



Layer 2/3 Commands

- [avb](#), on page 4
- [avb vlan](#), on page 5
- [channel-group](#), on page 6
- [channel-protocol](#), on page 9
- [clear lacp](#), on page 10
- [clear pagp](#), on page 11
- [clear spanning-tree counters](#), on page 12
- [clear spanning-tree detected-protocols](#), on page 13
- [debug etherchannel](#), on page 14
- [debug lacp](#), on page 15
- [debug pagp](#), on page 16
- [debug platform pm](#), on page 17
- [debug platform udd](#), on page 18
- [debug spanning-tree](#), on page 19
- [instance \(VLAN\)](#), on page 21
- [interface port-channel](#), on page 23
- [lacp max-bundle](#), on page 25
- [lacp port-priority](#), on page 26
- [lacp rate](#), on page 27
- [lacp system-priority](#), on page 28
- [mvrp vlan creation](#), on page 29
- [mvrp registration](#), on page 30
- [mvrp timer](#), on page 32
- [name \(MST\)](#), on page 34
- [no ptp enable](#), on page 35
- [pagp learn-method](#), on page 36
- [pagp port-priority](#), on page 38
- [policy-map](#), on page 39
- [port-channel](#), on page 41
- [port-channel auto](#), on page 42
- [port-channel load-balance](#), on page 43
- [port-channel load-balance extended](#), on page 46
- [port-channel min-links](#), on page 47

- [ptp priority1 value, on page 48](#)
- [ptp priority2 value, on page 49](#)
- [ptp profile dot1as, on page 50](#)
- [rep admin vlan, on page 51](#)
- [rep block port, on page 52](#)
- [rep lsl-age-timer, on page 54](#)
- [rep lsl-retries, on page 55](#)
- [rep preempt delay, on page 56](#)
- [rep preempt segment, on page 57](#)
- [rep segment, on page 58](#)
- [rep stcn, on page 60](#)
- [revision, on page 61](#)
- [show avb domain, on page 62](#)
- [show avb streams, on page 64](#)
- [show etherchannel, on page 65](#)
- [show interfaces rep detail, on page 68](#)
- [show lacp, on page 69](#)
- [show msrp port bandwidth, on page 73](#)
- [show msrp streams, on page 75](#)
- [show pagp, on page 77](#)
- [show platform etherchannel, on page 79](#)
- [show platform hardware fed active vlan ingress, on page 80](#)
- [show platform pm, on page 81](#)
- [show platform software fed switch ptp, on page 82](#)
- [show ptp brief, on page 84](#)
- [show ptp clock, on page 85](#)
- [show ptp parent, on page 86](#)
- [show ptp port, on page 88](#)
- [show rep topology, on page 89](#)
- [show spanning-tree, on page 91](#)
- [show spanning-tree mst, on page 97](#)
- [show udld, on page 100](#)
- [show vlan dot1q tag native, on page 104](#)
- [spanning-tree backbonefast, on page 105](#)
- [spanning-tree bpdufilter, on page 106](#)
- [spanning-tree bpduguard, on page 108](#)
- [spanning-tree bridge assurance, on page 110](#)
- [spanning-tree cost, on page 111](#)
- [spanning-tree etherchannel guard misconfig, on page 113](#)
- [spanning-tree extend system-id, on page 115](#)
- [spanning-tree guard, on page 116](#)
- [spanning-tree link-type, on page 117](#)
- [spanning-tree loopguard default, on page 119](#)
- [spanning-tree mode, on page 120](#)
- [spanning-tree mst, on page 121](#)
- [spanning-tree mst configuration, on page 122](#)

- spanning-tree mst forward-time, on page 124
- spanning-tree mst hello-time, on page 125
- spanning-tree mst max-age, on page 126
- spanning-tree mst max-hops, on page 127
- spanning-tree mst pre-standard, on page 128
- spanning-tree mst priority, on page 130
- spanning-tree mst root, on page 131
- spanning-tree mst simulate pvst global, on page 132
- spanning-tree pathcost method, on page 133
- spanning-tree port-priority, on page 134
- spanning-tree portfast edge bpdupfilter default, on page 136
- spanning-tree portfast edge bpduguard default, on page 138
- spanning-tree portfast default, on page 139
- spanning-tree transmit hold-count, on page 141
- spanning-tree uplinkfast, on page 142
- spanning-tree vlan, on page 143
- switchport, on page 146
- switchport access vlan, on page 147
- switchport mode, on page 148
- switchport nonegotiate, on page 150
- switchport trunk, on page 151
- switchport voice vlan, on page 154
- udld, on page 157
- udld fast-hello, on page 159
- udld port, on page 160
- udld reset, on page 162
- vtp mode, on page 163

avb

To enable AVB, use **avb** command in global configuration or interface configuration mode. To disable AVB on the switch, use the **no** form of the command.

avb
no avb

Command Modes	Global configuration (config)	
	Interface configuration (config-if)	
Command History	Release	Modification
	Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Usage Guidelines

Use the **avb** command in global configuration mode to enable AVB on the device.

Use the **avb** command in interface configuration mode to configure the interfaces, along the connectivity path, for AVB devices as dot1q trunk ports.

Example

This example shows how to enable AVB in global configuration mode:

```
Device> enable
Device# configure terminal
Device(config)# avb
```

This example shows how to enable AVB in interfaceconfiguration mode:

```
Device> enable
Device# configure terminal
Device(config)# interface te1/1/1
Device(config-if)# switchport mode trunk
Device(config-if)# exit
Device(config)# vlan 2
Device(config)# avb vlan 10
Device(config-vlan)# avb
```

avb vlan

To set a specified VLAN as the default AVB VLAN, use the **avb vlan** command in global configuration mode.

avb vlan *vlan-id*

Syntax Description	<i>vlan-id</i> The range for vlan-id varies from 2 to 4094.	
Command Default	VLAN 2 is the default AVB VLAN.	
Command Modes	Global configuration (config)	
Command History	Release	Modification
	Cisco IOS XE Fuji 16.8.1a	This command was introduced.
Usage Guidelines	Use this command when you need to set the default AVB VLAN other than VLAN 2.	

Example

This example shows how set a specified VLAN as the default AVB VLAN:

```
Device> enable
Device# configure terminal
Device(config)# interface tel1/1/1
Device(config-if)# switchport mode trunk
Device(config-if)# exit
Device(config)# vlan 2
Device(config)# avb vlan 10
```

channel-group

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

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

Syntax Description

<i>channel-group-number</i>	Channel group number. The range is 1 to 128.
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 Everest 16.5.1a	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

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

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

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

**Caution**

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

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

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

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

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

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

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



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

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

```
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 switch 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 switch stack. It uses LACP passive mode and assigns two ports on stack member 2 and one port on stack member 3 as static-access ports in VLAN 10 to channel 5:

```
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 Everest 16.5.1a	This command was introduced.
Usage Guidelines	<p>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 command in interface configuration mode.</p> <p>You must use the channel-group command in interface configuration mode to configure the EtherChannel parameters. The channel-group command also can set the mode for the EtherChannel.</p> <p>You cannot enable both the PAgP and LACP modes on an EtherChannel group.</p> <p>PAgP and LACP are not compatible; both ends of a channel must use the same protocol.</p> <p>You cannot configure PAgP on cross-stack configurations.</p> <p>This example shows how to specify LACP as the protocol that manages the EtherChannel:</p> <pre>Device> enable Device# configure terminal Device(config)# interface gigabitethernet2/0/1 Device(config-if)# channel-protocol lacp</pre> <p>You can verify your settings by entering the show etherchannel [<i>channel-group-number</i>] protocol command in privileged EXEC mode.</p>	

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	<div> <div><i>channel-group-number</i></div> <div>(Optional) Channel group number.</div> <div>The range is 1 to 128.</div> </div>	
	<div> <div>counters</div> <div>Clears traffic counters.</div> </div>	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Usage Guidelines	<p>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 <i>channel-group-number</i> counters command.</p> <p>This example shows how to clear all channel-group information:</p> <pre>Device> enable Device# clear lacp counters</pre> <p>This example shows how to clear LACP traffic counters for group 4:</p> <pre>Device> enable Device# clear lacp 4 counters</pre> <p>You can verify that the information was deleted by entering the show lacp counters or the show lacp <i>channel-group-number</i> counters command in privileged EXEC mode.</p>	

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	<table> <tr> <td data-bbox="380 501 641 537"><i>channel-group-number</i></td><td data-bbox="657 501 1528 590">(Optional) Channel group number. The range is 1 to 128.</td></tr> <tr> <td data-bbox="380 604 487 640">counters</td><td data-bbox="657 604 1528 640">Clears traffic counters.</td></tr> </table>	<i>channel-group-number</i>	(Optional) Channel group number. The range is 1 to 128.	counters	Clears traffic counters.
<i>channel-group-number</i>	(Optional) Channel group number. The range is 1 to 128.				
counters	Clears traffic counters.				
Command Modes	Privileged EXEC				
Command History	<table> <tr> <th data-bbox="380 764 487 800">Release</th><th data-bbox="1149 764 1292 800">Modification</th></tr> <tr> <td data-bbox="380 821 714 856">Cisco IOS XE Everest 16.5.1a</td><td data-bbox="1149 821 1487 856">This command was introduced.</td></tr> </table>	Release	Modification	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.5.1a	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 <i>channel-group-number</i> counters command.</p> <p>This example shows how to clear all channel-group information:</p> <pre>Device> enable Device# clear pagp counters</pre> <p>This example shows how to clear PAgP traffic counters for group 10:</p> <pre>Device> enable Device# clear pagp 10 counters</pre> <p>You can verify that the information was deleted by entering the show pagp command in privileged EXEC mode.</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	<p>interface <i>interface-id</i></p> <p>(Optional) Clears all spanning-tree counters on the specified interface. The command includes physical ports, VLANs, and port channels.</p> <p>The VLAN range is 1 to 4094.</p> <p>The port channel range is 1 to 128.</p>	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	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> enable 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 channels. The VLAN range is 1 to 4094. The port channel range is 1 to 128.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Usage Guidelines	<p>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).</p> <p>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.</p> <p>This example shows how to restart the protocol migration process on a port:</p> <pre>Device> enable Device# clear spanning-tree detected-protocols interface gigabitethernet2/0/1</pre>	

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 Everest 16.5.1a	This command was introduced.

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



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

This example shows how to display all EtherChannel debug messages:

```
Device> enable
Device# debug etherchannel all
```

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

```
Device> enable
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 Everest 16.5.1a	This command was introduced.

Usage Guidelines

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

This example shows how to display all LACP debug messages:

```
Device> enable
Device# debug LACP all
```

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

```
Device> enable
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 Everest 16.5.1a	This command was introduced.

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

This example shows how to display all PAgP debug messages:

```
Device> enable
Device# debug pagp all
```

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

```
Device> enable
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-vectors [detail] | ses | vlans}
no debug platform pm {all | counters | errdisable | fec | if-numbers | l2-control | link-status | platform | 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-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.
	vlans	Displays VLAN creation and deletion event debug messages.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

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

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

```
Device> enable
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 Everest 16.5.1a	This command was introduced.
Usage Guidelines	<p>The undebug platform udd command is the same as the no debug platform udd 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 command in privileged EXEC mode. 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 switch shim command debug messages. This shim is the software module that is the interface between the generic Spanning Tree Protocol (STP) code and the platform-specific code of various 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 Everest 16.5.1a	This command was introduced.

Usage Guidelines The **undebbug 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> enable
Device# debug spanning-tree all
```

instance (VLAN)

To map a VLAN or a group of VLANs to a multiple spanning tree (MST) instance, use the **instance** command in MST configuration mode. To return the VLANs to the default internal spanning tree (CIST) instance, use the **no** form of this command.

instance *instance-id* **vlan**s *vlan-range*
no instance *instance-id*

Syntax Description	<i>instance-id</i>	Instance to which the specified VLANs are mapped. The range is from 0 to 4094.
	vlan s <i>vlan-range</i>	Specifies the number of the VLANs to be mapped to the specified instance. The range is from 1 to 4094.

Command Default No VLANs are mapped to any MST instance (all VLANs are mapped to the CIST instance).

Command Modes MST configuration mode (config-mst)

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

The **vlan**s *vlan-range* is entered as a single value or a range.

The mapping is incremental, not absolute. When you enter a range of VLANs, this range is added or removed to the existing instances.

Any unmapped VLAN is mapped to the CIST instance.

Examples

The following example shows how to map a range of VLANs to instance 2:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# instance 2 vlans 1-100
Device(config-mst)#
```

The following example shows how to map a VLAN to instance 5:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# instance 5 vlans 1100
Device(config-mst)#
```

The following example shows how to move a range of VLANs from instance 2 to the CIST instance:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# no instance 2 vlans 40-60
Device(config-mst)#
```

The following example shows how to move all the VLANs that are mapped to instance 2 back to the CIST instance:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# no instance 2
Device(config-mst)#
```

Related Commands

Command	Description
name (MST configuration mode)	Sets the name of an MST region.
revision	Sets the revision number for the MST configuration.
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree mst configuration	Enters MST configuration mode.

interface port-channel

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

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

Syntax Description	<div> <div>port-channel-number</div> <div>Channel group number.</div> <div>The range is 1 to 128.</div> </div>	
Command Default	No port channel logical interfaces are defined.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Usage Guidelines	<p>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 command in interface configuration mode, 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 <i>channel-group-number</i> can be the same as the <i>port-channel-number</i>, or you can use a new number. If you use a new number, the channel-group command dynamically creates a new port channel.</p> <p>You create Layer 3 port channels by using the interface port-channel command followed by the no switchport command in interface configuration mode. You should manually configure the port-channel logical interface before putting the interface into the channel group.</p> <p>Only one port channel in a channel group is allowed.</p> <div> <div>⚠</div> <div> <div>Caution</div> <div>When using a port-channel interface as a routed port, do not assign Layer 3 addresses on the physical ports that are assigned to the channel group.</div> </div> </div> <div> <div>⚠</div> <div> <div>Caution</div> <div>Do not assign bridge groups on the physical ports in a channel group used as a Layer 3 port channel interface because it creates loops. You must also disable spanning tree.</div> </div> </div>	

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> enable
Device# configure terminal
Device(config)# interface port-channel 5
```

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

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 Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	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** command in privileged EXEC mode 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> enable
Device# configure terminal
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	<i>priority</i> Port priority for LACP. The range is 1 to 65535.				
Command Default	The default is 32768.				
Command Modes	Interface configuration				
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>Cisco IOS XE Everest 16.5.1a</td><td>This command was introduced.</td></tr> </table>	Release	Modification	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.5.1a	This command was introduced.				

