useful for troubleshooting a link failure. |
| detail | | (Optional) Displays detailed REP topology information. |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Denali 16.2.2 | This command was introduced |

The following is sample output from the show rep topology command.

```
Device# show rep topology

REP Segment 1
BridgeName      PortName      Edge Role
-----
10.64.106.63    Te5/4         Pri  Open
10.64.106.228   Te3/4         Open
10.64.106.228   Te3/3         Open
10.64.106.67    Te4/3         Open
10.64.106.67    Te4/4         Alt
10.64.106.63    Te4/4         Sec  Open

REP Segment 3
BridgeName      PortName      Edge Role
-----
10.64.106.63    Gi50/1        Pri  Open
SVT_3400_2      Gi0/3         Open
SVT_3400_2      Gi0/4         Open
10.64.106.68    Gi40/2        Open
10.64.106.68    Gi40/1        Open
10.64.106.63    Gi50/2        Sec  Alt
```

The following is sample output from the **show rep topology detail** command.

```
Device# show rep topology detail

REP Segment 1
```

```

10.64.106.63, Te5/4 (Primary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1700
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 1 / [-6]
10.64.106.228, Te3/4 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b1b.1f20
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 2 / [-5]
10.64.106.228, Te3/3 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b1b.1f20
  Port Number: 00E
  Port Priority: 000
  Neighbor Number: 3 / [-4]
10.64.106.67, Te4/3 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1800
  Port Number: 008
  Port Priority: 000
  Neighbor Number: 4 / [-3]
10.64.106.67, Te4/4 (Intermediate)
  Alternate Port, some vlans blocked
  Bridge MAC: 0005.9b2e.1800
  Port Number: 00A
  Port Priority: 000
  Neighbor Number: 5 / [-2]
10.64.106.63, Te4/4 (Secondary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1700
  Port Number: 00A
  Port Priority: 000
  Neighbor Number: 6 / [-1]

```

show uddl

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

```

show uddl [Auto-Template | Capwap | GigabitEthernet | GroupVI | InternalInterface |
Loopback | Null | Port-channel | TenGigabitEthernet | Tunnel | Vlan] interface_number
show uddl neighbors

```

| Syntax Description | Auto-Template | (Optional) Displays UDLD operational status of the auto-template interface. The range is from 1 to 999. |
|--------------------|------------------------|---|
| | Capwap | (Optional) Displays UDLD operational status of the CAPWAP interface. The range is from 0 to 2147483647. |
| | GigabitEthernet | (Optional) Displays UDLD operational status of the GigabitEthernet interface. The range is from 0 to 9. |
| | GroupVI | (Optional) Displays UDLD operational status of the group virtual interface. The range is from 1 to 255. |

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

Command Default None

Command Modes User EXEC

| Command History | Release | Modification |
|------------------------|--------------------|------------------------------|
| | Cisco IOS XE 3.2SE | This command was introduced. |

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

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

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

```
Neighbor echo 1 device: Switch-B
Neighbor echo 1 port: Gi2/0/2
Message interval: 5
CDP Device name: Switch-A
```

Table 3: show uddld Field Descriptions

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

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

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

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

switchport

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

switchport
no switchport

Syntax Description This command has no arguments or keywords.

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

Command Modes Interface configuration

Command History

| Release | Modification |
|--------------------|------------------------------|
| Cisco IOS XE 3.2SE | This command was introduced. |

Usage Guidelines

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



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

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

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



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

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

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

Examples

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

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

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

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

switchport access vlan

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

```
switchport access vlan {vlan-id | name vlan_name}
no switchport access vlan
```

Syntax Description

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

Command Default

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

Command Modes

Interface configuration

| Command History | Release | Modification |
|-----------------|----------------------------|--|
| | Cisco IOS XE 3.2SE | This command was introduced. |
| | Cisco IOS XE Denali 16.2.1 | The name <i>vlan_name</i> keyword was introduced. |

Usage Guidelines

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

If the switchport mode is set to **access vlan** *vlan-id*, the port operates as a member of the specified VLAN. An access port can be assigned to only one VLAN.