Usage Guidelines

The **lacp port-priority** command in interface configuration mode 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** command in global configuration mode for determining which device controls the link.

Use the **show lacp internal** command in privileged EXEC mode 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> enable
Device# configure terminal
Device(config)# 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** command in privileged EXEC mode.

lACP rate

To set the rate at which Link Aggregation Control Protocol (LACP) control packets are ingressed 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 ingressed at the normal rate, every 30 seconds after the link is bundled.				
	fast Specifies that LACP control packets are ingressed 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				
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>Cisco IOS XE Everest 16.5.1a</td><td>This command was introduced.</td></tr></table>	Release	Modification	Cisco IOS XE Everest 16.5.1a	This command was introduced.
	Release	Modification			
Cisco IOS XE Everest 16.5.1a	This command was introduced.				
Usage Guidelines	<p>Use this command to modify the duration of LACP timeout. The LACP timeout value on Cisco switch is three times the LACP rate that is 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.</p> <p>This command is supported only on LACP-enabled interfaces.</p> <p>This example shows how to specify the fast (1 second) ingress rate on interface GigabitEthernet 0/0:</p> <pre>Device> enable Device# configure terminal Device(config)# interface gigabitEthernet 0/0 Device(config-if)# lACP rate fast</pre>				

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	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>Cisco IOS XE Everest 16.5.1a</td><td>This command was introduced.</td></tr> </table>	Release	Modification	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.5.1a	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** command in privileged EXEC mode 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> enable
Device# configure terminal
Device(config)# lacp system-priority 20000
```

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

mvrp vlan creation

To enable dynamic VLAN creation on a device using Multiple VLAN Registration Protocol (MVRP), use the **mvrpvlancreation** command in global configuration mode. To disable dynamic VLAN creation for MVRP, use the **no** form of this command.

mvrp vlan creation
no mvrp vlan creation

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

Command Default	MVRP is disabled.
------------------------	-------------------

Command Modes	Global configuration (config)
----------------------	-------------------------------

Command History	Release	Modification
	Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Usage Guidelines	MVRP dynamic VLAN creation can be used only if Virtual Trunking Protocol (VTP) is in transparent mode.
-------------------------	--

Examples

The following example shows a command sequence enabling MVRP dynamic VLAN creation. Notice that the device recognizes that the VTP mode is incorrect and rejects the request for dynamic VLAN creation. Once the VTP mode is changed, MVRP dynamic VLAN creation is allowed.

```
Device(config)# mvrp vlan creation
%Command Rejected: VTP is in non-transparent (server) mode.
Device(config)# vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Device(config)# mvrp vlan creation
%VLAN now may be dynamically created via MVRP/
```

Related Commands	Command	Description
	mvrp global	Enables MVRP globally on a device.
	vtp mode	Sets the mode for VTP mode on the device.

mvrp registration

To set the registrars in a Multiple Registration Protocol (MRP) Attribute Declaration (MAD) instance associated with an interface, use the **mvrpregistration** command in global configuration mode. To disable the registrars, use the **no** form of this command.

mvrp registration {normal | fixed | forbidden}
no mvrp registration

Syntax Description

normal	Registrar responds normally to incoming Multiple VLAN Registration Protocol (MVRP) messages. Normal is the default state.
fixed	Registrar ignores all incoming MVRP messages and remains in the IN state.
forbidden	Registrar ignores all incoming MVRP messages and remains in the EMPTY (MT) state.

Command Default

Registrars are set to the normal state.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Usage Guidelines

The **mvrpregistration** command is operational only if MVRP is configured on an interface.

The **nomvrpregistration** command sets the registrar state to the default (normal).

This command can be used to set the registrar in a MAD instance associated with an interface to one of the three states. This command is effective only if MVRP is operational on the interface.

Given that up to 4094 VLANs can be configured on a trunk port, there may be up to 4094 Advanced Services Module (ASM) and Route Switch Module (RSM) pairs in a MAD instance associated with that interface.

Examples

The following example sets a fixed, forbidden, and normal registrar on a MAD instance:

```
Device(config)# mvrp global
%MVRP is now globally enabled. MVRP is operational on IEEE 802.1q trunk ports only.
Device(config)# interface fastethernet2/1
Device(config-if)# mvrp registration fixed
Device(config-if)# interface fastethernet2/2
Device(config-if)# mvrp registration forbidden
Device(config-if)# interface fastethernet2/3
Device(config-if)# no mvrp registration
```

Related Commands

Command	Description
clear mvrp statistics	Clears MVRP-related statistics recorded on one or all MVRP-enabled ports.

Command	Description
debug mvrp	Displays MVRP debugging information.
mvrp global	Enables MVRP globally on a device and on a particular interface.
mvrp mac-learning auto	Enables automatic learning of MAC table entries by MVRP.
mvrp timer	Sets period timers that are used in MRP on a given interface.
mvrp vlan create	Enables an MVRP dynamic VLAN.
show mvrp interface	Displays details of the administrative and operational MVRP states of all or one particular IEEE 802.1Q trunk port in the device.
show mvrp summary	Displays the MVRP configuration at the device level.

mvrp timer

To set period timers that are used in Multiple VLAN Registration Protocol (MVRP) on a given interface, use the **mvrp timer** command in interface configuration mode. To remove the timer value, use the **no** form of this command.

mvrp timer {**join** | **leave** | **leave-all** | **periodic**} [*centiseconds*]
no mvrp timer

Syntax Description

join	Specifies the time interval between two transmit opportunities that are applied to the Applicant State Machine (ASMs).
leave	Specifies the duration time before a registrar is moved to EMPTY (MT) state from leave-all (LV) state.
leave-all	Specifies the time it takes for a LeaveAll timer to expire.
periodic	Sets the timer value to periodic, a fixed value of 100 centiseconds.
<i>centiseconds</i>	Timer value measured in centiseconds. <ul style="list-style-type: none"> Join timer value range is 20 to 10000000. Leave timer value range is 60 to 10000000. LeaveAll timer value range is 10000 and 10000000. Periodic timer value is fixed at 100 centiseconds.

Command Default

Join timer value: 20 centiseconds
Leave timer value: 60 centiseconds
LeaveAll timer value: 10000 centiseconds

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Usage Guidelines

The **nomvrptimer** command resets the timer value to the default value.

Examples

The following example sets the timer levels on an interface:

```
Device(config)# mvrp global
%MVRP is now globally enabled. MVRP is operational on IEEE 802.1q trunk ports.
Device(config)# interface GigabitEthernet 6/1
Device(config-if)# mvrp timer join 30
Device(config-if)# mvrp timer leave 70
Device(config-if)# mvrp timer leaveAll 15000
```


Related Commands

Command	Description
clear mvrp statistics	Clears MVRP-related statistics recorded on one or all MVRP enabled ports.
debug mvrp	Displays MVRP debugging information.
mvrp global	Enables MVRP globally on a device and on a particular interface.
mvrp mac-learning auto	Enables automatic learning of MAC table entries by MVRP.
mvrp registration	Sets the registrars in a MAD instance associated with an interface.
mvrp vlan create	Enables an MVRP dynamic VLAN.
show mvrp interface	Displays details of the administrative and operational MVRP states of all or one particular IEEE 802.1q trunk port in the device.
show mvrp summary	Displays the MVRP configuration at the device level.

name (MST)

To set the name of a Multiple Spanning Tree (MST) region, use the **name** command in MST configuration submode. To return to the default name, use the **no** form of this command.

name *name*

no name *name*

Syntax Description

name	Name to give the MST region. It can be any string with a maximum length of 32 characters.
------	---

Command Modes

MST configuration (config-mst)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

Two or more devices with the same VLAN mapping and configuration version number are considered to be in different MST regions if the region names are different.



Note Be careful when using the **name** command to set the name of an MST region. If you make a mistake, you can put the device in a different region. The configuration name is a case-sensitive parameter.

Examples

This example shows how to name a region:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# name Cisco
Device(config-mst)#
```

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
revision	Sets the revision number for the MST configuration.
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree mst configuration	Enters MST configuration submode.

no ptp enable

To disable PTP on an interface, use the **no ptp enable** command in interface configuration mode.

To re-enable PTP on the same interface, use the **ptp enable** command in interface configuration mode.

no ptp enable
ptp enable

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

Command Default	PTP is enabled on all the ports, by default.
------------------------	--

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

Command History	Release	Modification
	Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Examples

This example shows how to disable PTP on an interface:

```
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# no ptp enable
```

Related Commands

Command	Description
ptp (interface)	Configures PTP on interfaces.
ptp profile dot1as	Enables Generalized Precision Time Protocol (gPTP) globally.

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 Everest 16.5.1a	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** commands in interface configuration mode 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** command in interface configuration mode. 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** command in global configuration mode. Use the **pagp learn-method** command in interface configuration mode 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> enable
Device# configure terminal
Device(config)# interface port-channel 2
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> enable
Device# configure terminal
```

```
Device(config)# interface port-channel 2  
Device(config-if)# pagp learn-method aggregation-port
```

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

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	priority 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 Everest 16.5.1a	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** commands in interface configuration mode 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** command in interface configuration mode. 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** command in global configuration mode. Use the **pagp learn-method** command in interface configuration mode only in this situation.

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

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# pagp port-priority 200
```

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

policy-map

To enter policy-map configuration mode and create or modify a policy map that can be attached to one or more interfaces to specify a service policy, use the **policy-map** command in global configuration mode. To delete a policy map, use the **no** form of this command.

policy-map [**type** { **access-control** | **control subscriber** | **packet-service** | **performance-monitor** }] *policy-map name*

Syntax Description	type	(Optional) Specifies the policy-map type.
	access-control	(Optional) Enables the access-control specific policy map.
	control subscriber	(Optional) Enables subscriber control policy domain.
	packet-service	(Optional) Enables packet service policy map.
	performance-monitor	(Optional) Enables policy map for the performance monitoring feature.
	<i>policy-map name</i>	Specifies the policy map.
Command Default	The policy map is not configured.	
Command History	Release	Modification
	Cisco IOS XE Fuji 16.8.1a	This command was introduced.
Command Modes	Global configuration (config)	
Usage Guidelines	Use the policy-map command to specify the name of the policy map to create (add or modify) before you configure policies for classes whose match criteria are defined in a class map with the class-map and match commands.	



Note You can configure class policies in a policy map only if the classes have match criteria defined for them.



Note Because you can configure a maximum of 64 class maps, a policy map cannot contain more than 64 class policies.

A single policy map can be attached concurrently to more than one interface. Except as noted, when you attempt to attach a policy map to an interface, the attempt is denied if the available bandwidth on the interface cannot accommodate the total bandwidth requested by the multiple policies. In such cases, if the policy map is already attached to other interfaces, the map is removed.

Example:

The following is sample output from the **policy-map** command:

```
Device# policy-map AVB-Output-Child-Policy

policy-map AVB-Output-Child-Policy
  class VOIP-PRIORITY-QUEUE
    bandwidth remaining percent 30
    queue-buffers ratio 10
  class MULTIMEDIA-CONFERENCING-STREAMING-QUEUE
    bandwidth remaining percent 15
    queue-limit dscp AF41 percent 80
    queue-limit dscp AF31 percent 80
    queue-limit dscp AF42 percent 90
    queue-limit dscp AF32 percent 90
    queue-buffers ratio 10
  class TRANSACTIONAL-DATA-QUEUE
    bandwidth remaining percent 15
    queue-limit dscp AF21 percent 80
    queue-limit dscp AF22 percent 90
    queue-buffers ratio 10
  class BULK-SCAVENGER-DATA-QUEUE
    bandwidth remaining percent 15
    queue-limit dscp AF11 percent 80
    queue-limit dscp AF12 percent 90
    queue-limit dscp CS1 percent 80
    queue-buffers ratio 15
  class class-default
    bandwidth remaining percent 25
    queue-buffers ratio 25
```


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 Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines You can use the **show etherchannel summary** command in privileged EXEC mode to display the EtherChannel information.

Examples

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

```
Device> enable
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

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 Everest 16.5.1a	This command was introduced.
Usage Guidelines	You can use the show etherchannel auto command in privileged EXEC mode to verify if the EtherChannel was created automatically.	
Examples	<p>This example shows how to enable the auto-LAG feature on the switch:</p> <pre>Device> enable Device# configure terminal Device(config)# port-channel auto</pre>	

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** | **vlan-dst-ip** | **vlan-dst-mixed-ip-port** | **vlan-src-dst-ip** | **vlan-src-dst-mixed-ip-port** | **vlan-src-ip** | **vlan-src-mixed-ip-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.
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.
vlan-dst-ip		Specifies load distribution based on the VLAN ID and destination IP address.

vlan-dst-mixed-ip-port	Specifies load distribution based on the VLAN ID, destination IP address, and TCP/UDP port number.
vlan-src-dst-ip	Specifies load distribution based on the VLAN ID, source and destination IP address.
vlan-src-dst-mixed-ip-port	Specifies load distribution based on the VLAN ID, source and destination IP address, and TCP/UDP port number.
vlan-src-ip	Specifies load distribution based on the VLAN ID and source IP address.
vlan-src-mixed-ip-port	Specifies load distribution based on the VLAN ID, source IP address, and TCP/UDP port number.

Command Default

The default for Cisco Catalyst 9500 Series Switches is **src-mac**

The default for Cisco Catalyst 9500 High Performance Series Switches is **src-dst-mixed-ip-port**

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.
Cisco IOS XE Gibraltar 16.11.1	This command was modified. The VLAN-based load balancing keywords vlan-dst-ip , vlan-dst-mixed-ip-port , vlan-src-dst-ip , vlan-src-dst-mixed-ip-port , vlan-src-ip , and vlan-src-mixed-ip-port were added on Cisco Catalyst 9500H switches.

Usage Guidelines

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



Note The VLAN-based load balancing keywords **vlan-dst-ip**, **vlan-dst-mixed-ip-port**, **vlan-src-dst-ip**, **vlan-src-dst-mixed-ip-port**, **vlan-src-ip**, and **vlan-src-mixed-ip-port** are supported only on Cisco Catalyst 9500H switches.

Examples

The following example shows how to set the load-distribution method to dst-mac:

```
Device> enable
Device# configure terminal
Device(config)# port-channel load-balance dst-mac
```

Related Commands

Command	Description
show etherchannel load-balance	Displays information about EtherChannel load balancing.
show running-config	Displays the running configuration.

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. This keyword is supported only on Cisco Catalyst 9500 Series Switches.
l3-proto	(Optional) Specifies load distribution based on the source MAC address and Layer 3 protocols. This keyword is supported only on Cisco Catalyst 9500 Series Switches.
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 Everest 16.5.1a	This command was introduced.

Usage Guidelines

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

Examples

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

```
Device> enable
Device# configure terminal
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 Modes	Interface configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Usage Guidelines	<p>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.</p> <p>The port-channel min-links command must specify a number a less than the number specified by the lacp max-bundle command.</p> <p>Use the show etherchannel summary command in privileged EXEC mode to see which ports are in the hot-standby mode (denoted with an H port-state flag in the output display).</p> <p>This example shows how to specify a minimum of three active LACP ports before port channel 2 becomes active:</p> <pre>Device> enable Device# configure terminal Device(config)# interface port-channel 2 Device(config-if)# port-channel min-links 3</pre>	

ptp priority1 value

To specify the priority 1 value to use when advertising a PTP clock, use the **ptp priority1 value** command in global configuration mode.

ptp priority1 *value*

Syntax Description	value	Specifies the priority 1 number to use for this clock. The range is 0 to 255. The default value is 128.
	Note	If the value of priority1 is configured to 255, the clock cannot become as Grandmaster.
Command Default	Default is 128.	
Command Modes	Global configuration (config)	
Command History	Release	Modification
	Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Example

This example shows how to specify the priority1 value:

```
Device> enable
Device# configure terminal
Device(config)# ptp priority1 120
```

Related Commands	Command	Description
	ptp priority2 value	Specifies the priority 2 number to use for this clock.
	no ptp enable	Disables PTP on an interface.
	ptp profile dot1as	Enables Generalized Precision Time Protocol (gPTP) globally.

ptp priority2 value

To specify the priority 2 number to use when advertising a PTP clock, use the **ptp priority2 value** command in global configuration mode.

ptp priority2 *value*

Syntax Description	value Specifies the priority 2 number to use for this clock. The range is 0 to 255. The default value is 128.
---------------------------	---

Command Default	Default is 128.
------------------------	-----------------

Command Modes	Global configuration (config)
----------------------	-------------------------------

Command History	Release	Modification
	Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Example

This example shows how to specify the priority2 value:

```
Device> enable
Device# configure terminal
Device(config)# ptp priority 2 120
```

Related Commands	Command	Description
	ptp priority1 value	Specifies the priority 1 number to use for this clock.
	no ptp enable	Disables PTP on an interface.
	ptp profile dot1as	Enables Generalized Precision Time Protocol (gPTP) globally.

ptp profile dot1as

To enable Generalized Precision Time Protocol (gPTP) globally, use the **ptp profile dot1as** command in global configuration mode. To disable gPTP, use the **no** form of the command.

ptp profile dot1as
no ptp profile dot1as

Command Default

PTP is disabled on interfaces.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Examples

This example shows how to enable gPTP:

```
Device> enable
Device# configure terminal
Device(config)# ptp profile dot1as
```

Related Commands

Command	Description
ptp (interface)	Configures PTP on interfaces.
no ptp enable	Disables PTP on an interface.

rep admin vlan

To configure a Resilient Ethernet Protocol (REP) administrative VLAN for the 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	<i>vlan-id</i> 48-bit static MAC address.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Usage Guidelines	<p>The range of the REP administrative VLAN is from 1 to 4094.</p> <p>There can be only one administrative VLAN on a device and on a segment.</p> <p>Verify your settings by entering the show interfaces rep detail command in privileged EXEC mode.</p>	
Examples	<p>The following example shows how to configure VLAN 100 as the REP administrative VLAN:</p> <pre>Device> enable Device# configure terminal Device(config)# rep admin vlan 100</pre>	
Related Commands	Command	Description
	show interfaces rep detail	Displays detailed REP configuration and status for all the interfaces or the specified interface, including the administrative VLAN.

rep block port

To configure Resilient Ethernet Protocol (REP) VLAN load balancing on a 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 <i>port-id</i>	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.
<i>neighbor-offset</i>	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, and 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 the 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

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

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.



Note 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 the 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.

Examples

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

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

Related Commands

Command	Description
show interfaces rep detail	Displays detailed REP configuration and status for all the interfaces or the specified interface, including the administrative VLAN.

rep lsl-age-timer

To configure the Resilient Ethernet Protocol (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 to 10000 in multiples of 40.
---------------------------	---

Command Default	The default LSL age-out timer value is 5 ms.
------------------------	--

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

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines	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.
-------------------------	--

Examples

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

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

Related Commands	Command	Description
	interface interface-type interface-name	Specifies a physical interface or port channel to receive STCNs.
	rep segment	Enables REP on an interface and assigns a segment ID.

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

number-of-retries 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

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	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> enable
Device# configure terminal
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 Resilient Ethernet Protocol (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	<i>seconds</i> 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	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Usage Guidelines	Enter this command on the REP primary edge port.	
	Enter this command and configure a preempt time delay for VLAN load balancing to be automatically triggered 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 port alerts the alternate port to perform VLAN load balancing (configured by using the rep block port command in interface configuration mode) 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 command.	

Examples

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

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

Related Commands	Command	Description
	rep block port	Configures VLAN load balancing.
	show interfaces rep detail	Displays detailed REP configuration and status for all the interfaces or the specified interface, including the administrative VLAN.

rep preempt segment

To manually start Resilient Ethernet Protocol (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 Everest 16.5.1a	This command was introduced.

Usage Guidelines

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

Ensure that all the other segment configurations are 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.

Enter the **show rep topology** command in privileged EXEC mode to see which port in the segment is the primary edge port.

If you do not configure VLAN load balancing, entering the **rep preempt segment** *segment-id* command results in the default behavior, that is, the primary edge port blocks all the VLANs.

You can 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.

Examples

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

```
Device> enable
Device# rep preempt segment 100
```

Related Commands

Command	Description
rep block port	Configures VLAN load balancing.
rep preempt delay	Configures a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered.
show rep topology	Displays REP topology information for a segment or for all the segments.

rep segment

To enable Resilient Ethernet Protocol (REP) on an 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

<i>segment-id</i>	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 a preferred port 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

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

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

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

- If only one port on a device is configured in a segment, that port should be an edge port.
- If two ports on a device belong to the same segment, both the ports must be regular segment ports.
- If two ports on a device 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.



Caution

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 that port to be a regular segment port.

Examples

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

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

rep stcn

To configure a Resilient Ethernet Protocol (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 task of sending 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 <i>interface-id</i>	Specifies a physical interface or port channel to receive STCNs.
	segment <i>segment-id-list</i>	Specifies one REP segment or a list of REP 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	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Usage Guidelines	You can verify your settings by entering the show interfaces rep detail command in privileged EXEC mode.	
Examples	<p>The following example shows how to configure a REP edge port to send STCNs to segments 25 to 50:</p> <pre> Device> enable Device# configure terminal Device(config)# interface TenGigabitEthernet 4/1 Device(config-if)# rep stcn segment 25-50 </pre>	

revision

To set the revision number for the Multiple Spanning Tree (802.1s) (MST) configuration, use the **revision** command in MST configuration submenu. To return to the default settings, use the **no** form of this command.

revision *version*
no revision

Syntax Description

version	Revision number for the configuration; valid values are from 0 to 65535.
---------	--

Command Default

version is 0

Command Modes

MST configuration (config-mst)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

Devices that have the same configuration but different revision numbers are considered to be part of two different regions.



Note Be careful when using the **revision** command to set the revision number of the MST configuration because a mistake can put the switch in a different region.

Examples

This example shows how to set the revision number of the MST configuration:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# revision 5
Device(config-mst)#
```

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
name (MST configuration submenu)	Sets the name of an MST region.
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree mst configuration	Enters MST-configuration submenu.

show avb domain

To display the AVB domain information, use the **show avb domain** command.

show avb domain

Command History	Release	Modification
	Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Command Modes Global configuration mode (#)

Example:

The following is sample output from the **show avb domain** command:

Device# **show avb domain**

```

AVB Class-A
  Priority Code Point    : 3
  VLAN                  : 2
  Core ports            : 1
  Boundary ports        : 67

```

```

AVB Class-B
  Priority Code Point    : 2
  VLAN                  : 2
  Core ports            : 1
  Boundary ports        : 67

```

Interface	State	Delay	PCP	VID	Information
Te1/0/1	down	N/A			Oper state not up
Te1/0/2	down	N/A			Oper state not up
Te1/0/3	down	N/A			Oper state not up
Te1/0/4	down	N/A			Oper state not up
Te1/0/5	up	N/A			Port is not asCapable
Te1/0/6	down	N/A			Oper state not up
Te1/0/7	down	N/A			Oper state not up
Te1/0/8	down	N/A			Oper state not up
Te1/0/9	down	N/A			Oper state not up
Te1/0/10	down	N/A			Oper state not up
Te1/0/11	down	N/A			Oper state not up
Te1/0/12	down	N/A			Oper state not up
Te1/0/13	down	N/A			Oper state not up
Te1/0/14	down	N/A			Oper state not up
Te1/0/15	down	N/A			Oper state not up
Te1/0/16	down	N/A			Oper state not up
Te1/0/17	down	N/A			Oper state not up
Te1/0/18	down	N/A			Oper state not up
Te1/0/19	up	N/A			Port is not asCapable
Te1/0/20	down	N/A			Oper state not up
Te1/0/21	down	N/A			Oper state not up
Te1/0/22	down	N/A			Oper state not up
Te1/0/23	up	N/A			Port is not asCapable
Te1/0/24	down	N/A			Oper state not up
Te1/0/25	down	N/A			Oper state not up
Te1/0/26	down	N/A			Oper state not up