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

Examples

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

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

Examples

This example show how to first populate the VLAN database by associating a VLAN ID with a VLAN name, and then configure the VLAN (using the name) on an interface, in the access mode: You can also verify your configuration by entering the **show interfaces interface-id switchport** in privileged EXEC command and examining information in the Access Mode VLAN: row.

Part 1 - Making the entry in the VLAN database:

```
Device# configure terminal
Device(config)# vlan 33
Device(config-vlan)# name test
Device(config-vlan)# end
Device#
```

Part 2 - Checking the VLAN database

```
Device # show vlan id 33
VLAN Name      Status Ports
-----
33   test       active
-----
VLAN Type  SAID      MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
33   enet  100033   1500  -     -     -    -    -      0      0
-----
Remote SPAN VLAN
-----
Disabled

Primary  Secondary Type          Ports
-----
```

Part 3 - Assigning VLAN to the interface by using the name of the VLAN

```
Device # configure terminal
Device(config)# interface GigabitEthernet3/1/1
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan name test
Device(config-if)# end
Device#
```


Part 4 - Verifying configuration

```
Device # show running-config interface GigabitEthernet3/1/1
Building configuration...
Current configuration : 113 bytes
!
interface GigabitEthernet3/1/1
switchport access vlan 33
switchport mode access
Switch#
```

Part 5 - Verifying interface switchport

```
Device # show interface GigabitEthernet3/1/1 switchport
Name: Gi3/1/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 33 (test)
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 trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Switch#
```

switchport mode

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

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

Syntax Description

| | |
|---------------|---|
| access | Sets the port to access mode (either static-access or dynamic-access depending on the setting of the switchport access vlan interface configuration command). The port is set to access unconditionally and operates as a nontrunking, single VLAN interface that sends and receives nonencapsulated (non-tagged) frames. An access port can be assigned to only one VLAN. |
|---------------|---|

| | |
|--------------------------|---|
| dynamic auto | Sets the port trunking mode dynamic parameter to auto to specify that the interface convert the link to a trunk link. This is the default switchport mode. |
| dynamic desirable | Sets the port trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link. |
| trunk | Sets the port to trunk unconditionally. The port is a trunking VLAN Layer 2 interface. The port sends and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two devices or between a device and a router. |

Command Default

The default mode is **dynamic auto**.

Command Modes

Interface configuration

Command History

| Release | Modification |
|--------------------|------------------------------|
| Cisco IOS XE 3.2SE | This command was introduced. |

Usage Guidelines

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

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

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

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

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

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

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

Access ports and trunk ports are mutually exclusive.

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

- If you try to enable IEEE 802.1x on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, the port mode is not changed.

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

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

Examples

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

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

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

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

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

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

switchport nonegotiate

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

```
switchport nonegotiate
no switchport nonegotiate
```

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Interface configuration

Command History

| Release | Modification |
|--------------------|------------------------------|
| Cisco IOS XE 3.2SE | This command was introduced. |

Usage Guidelines

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

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

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

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

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

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

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

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

switchport voice vlan

To configure voice VLAN on the port, use the **switchport voice vlan** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

```
switchport voice vlan {vlan-id | dot1p | none | untagged | name vlan_name}
no switchport voice vlan
```

| Syntax Description | | |
|--------------------|------------------------------|--|
| | <i>vlan-id</i> | The VLAN to be used for voice traffic. The range is 1 to 4094. By default, the IP phone forwards the voice traffic with an IEEE 802.1Q priority of 5. |
| | dot1p | Configures the telephone to use IEEE 802.1p priority tagging and uses VLAN 0 (the native VLAN). By default, the Cisco IP phone forwards the voice traffic with an IEEE 802.1p priority of 5. |
| | none | Does not instruct the IP telephone about the voice VLAN. The telephone uses the configuration from the telephone key pad. |
| | untagged | Configures the telephone to send untagged voice traffic. This is the default for the telephone. |
| | name <i>vlan_name</i> | (Optional) Specifies the VLAN name to be used for voice traffic. You can enter up to 128 characters. |

Command Default The default is not to automatically configure the telephone (**none**).
The telephone default is not to tag frames.