```

Tel/0/27      down      N/A      Oper state not up
Tel/0/28      down      N/A      Oper state not up
Tel/0/29      up        N/A      Port is not asCapable
Tel/0/30      down      N/A      Oper state not up
Tel/0/31      down      N/A      Oper state not up
Tel/0/32      down      N/A      Oper state not up
Tel/0/33      down      N/A      Oper state not up
Tel/0/34      down      N/A      Oper state not up
Tel/0/35      up        N/A      Port is not asCapable
Tel/0/36      down      N/A      Oper state not up
Tel/0/37      down      N/A      Oper state not up
Tel/0/38      down      N/A      Oper state not up
Tel/0/39      up        507ns
Class- A      core      3      2
Class- B      core      2      2
Tel/0/40      down      N/A      Oper state not up
Tel/0/41      down      N/A      Oper state not up
Tel/0/42      down      N/A      Oper state not up
Tel/0/43      down      N/A      Oper state not up
Tel/0/44      down      N/A      Oper state not up
Tel/0/45      down      N/A      Oper state not up
Tel/0/46      down      N/A      Oper state not up
Tel/0/47      down      N/A      Oper state not up
Tel/0/48      down      N/A      Oper state not up
Tel/1/1       down      N/A      Oper state not up
Tel/1/2       down      N/A      Oper state not up
Tel/1/3       down      N/A      Oper state not up
Tel/1/4       down      N/A      Oper state not up
Tel/1/5       down      N/A      Oper state not up
Tel/1/6       down      N/A      Oper state not up
Tel/1/7       down      N/A      Oper state not up
Tel/1/8       down      N/A      Oper state not up
Tel/1/9       down      N/A      Oper state not up
Tel/1/10      down      N/A      Oper state not up
Tel/1/11      down      N/A      Oper state not up
Tel/1/12      down      N/A      Oper state not up
Tel/1/13      down      N/A      Oper state not up
Tel/1/14      down      N/A      Oper state not up
Tel/1/15      down      N/A      Oper state not up
Tel/1/16      down      N/A      Oper state not up
Fol/1/1       down      N/A      Oper state not up
Fol/1/2       down      N/A      Oper state not up
Fol/1/3       down      N/A      Oper state not up
Fol/1/4       down      N/A      Oper state not up
.
.
.

```

show avb streams

To display the AVB stream information, use the **show avb streams** command.

show avb streams

Command History	Release	Modification
	Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Command Modes Global configuration mode (#)

Example:

The following is sample output from the **show avb streams** command:

```
Device# show avb streams

Stream ID:      0011.0100.0001:1      Incoming Interface:  Tel/1/1
Destination   : 91E0.F000.FE00
Class          : A
Rank           : 1
Bandwidth      : 6400 Kbit/s

Outgoing Interfaces:
-----
Interface      State      Time of Last Update      Information
-----
Tel/1/1        Ready      Tue Apr 26 01:25:40.634

Stream ID:      0011.0100.0002:2      Incoming Interface:  Tel/1/1
Destination   : 91E0.F000.FE01
Class          : A
Rank           : 1
Bandwidth      : 6400 Kbit/s

Outgoing Interfaces:
-----
Interface      State      Time of Last Update      Information
-----
Tel/1/1        Ready      Tue Apr 26 01:25:40.634

.
.
.
```


show etherchannel

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

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

Syntax Description	<i>channel-group-number</i>	(Optional) Channel group number. The range is 1 to 128.
	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 Modes	User EXEC
---------------	-----------

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

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

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

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    =           PoIGC = -              Pseudo port-channel = Po1
Port index      =           OLoad = 0x00            Protocol = LACP
```

show etherchannel

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 Priority	Admin Key	Oper Key	Port Number	Port 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	Gil/0/1	Active	0
0	00	Gil/0/2	Active	0

Time since last port bundled: 01d:20h:24m:44s Gil/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 Resilient Ethernet Protocol (REP) configuration and status for all interfaces or a 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

interface-id (Optional) Physical interface used to display the port ID.

Command Modes

Privileged EXEC

Command History

Release

Cisco IOS XE Everest 16.5.1a

Modification

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** command in privileged EXEC mode.

Examples

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

```
Device> enable
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
```

Related Commands

Command	Description
rep admin vlan	Configures a REP administrative VLAN for the REP to transmit HFL messages.

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 Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	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
          LACPDUs      Marker      Marker Response      LACPDUs
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
LACPDUs Sent and Recv	The number of LACP packets sent and received by a port.
Marker Sent and Recv	The number of LACP marker packets sent and received by a port.

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

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

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

Channel group 1

Port	Flags	State	LACP port Priority	Admin Key	Oper Key	Port Number	Port 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. • bndl—Port is attached to an aggregator and bundled with other ports. • susp—Port is in a suspended state; it is not attached to any aggregator. • hot-sby—Port is in a hot-standby state. • indiv—Port is incapable of bundling with any other port. • indep—Port is in an independent state (not bundled but able to handle data traffic. In this case, LACP is not running on the partner port). • down—Port is down.
LACP Port Priority	Port priority setting. LACP uses the port priority to put ports in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

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

```
Partner's information:
```

	Partner	Partner	Partner
Port	System ID	Port Number	Age
Gi2/0/2	32768,0007.eb49.5e80	0xD	15s
	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 msrp port bandwidth

To display Multiple Stream Reservation Protocol (MSRP) port bandwidth information, use the **show msrp port bandwidth** command.

show msrp port bandwidth

Command History

Release

Modification

Cisco IOS XE Fuji 16.8.1a

This command was introduced.

Command Modes

Global configuration mode (#)

Example:

The following is sample output from the **show msrp port bandwidth** command:

Device# **show msrp port bandwidth**

Ethernet Interface	Capacity (Kbit/s)	Assigned		Available		Reserved	
		A	B	A	B	A	B
Tel/0/1	10000000	75	0	75	75	0	0
Tel/0/2	10000000	75	0	75	75	0	0
Tel/0/3	10000000	75	0	75	75	0	0
Tel/0/4	10000000	75	0	75	75	0	0
Tel/0/5	10000000	75	0	75	75	0	0
Tel/0/6	10000000	75	0	75	75	0	0
Tel/0/8	10000000	75	0	75	75	0	0
Tel/0/9	10000000	75	0	75	75	0	0
Tel/0/10	10000000	75	0	75	75	0	0
Tel/0/11	10000000	75	0	75	75	0	0
Tel/0/12	10000000	75	0	75	75	0	0
Tel/0/13	10000000	75	0	75	75	0	0
Tel/0/14	10000000	75	0	75	75	0	0
Tel/0/15	10000000	75	0	75	75	0	0
Tel/0/16	10000000	75	0	75	75	0	0
Tel/0/17	10000000	75	0	75	75	0	0
Tel/0/18	10000000	75	0	75	75	0	0
Tel/0/19	10000000	75	0	75	75	0	0
Tel/0/20	10000000	75	0	75	75	0	0
Tel/0/21	10000000	75	0	75	75	0	0
Tel/0/22	10000000	75	0	75	75	0	0
Tel/0/23	10000000	75	0	75	75	0	0
Tel/0/24	10000000	75	0	75	75	0	0
Gi1/1/1	10000000	75	0	75	75	0	0
Gi1/1/2	10000000	75	0	75	75	0	0
Gi1/1/3	10000000	75	0	75	75	0	0
Gi1/1/4	10000000	75	0	75	75	0	0
Tel/1/1	10000000	75	0	75	75	0	0
Tel/1/2	10000000	75	0	75	75	0	0
Tel/1/3	10000000	75	0	75	75	0	0
Tel/1/4	10000000	75	0	75	75	0	0
Tel/1/5	10000000	75	0	75	75	0	0
Tel/1/6	10000000	75	0	75	75	0	0
Tel/1/7	10000000	75	0	75	75	0	0
Tel/1/8	10000000	75	0	75	75	0	0
Fo1/1/1	40000000	75	0	75	75	0	0

show msrp port bandwidth

Fe1/1/2	40000000	75 0	75 75	0 0
---------	----------	--------	---------	-------

show msrp streams

To display information about the Multiple Stream Reservation Protocol (MSRP) streams, use the **show msrp streams** command.

show msrp streams [**detailed** | **brief**]

Syntax Description	detailed	Displays detailed MSRP stream information.
	brief	Displays MSRP stream information in brief.
Command History	Release	Modification
	Cisco IOS XE Fuji 16.8.1a	This command was introduced.
Command Modes	Global configuration mode (#)	

Example:

The following is sample output from the **show msrp streams** command:

```
Device# show msrp streams
```

```
-----
Stream ID Talker Listener
Advertise Fail Ready ReadyFail AskFail
R | D R | D R | D R | D R | D
-----
yy:yy:yy:yy:yy:yy:0001 1 | 2 0 | 0 1 | 0 0 | 1 1 | 0
zz:zz:zz:zz:zz:zz:0002 1 | 0 0 | 1 1 | 0 0 | 0 0 | 1
```

The following is sample output from the **show msrp streams detailed** command:

```
Device# show msrp streams detailed
```

```
Stream ID:          0011.0100.0001:1
  Stream Age: 01:57:46 (since Mon Apr 25 23:41:11.413)
  Create Time: Mon Apr 25 23:41:11.413
  Destination Address: 91E0.F000.FE00
  VLAN Identifier: 1
  Data Frame Priority: 3 (Class A)
  MaxFrameSize: 100
  MaxIntervalFrames: 1 frames/125us
  Stream Bandwidth: 6400 Kbit/s
  Rank: 1
  Received Accumulated Latency: 20
  Stream Attributes Table:
  -----
  Interface          Attr State      Direction      Type
  -----
  Gi1/0/1            Register      Talker         Advertise
  Attribute Age: 01:57:46 (since Mon Apr 25 23:41:11.413)
  MRP Applicant: Very Anxious Observer, send None
  MRP Registrar: In
  Accumulated Latency: 20
  ----
```

show msrp streams

```

Tel1/1/1      Declare      Talker      Advertise
Attribute Age: 00:19:52 (since Tue Apr 26 01:19:05.525)
MRP Applicant: Quiet Active, send None
MRP Registrar: In
Accumulated Latency: 20
-----
Tel1/1/1      Register      Listener    Ready
Attribute Age: 00:13:17 (since Tue Apr 26 01:25:40.635)
MRP Applicant: Very Anxious Observer, send None
MRP Registrar: In
-----
Gi1/0/1      Declare      Listener    Ready
Attribute Age: 00:13:17 (since Tue Apr 26 01:25:40.649)
MRP Applicant: Quiet Active, send None
MRP Registrar: In

```

The following is sample output from the **show msrp streams brief** command:

Device# **show msrp streams brief**

Legend: R = Registered, D = Declared.

Stream ID	Destination Address	Bandwidth (Kbit/s)	Talkers R D	Listeners R D	Fail
0011.0100.0001:1	91E0.F000.FE00	6400	1 1	1 1	No
0011.0100.0002:2	91E0.F000.FE01	6400	1 1	1 1	No
0011.0100.0003:3	91E0.F000.FE02	6400	1 1	1 1	No
0011.0100.0004:4	91E0.F000.FE03	6400	1 1	1 1	No
0011.0100.0005:5	91E0.F000.FE04	6400	1 1	1 1	No
0011.0100.0006:6	91E0.F000.FE05	6400	1 1	1 1	No
0011.0100.0007:7	91E0.F000.FE06	6400	1 1	1 1	No
0011.0100.0008:8	91E0.F000.FE07	6400	1 1	1 1	No
0011.0100.0009:9	91E0.F000.FE08	6400	1 1	1 1	No
0011.0100.000A:10	91E0.F000.FE09	6400	1 1	1 1	No

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 Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	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              -p2             Gi3/0/3   N/A
Gi1/0/2   No              -p2             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 Interval	Partner Count	PAGP Priority	Learning Method	Group Ifindex
Gi1/0/1	SC	U6/S7	H	30s	1	128	Any	16
Gi1/0/2	SC	U6/S7	H	30s	1	128	Any	16

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

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

show platform etherchannel

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	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 hardware fed active vlan ingress

To display if native vlan tagging is enabled or disabled for a particular vlan, use the **show platform hardware fed active vlan ingress**

show platform hardware fed active vlan *vlan ID* ingress

Syntax Description

Syntax	Description
vlan <i>vlan ID</i>	Specifies the VLAN ID.
ingress	Specifies Spanning Tree Protocol (STP) state information in ingress direction.