Command Modes

Interface configuration

Command History

| Release | Modification |
|----------------------------|--|
| Cisco IOS XE 3.2SE | This command was introduced. |
| Cisco IOS XE Denali 16.2.1 | Option to specify a VLAN name for voice VLAN. The ' name ' keyword was added. |

Usage Guidelines

You should configure voice VLAN on Layer 2 access ports.

You must enable Cisco Discovery Protocol (CDP) on the switch port connected to the Cisco IP phone for the device to send configuration information to the phone. CDP is enabled by default globally and on the interface.

Before you enable voice VLAN, we recommend that you enable quality of service (QoS) on the interface by entering the **trust device cisco-phone** interface configuration command. If you use the auto QoS feature, these settings are automatically configured.

When you enter a VLAN ID, the IP phone forwards voice traffic in IEEE 802.1Q frames, tagged with the specified VLAN ID. The device puts IEEE 802.1Q voice traffic in the voice VLAN.

When you select **dot1p**, **none**, or **untagged**, the device puts the indicated voice traffic in the access VLAN.

In all configurations, the voice traffic carries a Layer 2 IP precedence value. The default is 5 for voice traffic.

When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to 2. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but not on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the Cisco IP phone.

If any type of port security is enabled on the access VLAN, dynamic port security is automatically enabled on the voice VLAN.

You cannot configure static secure MAC addresses in the voice VLAN.

The Port Fast feature is automatically enabled when voice VLAN is configured. When you disable voice VLAN, the Port Fast feature is not automatically disabled.

This example show how to first populate the VLAN database by associating a VLAN ID with a VLAN name, and then configure the VLAN (using the name) on an interface, in the access mode: You can also verify your configuration by entering the **show interfaces interface-id switchport** in privileged EXEC command and examining information in the Voice VLAN: row.

Part 1 - Making the entry in the VLAN database:

```
Device# configure terminal
Device(config)# vlan 55
Device(config-vlan)# name test
Device(config-vlan)# end
Device#
```

Part 2 - Checking the VLAN database:

```
Device# show vlan id 55
VLAN Name Status Ports
-----
```

```

55 test active
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
-----
55 enet 100055 1500 - - - - - 0 0
Remote SPAN VLAN
-----
Disabled
Primary Secondary Type Ports
-----

```

Part 3- Assigning VLAN to the interface by using the name of the VLAN:

```

Device# configure terminal
Device(config)# interface gigabitethernet3/1/1
Device(config-if)# switchport mode access
Device(config-if)# switchport voice vlan name test
Device(config-if)# end
Device#

```

Part 4 - Verifying configuration:

```

Device# show running-config
interface gigabitethernet3/1/1
Building configuration...
Current configuration : 113 bytes
!
interface GigabitEthernet3/1/1
switchport voice vlan 55
switchport mode access
Switch#

```

Part 5 - Also can be verified in interface switchport:

```

Device# show interface GigabitEthernet3/1/1 switchport
Name: Gi3/1/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 55 (test)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Device#

```

udld

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

```
udld {aggressive | enable | message time message-timer-interval}
no udld {aggressive | enable | message}
```

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

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

Command Modes
Global configuration

| Command History | Release | Modification |
|-----------------|--------------------|------------------------------|
| | Cisco IOS XE 3.2SE | This command was introduced. |

Usage Guidelines
UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links. For information about normal and aggressive modes, see the *Catalyst 2960-X Switch Layer 2 Configuration Guide*, *Catalyst 2960-XR Switch Layer 2 Configuration Guide*, and *Layer 2/3 Configuration Guide (Catalyst 3850 Switches)*.