Command Modes Privileged EXEC mode (#)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Example

The following is sample output from the **show platform hardware fed active vlan ingress** command:

```
Device# show platform hardware fed active vlan 1 ingress
VLAN STP State in hardware

vlan id is:: 1

Interfaces in forwarding state: : Hu1/0/45 (Tagged)

flood list: : Hu1/0/45
```


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**}

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.
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	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 platform software fed switch ptp

To display information about ptp status on the port, use the **show platform software fed switch ptp** command.

show platform software fed switch { *switch-number* | **active** | **standby** } **ptp** { **domain** *domain-value* | **if-id** *value* | **test** }

Syntax Description

switch <i>switch-number</i>	Displays information about the switch. Valid values for <i>switch-number</i> argument are from 0 to 9.
active	Displays information about the active instance of the switch.
standby	Displays information about the standby instance of the switch.
domain <i>domain-value</i>	Displays information about the specified domain.
if-id <i>value</i>	Displays information about the specified interface.
test	Executes ptp test

Command History

Release	Modification
Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Command Modes

Global configuration mode (#)

Example:

The following is sample output from the **show platform software fed switch active ptp if-id 0x20** command:

```
Device# show platform software fed switch active ptp if-id 0x20
```

```
Displaying port data for if_id 20
=====

Port Mac Address 04:6C:9D:4E:3A:9A
Port Clock Identity 04:6C:9D:FF:FE:4E:3A:80
Port number 28
PTP Version 2
domain_value 0
dotlas capable: FALSE
sync_recpt_timeout_time_interval 375000000 nanoseconds
sync_interval 125000000 nanoseconds
neighbor_rate_ratio 0.000000
neighbor_prop_delay 0 nanoseconds
compute_neighbor_rate_ratio: TRUE
compute_neighbor_prop_delay: TRUE
port_enabled: TRUE
ptt_port_enabled: TRUE
current_log_pdelay_req_interval 0
pdelay_req_interval 0 nanoseconds
allowed_lost_responses 3
neighbor_prop_delay_threshold 2000 nanoseconds
```

```
is_measuring_delay : FALSE
Port state: : MASTER
sync_seq_num 22023
delay_req_seq_num 23857
num sync messages transmitted 0
num sync messages received 0
num followup messages transmitted 0
num followup messages received 0
num pdelay requests transmitted 285695
num pdelay requests received 0
num pdelay responses transmitted 0
num pdelay responses received 0
num pdelay followup responses transmitted 0
num pdelay followup responses received 0
```

show ptp brief

To display a brief status of PTP on the interfaces, use the **show ptp brief** command in global configuration mode.

show ptp brief

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Examples

The following is a sample output from the **show ptp brief** command:

Device# **show ptp brief**

```

Interface                               Domain   PTP State
FortyGigabitEthernet1/1/1              0        FAULTY
FortyGigabitEthernet1/1/2              0        SLAVE
GigabitEthernet1/1/1                   0        FAULTY
GigabitEthernet1/1/2                   0        FAULTY
GigabitEthernet1/1/3                   0        FAULTY
GigabitEthernet1/1/4                   0        FAULTY
TenGigabitEthernet1/0/1                 0        FAULTY
TenGigabitEthernet1/0/2                 0        FAULTY
TenGigabitEthernet1/0/3                 0        MASTER
TenGigabitEthernet1/0/4                 0        FAULTY
TenGigabitEthernet1/0/5                 0        FAULTY
TenGigabitEthernet1/0/6                 0        FAULTY
TenGigabitEthernet1/0/7                 0        MASTER
TenGigabitEthernet1/0/8                 0        FAULTY
TenGigabitEthernet1/0/9                 0        FAULTY
TenGigabitEthernet1/0/10                0        FAULTY
TenGigabitEthernet1/0/11                0        MASTER
TenGigabitEthernet1/0/12                0        FAULTY
TenGigabitEthernet1/0/13                0        FAULTY
TenGigabitEthernet1/0/14                0        FAULTY
TenGigabitEthernet1/0/15                0        FAULTY
TenGigabitEthernet1/0/16                0        FAULTY
.
.
.
```

Related Commands

Command	Description
show ptp clock	Displays PTP clock information.
show ptp parent	Displays the parent clock information.
show ptp port	Displays the PTP port information.
show ptp time-property	Displays the PTP clock time property.

show ptp clock

To display PTP clock information, use the **show ptp clock** command in global configuration mode.

show ptp clock

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Examples

The following is a sample output from the **show ptp clock** command:

```
Device# show ptp clock
```

```
PTP CLOCK INFO
  PTP Device Type: Boundary clock
  PTP Device Profile: IEEE 802/1AS Profile
  Clock Identity: 0x4:6C:9D:FF:FE:4F:95:0
  Clock Domain: 0
  Number of PTP ports: 38
  PTP Packet priority: 4
  Priority1: 128
  Priority2: 128
  Clock Quality:
    Class: 248
    Accuracy: Unknown
    Offset (log variance): 16640
  Offset From Master(ns): 0
  Mean Path Delay(ns): 0
  Steps Removed: 3
  Local clock time: 00:12:13 UTC Jan 1 1970
```

Related Commands

Command	Description
show ptp brief	Displays a brief status of PTP on the interfaces.
show ptp parent	Displays the parent clock information.
show ptp port	Displays the PTP port information.
show ptp time-property	Displays the PTP clock time property.

show ptp parent

To display the PTP parent clock information, use the **show ptp parent** command in global configuration mode.

show ptp parent

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Examples

The following is a sample output from the **show ptp parent** command:

```
Device# show ptp parent
```

```
Steps Removed: 3
Local clock time: 00:12:13 UTC Jan 1 1970
```

This command can be used to view the parent clock information.

```
Device#show ptp parent
```

```
PTP PARENT PROPERTIES
Parent Clock:
Parent Clock Identity: 0xB0:7D:47:FF:FE:9E:B6:80
Parent Port Number: 3
Observed Parent Offset (log variance): 16640
Observed Parent Clock Phase Change Rate: N/A

Grandmaster Clock:
Grandmaster Clock Identity: 0x4:6C:9D:FF:FE:67:3A:80
Grandmaster Clock Quality:
Class: 248
Accuracy: Unknown
Offset (log variance): 16640
Priority1: 0
Priority2: 128
```

Related Commands

Command	Description
show ptp brief	Displays a brief status of PTP on the interfaces.
show ptp clock	Displays PTP clock information.
show ptp port	Displays the PTP port information.

Command	Description
show ptp time-property	Displays the PTP clock time property.

show ptp port

To display the PTP port information, use the **show ptp port** command in global configuration mode.

show ptp port

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

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

Command History	Release	Modification
	Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Examples

The following is a sample output from the **show ptp port** command:

```
Device# show ptp port
```

```
PTP PORT DATASET: FortyGigabitEthernet1/1/1
  Port identity: clock identity: 0x4:6C:9D:FF:FE:4E:3A:80
  Port identity: port number: 1
  PTP version: 2
  Port state: FAULTY
  Delay request interval(log mean): 5
  Announce receipt time out: 3
  Peer mean path delay(ns): 0
  Announce interval(log mean): 1
  Sync interval(log mean): 0
  Delay Mechanism: End to End
  Peer delay request interval(log mean): 0
  Sync fault limit: 500000000
```

```
PTP PORT DATASET: FortyGigabitEthernet1/1/2
  Port identity: clock identity: 0x4:6C:9D:FF:FE:4E:3A:80
  Port identity: port number: 2
  PTP version: 2
  Port state: FAULTY
  Delay request interval(log mean): 5
  Announce receipt time out: 3
  Peer mean path delay(ns): 0
  Announce interval(log mean): 1
--More--
```

Related Commands

Command	Description
show ptp brief	Displays a brief status of PTP on the interfaces.
show ptp clock	Displays PTP clock information.
show ptp parent	Displays the parent clock information.
show ptp time-property	Displays the PTP clock time property.

show rep topology

To display Resilient Ethernet Protocol (REP) topology information for a segment or for all the 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 the REP topology information. The <i>segment-id</i> 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 Everest 16.5.1a	This command was introduced.

Examples

The following is a 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 a 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 spanning-tree

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

show spanning-tree [*bridge-group*] [{ **active** | **backbonefast** | **blockedports** | **bridge** [*id*] | **detail** | **inconsistentports** | **instances** | **interface** *interface-type interface-number* | **mst** [{ *list* | **configuration** [*digest*] }] | **pathcost method** | **root** | **summary** [*totals*] | **uplinkfast** | **vlan** *vlan-id* }]

Syntax Description		
	<i>bridge-group</i>	(Optional) Specifies the bridge group number. The range is 1 to 255.
	active	(Optional) Displays spanning-tree information on active interfaces only.
	backbonefast	(Optional) Displays spanning-tree BackboneFast status.
	blockedports	(Optional) Displays blocked port information.
	bridge	(Optional) Displays status and configuration of this switch.
	detail	(Optional) Shows status and configuration details.
	inconsistentports	(Optional) Displays information about inconsistent ports.
	instances	(Optional) Displays information about maximum STP instances.
	interface <i>interface-type interface-number</i>	(Optional) Specifies the type and number of the interface. Enter each interface designator, using a space to separate it from the one before and the one after. Ranges are not supported. Valid interfaces include physical ports and virtual LANs (VLANs). See the “Usage Guidelines” for valid values.
	mst	(Optional) Specifies multiple spanning-tree.
	<i>list</i>	(Optional) Specifies a multiple spanning-tree instance list.
	configuration digest	(Optional) Displays the multiple spanning-tree current region configuration.
	pathcost <i>method</i>	(Optional) Displays the default path-cost calculation method that is used. See the “Usage Guidelines” section for the valid values.
	root	(Optional) Displays root-switch status and configuration.
	summary	(Optional) Specifies a summary of port states.
	totals	(Optional) Displays the total lines of the spanning-tree state section.
	uplinkfast	(Optional) Displays spanning-tree UplinkFast status.
	vlan <i>vlan-id</i>	(Optional) Specifies the VLAN ID. The range is 1 to 4094. If the <i>vlan-id</i> value is omitted, the command applies to the spanning-tree instance for all VLANs.
	<i>id</i>	(Optional) Identifies the spanning tree bridge.

port-channel <i>number</i>	(Optional) Identifies the Ethernet channel associated with the interfaces.
-----------------------------------	--

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

The keywords and arguments that are available with the **show spanning-tree** command vary depending on the platform you are using and the network modules that are installed and operational.

The **port-channel** *number* values from 257 to 282 are supported on the Content Switching Module (CSM) and the Firewall Services Module (FWSM) only.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 2 to 13 and valid values for the port number are from 1 to 48.

When checking spanning tree-active states and you have a large number of VLANs, you can enter the **show spanning-tree summary total** command. You can display the total number of VLANs without having to scroll through the list of VLANs.

The valid values for keyword **pathcost** *method* are:

- **append**: Appends the redirected output to a URL (supporting the append operation).
- **begin**: Begins with the matching line.
- **exclude**: Excludes matching lines.
- **include**: Includes matching lines.
- **redirect**: Redirects output to a URL.
- **tee**: Copies output to a URL.

When you run the **show spanning-tree** command for a VLAN or an interface the switch router will display the different port states for the VLAN or interface. The valid spanning-tree port states are listening, learning, forwarding, blocking, disabled, and loopback.

```
Device#
show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
            Address     5c71.0dfe.8380
            This bridge is the root
            Hello Time  2 sec    Max Age 20 sec    Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
            Address     5c71.0dfe.8380
            Hello Time  2 sec    Max Age 20 sec    Forward Delay 15 sec
            Aging Time  300 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----	----	---	-----	-----	-----
Gil/0/1	Desg	FWD	20000	128.1	P2p
Gil/0/18	Desg	FWD	20000	128.18	P2p
Gil/0/21	Desg	FWD	20000	128.21	P2p
Tel/0/25	Desg	FWD	20000	128.25	P2p
Tel/0/37	Desg	FWD	2000	128.37	P2p
Tel/0/38	Desg	FWD	2000	128.38	P2p
Tel/0/45	Desg	FWD	20000	128.45	P2p
Tel/0/48	Desg	FWD	20000	128.48	P2p

See the table below for definitions of the port states:

Table 3: show spanning-tree vlan Command Port States

Field	Definition
BLK	Blocked is when the port is still sending and listening to BPDU packets but is not forwarding traffic.
DIS	Disabled is when the port is not sending or listening to BPDU packets and is not forwarding traffic.
FWD	Forwarding is when the port is sending and listening to BPDU packets and forwarding traffic.
LBK	Loopback is when the port receives its own BPDU packet back.
LIS	Listening is when the port spanning tree initially starts to listen for BPDU packets for the root bridge.
LRN	Learning is when the port sets the proposal bit on the BPDU packets it sends out

This example shows how to display a summary of interface information:

```

Device#
show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     6cb2.ae4a.4fc0
             This bridge is the root
             Hello Time  2 sec    Max Age 20 sec    Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
             Address     6cb2.ae4a.4fc0
             Hello Time  2 sec    Max Age 20 sec    Forward Delay 15 sec
             Aging Time  300 sec

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----	----	---	-----	-----	-----
Fif1/0/17	Desg	FWD	2000	128.17	P2p
Fif1/0/19	Desg	FWD	800	128.19	P2p
Fif1/0/21	Desg	FWD	2000	128.21	P2p
Fif1/0/23	Desg	FWD	2000	128.23	P2p
TwoH1/0/42	Desg	FWD	500	128.42	P2p
Fou1/0/44	Desg	FWD	50	128.44	P2p
Fif2/0/17	Back	BLK	2000	128.185	P2p
Fif2/0/19	Back	BLK	800	128.187	P2p
Fif2/0/21	Back	BLK	2000	128.189	P2p
Fif2/0/23	Back	BLK	2000	128.191	P2p
Fou2/0/43	Desg	FWD	50	128.211	P2p
Fou2/0/44	Back	BLK	50	128.212	P2p
Hu5/0/13	Desg	FWD	500	128.685	P2p

show spanning-tree

```

Hu5/0/15          Desg FWD 500      128.687 P2p
Hu5/0/21          Back BLK 500      128.693 P2p
Hu5/0/23          Back BLK 500      128.695 P2p
Fou6/0/27         Back BLK 50       128.867 P2p
Hu6/0/29          Desg FWD 200      128.869 P2p
Hu6/0/30          Back BLK 200      128.870 P2p

```

The table below describes the fields that are shown in the example.