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

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

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

- The **udld reset** privileged EXEC command to reset all interfaces shut down by UDLD.
- The **shutdown** and **no shutdown** interface configuration commands.
- The **no udld enable** global configuration command followed by the **udld {aggressive | enable}** global configuration command to reenab UDLD globally.
- The **no udld port** interface configuration command followed by the **udld port** or **udld port aggressive** interface configuration command to reenab UDLD on the specified interface.

- The **errdisable recovery cause udld** and **errdisable recovery interval *interval*** global configuration commands to automatically recover from the UDLD error-disabled state.

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

```
Device(config)# udld enable
```

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

udld port

To enable UniDirectional Link Detection (UDLD) on an individual interface or to prevent a fiber-optic interface from being enabled by the **udld** global configuration command, use the **udld port** command in interface configuration mode. To return to the **udld** global configuration command setting or to disable UDLD if entered for a nonfiber-optic port, use the **no** form of this command.

udld port [aggressive]
no udld port [aggressive]

Syntax Description

aggressive (Optional) Enables UDLD in aggressive mode on the specified interface.

Command Default

On fiber-optic interfaces, UDLD is disabled and fiber-optic interfaces enable UDLD according to the state of the **udld enable** or **udld aggressive** global configuration command.

On nonfiber-optic interfaces, UDLD is disabled.

Command Modes

Interface configuration

Command History

| Release | Modification |
|--------------------|------------------------------|
| Cisco IOS XE 3.2SE | This command was introduced. |

Usage Guidelines

A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another device.

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links.

To enable UDLD in normal mode, use the **udld port** interface configuration command. To enable UDLD in aggressive mode, use the **udld port aggressive** interface configuration command.

Use the **no udld port** command on fiber-optic ports to return control of UDLD to the **udld enable** global configuration command or to disable UDLD on nonfiber-optic ports.

Use the **udld port aggressive** command on fiber-optic ports to override the setting of the **udld enable** or **udld aggressive** global configuration command. Use the **no** form on fiber-optic ports to remove this setting and to return control of UDLD enabling to the **udld** global configuration command or to disable UDLD on nonfiber-optic ports.

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

- The **udld reset** privileged EXEC command resets all interfaces shut down by UDLD.
- The **shutdown** and **no shutdown** interface configuration commands.
- The **no udld enable** global configuration command, followed by the **udld {aggressive | enable}** global configuration command reenables UDLD globally.
- The **no udld port** interface configuration command, followed by the **udld port** or **udld port aggressive** interface configuration command reenables UDLD on the specified interface.
- The **errdisable recovery cause udld** and **errdisable recovery interval *interval*** global configuration commands automatically recover from the UDLD error-disabled state.

This example shows how to enable UDLD on an port:

```
Device(config)# interface gigabitethernet6/0/1
Device(config-if)# udld port
```

This example shows how to disable UDLD on a fiber-optic interface despite the setting of the **udld** global configuration command:

```
Device(config)# interface gigabitethernet6/0/1
Device(config-if)# no udld port
```

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

udld reset

To reset all interfaces disabled by UniDirectional Link Detection (UDLD) and permit traffic to begin passing through them again (though other features, such as spanning tree, Port Aggregation Protocol (PAgP), and Dynamic Trunking Protocol (DTP) still have their normal effects, if enabled), use the **udld reset** command in privileged EXEC mode.

udld reset

| | | |
|---------------------------|---|------------------------------|
| Syntax Description | This command has no arguments or keywords. | |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE 3.2SE | This command was introduced. |
| Usage Guidelines | If the interface configuration is still enabled for UDLD, these ports begin to run UDLD again and are disabled for the same reason if the problem has not been corrected. | |

This example shows how to reset all interfaces disabled by UDLD:

```
Device# udld reset  
1 ports shutdown by UDLD were reset.
```