Table 4: show spanning-tree Command Output Fields

Field	Definition
Port ID Prio.Nbr	Port ID and priority number.
Cost	Port cost.
Sts	Status information.

This example shows how to display information about the spanning tree for this bridge only:

```
Device# show spanning-tree bridge
```

```

Vlan                Bridge ID                Hello Time  Max Age  Fwd Dly  Protocol
-----
VLAN0001            32769 (32768, 1) 5c71.0dfe.8380  2       20    15    rstp

```

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

```

Device#
show spanning-tree detail
VLAN0001 is executing the rstp compatible Spanning Tree protocol
Bridge Identifier has priority 32768, sysid 1, address 5c71.0dfe.8380
Configured hello time 2, max age 20, forward delay 15, transmit hold-count 6
We are the root of the spanning tree
Topology change flag not set, detected flag not set
Number of topology changes 27 last change occurred 4d19h ago
    from TenGigabitEthernet1/0/48
Times: hold 1, topology change 35, notification 2
    hello 2, max age 20, forward delay 15
Timers: hello 0, topology change 0, notification 0, aging 300

Port 1 (GigabitEthernet1/0/1) of VLAN0001 is designated forwarding
Port path cost 20000, Port priority 128, Port Identifier 128.1.
Designated root has priority 32769, address 5c71.0dfe.8380
Designated bridge has priority 32769, address 5c71.0dfe.8380
Designated port id is 128.1, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 208695, received 1

Port 18 (GigabitEthernet1/0/18) of VLAN0001 is designated forwarding
!
!
<<output truncated>>

```

This example shows how to display a summary of port states:

```
Device#
```

show spanning-tree summary

```
Switch is in rapid-pvst mode
Root bridge for: VLAN0001
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                  is enabled but inactive in rapid-pvst mode
Configured Pathcost method used is long
```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0001	1	0	0	26	27
1 vlan	1	0	0	26	27

This example shows how to display the total lines of the spanning-tree state section:

Device#

show spanning-tree summary total Switch is in rapid-pvst mode

```
Root bridge for: VLAN0001
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                  is enabled but inactive in rapid-pvst mode
Configured Pathcost method used is long
```

Name	Blocking	Listening	Learning	Forwarding	STP Active
1 vlan	1	0	0	26	27

This example shows how to display information about the spanning tree for a specific VLAN:

Device#

show spanning-tree vlan 200

```
VLAN0001
Spanning tree enabled protocol rstp
Root ID    Priority    32769
           Address     5c71.0dfe.8380
           This bridge is the root
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
           Address     5c71.0dfe.8380
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time  300 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Gi1/0/1	Desg	FWD	20000	128.1	P2p
Gi1/0/18	Desg	FWD	20000	128.18	P2p
Gi1/0/21	Desg	FWD	20000	128.21	P2p
Tel/0/25	Desg	FWD	20000	128.25	P2p
Tel/0/37	Desg	FWD	2000	128.37	P2p
Tel/0/38	Desg	FWD	2000	128.38	P2p
Tel/0/45	Desg	FWD	20000	128.45	P2p

```

Te1/0/48          Desg FWD 20000      128.48    P2p
!
!
<<output truncated>>

```

The table below describes the fields that are shown in the example.

Table 5: show spanning-tree vlan Command Output Fields

Field	Definition
Role	Current 802.1w role; valid values are Boun (boundary), Desg (designated), Root, Altn (alternate), and Back (backup).
Sts	Spanning-tree states; valid values are BKN* (broken) ¹ , BLK (blocking), DWN (down), LTN (listening), LBK (loopback), LRN (learning), and FWD (forwarding).
Cost	Port cost.
Prio.Nbr	Port ID that consists of the port priority and the port number.
Status	<p>Status information; valid values are as follows:</p> <ul style="list-style-type: none"> • P2p/Shr: The interface is considered as a point-to-point (resp. shared) interface by the spanning tree. • Edge: PortFast has been configured (either globally using the default command or directly on the interface) and no BPDU has been received. • *ROOT_Inc, *LOOP_Inc, *PVID_Inc and *TYPE_Inc: The port is in a broken state (BKN*) for an inconsistency. The port would be (respectively) Root inconsistent, Loopguard inconsistent, PVID inconsistent, or Type inconsistent. • Bound(type): When in MST mode, identifies the boundary ports and specifies the type of the neighbor (STP, RSTP, or PVST). • Peer(STP): When in PVRST rapid-pvst mode, identifies the port connected to a previous version of the 802.1D bridge.

¹ For information on the *, see the definition for the Status field.

show spanning-tree mst

To display the information about the Multiple Spanning Tree (MST) protocol, use the **show spanning-tree mst** command in privileged EXEC mode.

show spanning-tree mst [{ **configuration** [**digest**] | *instance-id-number* }] [**interface** *interface*] [**detail**] [**service** *instance*]

Syntax Description	
<i>instance-id-number</i>	(Optional) Instance identification number. The range is from 0 to 4094.
detail	(Optional) Displays detailed information about the MST protocol.
<i>interface</i>	(Optional) Displays the information about the interfaces. See the “Usage Guidelines” section for valid number values.
configuration	(Optional) Displays information about the region configuration.
digest	(Optional) Displays information about the message digest 5 (MD5) algorithm included in the current MST configuration identifier (MSTCI).
interface	(Optional) Displays information about the interface type.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines The valid values for the *interface* argument depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 2 to 13 and valid values for the port number are from 1 to 48.

The number of valid values for **port-channel** *number* are a maximum of 64 values ranging from 1 to 282. The **port-channel** *number* values from 257 to 282 are supported on the Content Switching Module (CSM) and the Firewall Services Module (FWSM) only.

The number of valid values for **vlan** are from 1 to 4094.

In the output display of the **show spanning-tree mst configuration** command, a warning message may be displayed. This message appears if you do not map secondary VLANs to the same instance as the associated primary VLAN. The display includes a list of the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The warning message is as follows:

```
These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

In the output display of the **show spanning-tree mst configuration digest** command, if the output applies to both standard and prestandard bridges at the same time on a per-port basis, two different digests are displayed.

If you configure a port to transmit prestandard PortFast bridge protocol data units (BPDUs) only, the prestandard flag displays in the **show spanning-tree** commands. The variations of the prestandard flag are as follows:

- Pre-STD (or pre-standard in long format): This flag is displayed if the port is configured to transmit prestandard BPDUs and if a prestandard neighbor bridge has been detected on this interface.
- Pre-STD-Cf (or pre-standard (config) in long format): This flag is displayed if the port is configured to transmit prestandard BPDUs but a prestandard BPDU has not been received on the port, the autodetection mechanism has failed, or a misconfiguration, if there is no prestandard neighbor, has occurred.
- Pre-STD-Rx (or prestandard (rcvd) in long format): This flag is displayed when a prestandard BPDU has been received on the port, but it has not been configured to send prestandard BPDUs. The port will send prestandard BPDUs, but Cisco recommends that you change the port configuration so that the interaction with the prestandard neighbor does not rely only on the autodetection mechanism.

If the configuration is not prestandard compliant (for example, a single MST instance has an ID that is greater than or equal to 16,) the prestandard digest is not computed and the following output is displayed:

```
Device# show spanning-tree mst configuration digest

Name          [region1]
Revision 2      Instances configured 3
Digest         0x3C60DBF24B03EBF09C5922F456D18A03
Pre-std Digest N/A, configuration not pre-standard compatible
```

MST BPDUs include an MSTCI that consists of the region name, region revision, and an MD5 digest of the VLAN-to-instance mapping of the MST configuration.

See the **show spanning-tree mst** command field description table for output descriptions.

Examples

The following example shows how to display information about the region configuration:

```
Device# show spanning-tree mst configuration
```

```
Name          [train]
Revision 2702
Instance Vlan mapped
-----
0          1-9,11-19,21-29,31-39,41-4094
1          10,20,30,40
-----
```

The following example shows how to display additional MST-protocol values:

```
Device# show spanning-tree mst 3 detail
```

```
##### MST03 vlans mapped: 3,3000-3999
Bridge address 0002.172c.f400 priority 32771 (32768 sysid 3)
Root this switch for MST03
GigabitEthernet1/1 of MST03 is boundary forwarding
Port info port id 128.1 priority 128
cost 20000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port
id 128.1
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 4, received 0
FastEthernet4/1 of MST03 is designated forwarding
Port info port id 128.193 priority 128 cost
200000
Designated root address 0002.172c.f400 priority 32771
```

```

cost 0
Designated bridge address 0002.172c.f400 priority 32771 port id
128.193
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 254, received 1
FastEthernet4/2 of MST03 is backup blocking
Port info port id 128.194 priority 128 cost
200000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port id
128.193
Timers: message expires in 2 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 3, received 252

```

The following example shows how to display the MD5 digest included in the current MSTCI:

Device# **show spanning-tree mst configuration digest**

```

Name      [mst-config]
Revision  10      Instances configured 25
Digest    0x40D5ECA178C657835C83BBCB16723192
Pre-std Digest 0x27BF112A75B72781ED928D9EC5BB4251

```

Related Commands

Command	Description
spanning-tree mst	Sets the path cost and port-priority parameters for any MST instance.
spanning-tree mst forward-time	Sets the forward-delay timer for all the instances on the Cisco 7600 series router.
spanning-tree mst hello-time	Sets the hello-time delay timer for all the instances on the Cisco 7600 series router.
spanning-tree mst max-hops	Specifies the number of possible hops in the region before a BPDU is discarded.

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 [ANI | AccessTunnel | Auto-Template | BDI | CEM-PG | GMPLS |
GigabitEthernet | HundredGigE | InternalInterface | LISP | Loopback | Null |
PROTECTION_GROUP | Port-channel | SDH_ACR | SERIAL-ACR | Serial-PG | TLS-VIF
| Tunnel | Tunnel-tp | TwentyFiveGigE | VirtualPortGroup | Vlan | nve] interface_number
show uddl neighbors
show uddl fast-hello interface_number
```

Syntax Description

ANI	(Optional) Displays UDLD operational status of the Autonomic-Networking virtual interface.
AccessTunnel	(Optional) Displays UDLD operational status of the Access Tunnel Interface.
Auto-Template	(Optional) Displays UDLD operational status of the auto-template interface. The range is from 1 to 999.
BDI	(Optional) Displays UDLD operational status of the Bridge-Domain interface.
CEM-PG	(Optional) Displays UDLD operational status of the Circuit Emulation interface with Protection group.
GMPLS	(Optional) Displays UDLD operational status of the MPLS interface.
GigabitEthernet	(Optional) Displays UDLD operational status of the GigabitEthernet interface.
HundredGigE	(Optional) Displays UDLD operational status of the Hundred Gigabit Ethernet.
InternalInterface	(Optional) Displays UDLD operational status of the internal interface. The range is from 0 to 9.
LISP	(Optional) Displays UDLD operational status of the Locator/ID Separation Protocol Virtual Interface.
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.
PROTECTION_GROUP	(Optional) Displays UDLD operational status of the Protection-group controller.

Port-channel	(Optional) Displays UDLD operational status of the Ethernet channel interfaces. The range is 1 to 128.
SDH_ACR	(Optional) Displays UDLD operational status of the Virtual SDH-ACR controller.
SERIAL-ACR	(Optional) Displays UDLD operational status of the Serial interface with ACR.
Serial-PG	(Optional) Displays UDLD operational status of the Serial interface with Protection Group.
TLS-VIF	(Optional) Displays UDLD operational status of the TLS Virtual Interface.
Tunnel	(Optional) Displays UDLD operational status of the tunnel interface. The range is from 0 to 2147483647.
Tunnel-tp	(Optional) Displays UDLD operational status of the MPLS Transport Profile interface.
TwentyFiveGigE	(Optional) Displays UDLD operational status of the Twenty Five Gigabit Ethernet.
VirtualPortGroup	(Optional) Displays UDLD operational status of the Virtual Port Group.
Vlan	(Optional) Displays UDLD operational status of the VLAN interface. The range is from 1 to 4095.
<i>interface_number</i>	(Optional) ID of the interface and port number. Valid interfaces include physical ports, VLANs, and port channels.
nve	(Optional) Displays UDLD operational status of Network virtualization endpoint interface
neighbors	(Optional) Displays neighbor information only.
fast-hello	(Optional) Displays ports that have fast-hello configured and their fast-hello operational status.
fast-hello <i>interface_number</i>	(Optional) Displays the fast-hello information of a specific interface.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.
Cisco IOS XE Fuji 16.9.1	The fast-hello keyword was added to the command.

Usage Guidelines

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

Examples:

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

```
Device> show udld TwentyFiveGigE1/0/1
Interface TwentyFiveGigE1/0/1
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 7000 ms
Time out interval: 5000 ms

Port fast-hello configuration setting: Enabled
Port fast-hello interval: 200 ms
Port fast-hello operational state: Enabled
Neighbor fast-hello configuration setting: Enabled
Neighbor fast-hello interval: 200 ms

Entry 1
---
Expiration time: 1400 ms
Cache Device index: 1
Current neighbor state: Bidirectional
Device ID: 0A74286120
Port ID: Hu1/0/2
Neighbor echo 1 device: 0A74286A80
Neighbor echo 1 port: Hu1/0/10

TLV Message interval: 15
TLV fast-hello interval: 500 ms
TLV Time out interval: 5
TLV CDP Device name: SkyFox-59
```

This is an example of output from the **show udld fast-hello interface-id** command. For this display, UDLD is enabled on both ends of the link, and UDLD detects that the link is bidirectional. The fast-hello information of the port is displayed along with the UDLD operational status.

```
Device> show udld fast-hello hundredGigE 1/0/10
Interface hundredGigE 1/0/10
---Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 500 ms
Time out interval: 5000 ms

Port fast-hello configuration setting: Enabled
Port fast-hello interval: 500 ms
Port fast-hello operational state: Enabled
Neighbor fast-hello configuration setting: Enabled
Neighbor fast-hello interval: 500 ms

Entry 1
---
Expiration time: 1400 ms
Cache Device index: 1
Current neighbor state: Bidirectional
Device ID: 0A74286120
Port ID: Hu1/0/2
```

```
Neighbor echo 1 device: 0A74286A80
Neighbor echo 1 port: Hu1/0/10
```

```
TLV Message interval: 15
TLV fast-hello interval: 500 ms
TLV Time out interval: 5
TLV CDP Device name: SkyFox-59
```

This is an example of output from the **show udd fast-hello** global command.

```
Device> show udd fast-hello
```

```
Total ports on which fast hello can be configured: 32
```

```
Total ports with fast hello configured: 3
```

```
Total ports with fast hello operational: 3
```

```
Total ports with fast hello non-operational: 0
```

Port-ID	Hello	Neighbor-Hello	Neighbor-Device	Neighbor-Port	Status
Hu1/0/10	500	500	0A74286120	Hu1/0/2	Operational
Hu1/0/12	500	500	0A74286120	Hu1/0/18	Operational
Hu1/0/14	500	500	0A74286120	Hu1/0/4	Operational

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

```
Device> enable
```

```
Device# show udd neighbors
```

Port	Device Name	Device ID	Port-ID	OperState
Gi2/0/1	Switch-A	1	Gi2/0/1	Bidirectional
Gi3/0/1	Switch-A	2	Gi3/0/1	Bidirectional

show vlan dot1q tag native

To display the status of tagging on the native VLAN use the **show vlan dot1q tag native** command.

show vlan dot1q tag native

Syntax Description

This command has no arguments or keywords.

Command Modes	Privileged EXEC mode (#)	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1aCisco IOS XE Gibraltar 16.11.1	This command was introduced.

Example

The following is sample output from the **show vlan dot1q tag native** command:

```
Device# show vlan dot1q tag native
*Feb  1 06:47:30.719: %SYS-5-CONFIG_I: Configured from console by console
dot1q native vlan tagging is enabled globally

Per Port Native Vlan Tagging State
-----
Port           Operational      Native VLAN
              Mode          Tagging State
-----
Hu1/0/45      trunk          enabled
```


spanning-tree backbonefast

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

spanning-tree backbonefast
no spanning-tree backbonefast

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

Command Default	BackboneFast is disabled.
------------------------	---------------------------

Command Modes	Global configuration (config)
----------------------	-------------------------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines	BackboneFast should be enabled on all of the Cisco devices containing an Ethernet switch network module. BackboneFast provides for fast convergence in the network backbone after a spanning-tree topology change. It enables the switch to detect an indirect link failure and to start the spanning-tree reconfiguration sooner than it would under normal spanning-tree rules.
-------------------------	---

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

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

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

Related Commands	Command	Description
	show spanning-tree	Displays information about the spanning-tree state.

spanning-tree bpdudfilter

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

spanning-tree bpdudfilter { enable | disable }
no spanning-tree bpdudfilter

Syntax Description	enable	Enables BPDU filtering on this interface.
	disable	Disables BPDU filtering on this interface.
Command Default	The setting that is already configured when you enter the spanning-tree portfast edge bpdudfilter default command .	
Command Modes	Interface configuration (config-if) Template configuration (config-template)	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines



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

Entering the **spanning-tree bpdudfilter enable** command to enable BPDU filtering overrides the PortFast configuration.

When configuring Layer 2-protocol tunneling on all the service-provider edge switches, you must enable spanning-tree BPDU filtering on the 802.1Q tunnel ports by entering the **spanning-tree bpdudfilter enable** command.

BPDU filtering prevents a port from sending and receiving BPDUs. The configuration is applicable to the whole interface, whether it is trunking or not. This command has three states:

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

Use the **spanning-tree portfast bpdudfilter default** command to enable BPDU filtering on all ports that are already configured for PortFast.

Examples

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

```
Device(config-if) # spanning-tree bpdufilter enable
Device(config-if) #
```

The following example shows how to enable BPDU filtering on an interface using interface template:

```
Device# configure terminal
Device(config) # template user-templ1
Device(config-template) # spanning-tree bpdufilter enable
Device(config-template) # end
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree portfast edge bpdufilter default	Enables BPDU filtering by default on all PortFast ports.

spanning-tree bpduguard

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

spanning-tree bpduguard { enable | disable }
no spanning-tree bpduguard

Syntax Description

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

Command Modes

Interface configuration (config-if)
 Template configuration (config-template)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

BPDU guard prevents a port from receiving BPDUs. Typically, this feature is used in a service-provider environment where the network administrator wants to prevent an access port from participating in the spanning tree. If the port still receives a BPDU, it is put in the error-disabled state as a protective measure. This command has three states:

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

Examples

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

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

The following example shows how to enable BPDU guard on an interface using interface template:

```
Device# configure terminal
Device(config)# template user-templatel
Device(config-template)# spanning-tree bpduguard enable
Device(config-template)# end
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

Command	Description
spanning-tree portfast edge bpduguard default	Enables BPDU guard by default on all PortFast ports.

spanning-tree bridge assurance

To enable bridge assurance on all network ports on the device, use the **spanning-tree bridge assurance** command in global configuration mode. To disable bridge assurance, use the **no** form of this command.

spanning-tree bridge assurance
no spanning-tree bridge assurance

Syntax Description This command has no arguments or keywords.

Command Default Bridge assurance is enabled.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines Bridge assurance protects against a unidirectional link failure or other software failure and a device that continues to forward data traffic when it is no longer running the spanning tree algorithm.

Bridge assurance is enabled only on spanning tree network ports that are point-to-point links. Both ends of the link must have bridge assurance enabled. If the device on one side of the link has bridge assurance enabled and the device on the other side either does not support bridge assurance or does not have this feature enabled, the connecting port is blocked.

Disabling bridge assurance causes all configured network ports to behave as normal spanning tree ports.

Examples

This example shows how to enable bridge assurance on all network ports on the switch:

```
Device(config)#  
spanning-tree bridge assurance  
Device(config)#
```

This example shows how to disable bridge assurance on all network ports on the switch:

```
Device(config)#  
no spanning-tree bridge assurance  
Device(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

spanning-tree cost

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

spanning-tree cost *cost*
no spanning-tree cost

Syntax Description

<i>cost</i>	Path cost. The range is from 1 to 200000000.
-------------	--

Command Modes

Interface configuration (config-if)
 Template configuration (config-template)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

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

If a loop occurs, spanning tree uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission.

Examples

The following example shows how to access an interface and set a path cost value of 250 for the spanning tree VLAN associated with that interface:

```
Router(config)# interface ethernet 2/0
Router(config-if)# spanning-tree cost 250
```

The following example shows how to set a path cost value of 250 for the spanning tree VLAN associated with an interface using an interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# spanning-tree cost 250
Device(config-template)# end
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information for the specified spanning-tree instances.
spanning-tree port-priority	Sets an interface priority when two bridges tie for position as the root bridge.

Command	Description
spanning-tree portfast (global)	Enables PortFast mode, where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire.
spanning-tree portfast (interface)	Enables PortFast mode, where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire.
spanning-tree uplinkfast	Enables the UplinkFast feature.
spanning-tree vlan	Configures STP on a per-VLAN basis.

spanning-tree etherchannel guard misconfig

To display an error message when a loop due to a channel misconfiguration is detected, use the **spanning-tree etherchannel guard misconfig** command in global configuration mode. To disable the error message, use the **no** form of this command.

spanning-tree etherchannel guard misconfig
no spanning-tree etherchannel guard misconfig

Syntax Description

This command has no arguments or keywords.

Command Default

Error messages are displayed.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

EtherChannel uses either Port Aggregation Protocol (PAgP) or Link Aggregation Control Protocol (LACP) and does not work if the EtherChannel mode of the interface is enabled using the **channel-group** group-number mode on command.

The **spanning-tree etherchannel guard misconfig** command detects two types of errors: misconfiguration and misconnection errors. A misconfiguration error is an error between the port-channel and an individual port. A misconnection error is an error between a device that is channeling more ports and a device that is not using enough Spanning Tree Protocol (STP) Bridge Protocol Data Units (BPDUs) to detect the error. In this case, the device will only error disable an EtherChannel if the switch is a nonroot device.

When an EtherChannel-guard misconfiguration is detected, this error message displays:

```
msgdef(CHNL_MISCFG, SPANTREE, LOG_CRIT, 0, "Detected loop due to etherchannel misconfiguration  
of %s %s")
```

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

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

Examples

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

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

Related Commands

Command	Description
show etherchannel summary	Displays the EtherChannel information for a channel.

Command	Description
show interfaces status err-disabled	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.
shutdown	Disables an interface.

spanning-tree extend system-id

To enable the extended-system ID feature on chassis that support 1024 MAC addresses, use the **spanning-tree extend system-id** command in global configuration mode. To disable the extended system identification, use the **no** form of this command.

spanning-tree extend system-id
no spanning-tree extend system-id

Syntax Description This command has no arguments or keywords.

Command Default Enabled on systems that do not provide 1024 MAC addresses.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines Enabling or disabling the extended-system ID updates the bridge IDs of all active Spanning Tree Protocol (STP) instances, which might change the spanning-tree topology.

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

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

Related Commands	Command	Description
	show spanning-tree	Displays information about the spanning-tree state.

spanning-tree guard

To enable or disable the guard mode, use the **spanning-tree guard** command in interface configuration and template configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree guard { **loop** | **root** | **none** }
no spanning-tree guard

Syntax Description

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

Command Default

Guard mode is disabled.

Command Modes

Interface configuration (config-if)
Template configuration (config-template)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Examples

This example shows how to enable root guard:

```
Device(config-if) # spanning-tree guard root  
Device(config-if) #
```

The following example shows how to enable root guard on an interface using an interface template:

```
Device# configure terminal  
Device(config) # template user-templatel  
Device(config-template) # spanning-tree guard root  
Device(config-template) # end
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree loopguard default	Enables loop guard as a default on all ports of a given bridge.

spanning-tree link-type

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

spanning-tree link-type { point-to-point | shared }
no spanning-tree link-type

Syntax Description

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

Command Default

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

Command Modes

Interface configuration (config-if)
Template configuration (config-template)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

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

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

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

If you connect a port (local port) to a remote port through a point-to-point link and the local port becomes a designated port, the device negotiates with the remote port and rapidly changes the local port to the forwarding state

Examples

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

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

The following example shows how to configure the port as a shared link using an interface template:

```
Device# configure terminal
Device(config) # template user-templatel
Device(config-template) # spanning-tree link-type shared
Device(config-template) # end
```

Related Commands

Command	Description
show spanning-tree interface	Displays information about the spanning-tree state.

spanning-tree loopguard default

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

spanning-tree loopguard default
no spanning-tree loopguard default

Syntax Description This command has no arguments or keywords.

Command Default Loop guard is disabled.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

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

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

The individual loop-guard port configuration overrides this command.

Examples

This example shows how to enable loop guard:

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

Related Commands	Command	Description
	show spanning-tree	Displays information about the spanning-tree state.
	spanning-tree guard	Enables or disables the guard mode.

spanning-tree mode

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

spanning-tree mode [{ **pvst** | **mst** | **rapid-pvst** }]
no spanning-tree mode

Syntax Description

pvst	(Optional) PVST+ mode.
mst	(Optional) MST mode.
rapid-pvst	(Optional) Rapid-PVST+ mode.

Command Default

pvst

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines



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

Examples

This example shows how to switch to MST mode:

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

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

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

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst

To set the priority parameters or configure the device as a root for any Multiple Spanning Tree (MST) instance, use the **spanning-tree mst** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

```
spanning-tree mst instance-id { priority priority | root { primary | secondary } }  
no spanning-tree mst instance-id { { priority priority | root { primary | secondary } } }
```

Syntax Description

priority <i>priority</i>	Port priority for an instance. The range is from 0 to 61440 in increments of 4096.
root	Configures the device as a root.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Examples

This example shows how to set the priority:

```
Device(config-if)#  
spanning-tree mst 0 priority 1  
Device(config-if)#
```

This example shows how to set the device as a primary root:

```
Device(config-if)#  
spanning-tree mst 0 root primary  
Device(config-if)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst configuration

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

spanning-tree mst configuration
no spanning-tree mst configuration

Syntax Description

This command has no arguments or keywords.

Command Default

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

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

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

The MST configuration consists of three main parameters:

- Instance VLAN mapping: See the **instance** command.
- Region name: See the **name** command (MST configuration submode).
- Configuration revision number: See the **revision** command.

The **abort** and **exit** commands allow you to exit MST configuration submode. The difference between the two commands depends on whether you want to save your changes or not.

The **exit** command commits all the changes before leaving MST configuration submode. If you do not map secondary VLANs to the same instance as the associated primary VLAN, when you exit MST-configuration submode, a warning message displays and lists the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The warning message is as follows:

```
These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

The **abort** command leaves MST-configuration submode without committing any changes.

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

In the unlikely event that two users commit a new configuration at exactly at the same time, this warning message displays:

```
% MST CFG:Configuration change lost because of concurrent access
```

Examples

This example shows how to enter MST-configuration submode:

```
Device(config)# spanning-tree mst configuration  
Device(config-mst)#
```

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

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

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
name (MST)	Sets the name of an MST region.
revision	Sets the revision number for the MST configuration.
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst forward-time

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

spanning-tree mst forward-time *seconds*

no spanning-tree mst forward-time

Syntax Description

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

Command Default

15 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Examples

This example shows how to set the forward-delay timer:

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

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst hello-time

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

spanning-tree mst hello-time *seconds*
no spanning-tree mst hello-time

Syntax Description	<i>seconds</i>	Number of seconds to set the hello-time delay timer for all the instances on the device. The range is from 1 to 10 in seconds.
---------------------------	----------------	--

Command Default	2 seconds
------------------------	-----------

Command Modes	Global configuration (config)
----------------------	-------------------------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines	If you do not specify the <i>hello-time</i> value, the value is calculated from the network diameter.
-------------------------	---

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

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

Related Commands	Command	Description
	show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst max-age

To set the max-age timer for all the instances on the device, use the **spanning-tree mst max-age** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst max-age *seconds*

no spanning-tree mst max-age

Syntax Description

<i>seconds</i>	Number of seconds to set the max-age timer for all the instances on the device. The range is from 6 to 40 in seconds.
----------------	---

Command Default

20 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Examples

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

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

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst max-hops

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

spanning-tree mst max-hops *hopnumber*
no spanning-tree mst max-hops

Syntax Description	<i>hopnumber</i>	Number of possible hops in the region before a BPDU is discarded. The range is from 1 to 255 hops.
Command Default	20 hops	
Command Modes	Global configuration (config)	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

Examples

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

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

Related Commands	Command	Description
	show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst pre-standard

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

spanning-tree mst pre-standard
no spanning-tree mst pre-standard

Syntax Description

This command has no arguments or keywords.

Command Default

The default is to automatically detect prestandard neighbors.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

Even with the default configuration, the port can receive both prestandard and standard BPDUs.

Prestandard BPDUs are based on the Cisco IOS Multiple Spanning Tree (MST) implementation that was created before the IEEE standard was finalized. Standard BPDUs are based on the finalized IEEE standard.

If you configure a port to transmit prestandard BPDUs only, the prestandard flag displays in the **show spanning-tree** commands. The variations of the prestandard flag are as follows:

- Pre-STD (or pre-standard in long format): This flag displays if the port is configured to transmit prestandard BPDUs and if a prestandard neighbor bridge has been detected on this interface.
- Pre-STD-Cf (or pre-standard (config) in long format): This flag displays if the port is configured to transmit prestandard BPDUs but a prestandard BPDU has not been received on the port, the autodetection mechanism has failed, or a misconfiguration, if there is no prestandard neighbor, has occurred.
- Pre-STD-Rx (or pre-standard (revd) in long format): This flag displays when a prestandard BPDU has been received on the port but it has not been configured to send prestandard BPDUs. The port will send prestandard BPDUs, but we recommend that you change the port configuration so that the interaction with the prestandard neighbor does not rely only on the autodetection mechanism.

If the MST configuration is not compatible with the prestandard (if it includes an instance ID greater than 15), only standard MST BPDUs are transmitted, regardless of the STP configuration on the port.

Examples

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

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


Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst priority

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

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

Syntax Description	<i>instance</i>	Instance identification number; valid values are from 0 to 4094.
	priority <i>priority</i>	Specifies the bridge priority; see the “Usage Guidelines” section for valid values and additional information.

Command Default	<i>priority</i> is 32768
-----------------	---------------------------------

Command Modes	Global configuration (config)
---------------	-------------------------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

You can set the bridge priority in increments of 4096 only. When you set the priority, valid values are **0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440**.

You can set the *priority* to **0** to make the switch root.

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

Examples

This example shows how to set the bridge priority:

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

Related Commands	Command	Description
	show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst root

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

```
spanning-tree mst instance root { primary | secondary } [ diameter diameter [ hello-time seconds ] ]
no spanning-tree mst instance root
```

Syntax Description		
<i>instance</i>		Instance identification number. The range is from 0 to 4094.
primary		Specifies the high enough priority (low value) to make the root of the spanning-tree instance.
secondary		Specifies the switch as a secondary root, should the primary root fail.
diameter <i>diameter</i>		(Optional) Specifies the timer values for the root switch that are based on the network diameter. The range is from 1 to 7.
hello-time <i>seconds</i>		(Optional) Specifies the duration between the generation of configuration messages by the root switch.

Command Default The **spanning-tree mst root** command has no default settings.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

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

The **spanning-tree mst root secondary** value is 16384.

The **diameter** *diameter* and **hello-time** *seconds* keywords and arguments are available for instance 0 only.

If you do not specify the *seconds* argument, the value for it is calculated from the network diameter.

Examples This example shows how to designate the primary root switch and timer values for an instance:

```
Router(config)# spanning-tree mst 0 root primary diameter 7 hello-time 2
Router(config)# spanning-tree mst 5 root primary
Router(config)#
```

Related Commands	Command	Description
	show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst simulate pvst global

To enable Per-VLAN Spanning Tree (PVST) simulation globally, enter the **spanning-tree mst simulate pvst global** command in global configuration mode. To disable PVST simulation globally, enter the **no** form of this command.

spanning-tree mst simulate pvst global
no spanning-tree mst simulate pvst global

Syntax Description This command has no arguments or keywords.

Command Default PVST simulation is enabled.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	Support for this command was introduced.

Usage Guidelines PVST simulation is enabled by default so that all interfaces on the device interoperate between Multiple Spanning Tree (MST) and Rapid Per-VLAN Spanning Tree Plus (PVST+). To prevent an accidental connection to a device that does not run MST as the default Spanning Tree Protocol (STP) mode, you can disable PVST simulation. If you disable PVST simulation, the MST-enabled port moves to the blocking state once it detects it is connected to a Rapid PVST+-enabled port. This port remains in the inconsistent state until the port stops receiving Bridge Protocol Data Units (BPDUs), and then the port resumes the normal STP transition process.

To override the global PVST simulation setting for a port, enter the **spanning-tree mst simulate pvst** interface command in the interface command mode.

Examples

This example shows how to prevent the switch from automatically interoperating with a connecting device that is running Rapid PVST+:

```
Device(config)#  
no spanning-tree mst simulate pvst global  
Device(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree pathcost method

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

spanning-tree pathcost method { long | short }
no spanning-tree pathcost method

Syntax Description

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

Command Default

short

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

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

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

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

spanning-tree port-priority

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

spanning-tree port-priority *port-priority*
no spanning-tree port-priority

Syntax Description	<i>port-priority</i> Port priority. The range is from 0 to 240 in increments of 16 . The default is 128.
---------------------------	--

Command Default The default port priority is 128.

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

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines The priority you set breaks the tie between two bridges to be designated as a root bridge.

Examples The following example shows how to increase the likelihood that spanning-tree instance 20 is chosen as the root-bridge on interface Ethernet 2/0:

```
Device(config)# interface ethernet 2/0
Device(config-if)# spanning-tree port-priority 20
Device(config-if)#
```

The following example shows how increase the likelihood that spanning-tree instance 20 is chosen as the root-bridge on an interface using an interface template:

```
Device# configure terminal
Device(config)# template user-templatel
Device(config-template)# spanning-tree port-priority 20
Device(config-template)# end
```

Related Commands	Command	Description
	show spanning-tree	Displays spanning-tree information for the specified spanning-tree instances.
	spanning-tree cost	Sets the path cost of the interface for STP calculations.
	spanning-tree portfast (global)	Enables PortFast mode, where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire.

Command	Description
spanning-tree uplinkfast	Enables the UplinkFast feature.
spanning-tree vlan	Configures STP on a per-VLAN basis.

spanning-tree portfast edge bpdupfilter default

To enable bridge protocol data unit (BPDU) filtering by default on all PortFast ports, use the **spanning-tree portfast edge bpdupfilter default** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree portfast edge bpdupfilter default
no spanning-tree portfast edge bpdupfilter default

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines The **spanning-tree portfast edge bpdupfilter** command enables BPDU filtering globally on PortFast ports. BPDU filtering prevents a port from sending or receiving any BPDUs.

You can override the effects of the **portfast edge bpdupfilter default** command by configuring BPDU filtering at the interface level.



Note Be careful when enabling BPDU filtering. The feature's functionality is different when you enable it on a per-port basis or globally. When enabled globally, BPDU filtering is applied only on ports that are in an operational PortFast state. Ports send a few BPDUs at linkup before they effectively filter outbound BPDUs. If a BPDU is received on an edge port, it immediately loses its operational PortFast status and BPDU filtering is disabled. When enabled locally on a port, BPDU filtering prevents the device from receiving or sending BPDUs on this port.



Caution Be careful when using this command. Using this command incorrectly can cause bridging loops.

Examples

This example shows how to enable BPDU filtering by default:

```
Device(config)#  
spanning-tree portfast edge bpdupfilter default  
Device(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

Command	Description
spanning-tree bpdupfilter	Enables BPDU filtering on the interface.

spanning-tree portfast edge bpduguard default

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

spanning-tree portfast edge bpduguard default
no spanning-tree portfast edge bpduguard default

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines



Caution Be careful when using this command. You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the device and network operation.

BPDU guard disables a port if it receives a BPDU. BPDU guard is applied only on ports that are PortFast enabled and are in an operational PortFast state.

Examples

This example shows how to enable BPDU guard by default:

```
Device(config)#  
spanning-tree portfast edge bpduguard default  
Device(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree bpduguard	Enables BPDU filtering on the interface.

spanning-tree portfast default

To enable PortFast by default on all access ports, use the **spanning-tree portfast {edge | network | normal} default** command in global configuration mode. To disable PortFast by default on all access ports, use the **no** form of this command.

spanning-tree portfast { edge [{ bpdudfilter | bpduguard }] | network | normal } default
no spanning-tree portfast { edge [{ bpdudfilter | bpduguard }] | network | normal } default

Syntax Description

bpdudfilter	Enables PortFast edge BPDU filter by default on all PortFast edge ports.
bpduguard	Enables PortFast edge BPDU guard by default on all PortFast edge ports.
edge	Enables PortFast edge mode by default on all switch access ports.
network	Enables PortFast network mode by default on all switch access ports.
normal	Enables PortFast normal mode by default on all switch access ports.

Command Default

PortFast is disabled by default on all access ports.

Command Modes

Global configuration (config)

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines



Note Be careful when using this command. You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the operation of the router or switch and the network.

An interface with PortFast mode enabled is moved directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-time delay.

You can enable PortFast mode on individual interfaces using the **spanning-tree portfast (interface)** command.

Examples

This example shows how to enable PortFast edge mode with BPDU Guard by default on all access ports:

```
Device(config)#
spanning-tree portfast edge bpduguard default
Device(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree portfast (interface)	Enables PortFast on a specific interface.

spanning-tree transmit hold-count

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

spanning-tree transmit hold-count *value*
no spanning-tree transmit hold-count

Syntax Description	<i>value</i>	Number of bridge protocol data units (BPDUs) that can be sent before pausing for 1 second. The range is from 1 to 20.
---------------------------	--------------	---

Command Default	<i>value</i> is 6
------------------------	--------------------------

Command Modes	Global configuration (config)
----------------------	-------------------------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines This command is supported on all spanning-tree modes.

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



Note Changing this parameter to a higher value may have a significant impact on CPU utilization, especially in rapid-Per-VLAN Spanning Tree (PVST) mode. Lowering this parameter could slow convergence in some scenarios. We recommend that you do not change the value from the default setting.

If you change the *value* setting, enter the **show running-config** command to verify the change.

If you delete the command, use the **show spanning-tree mst** command to verify the deletion.

Examples

This example shows how to specify the transmit hold count:

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

Related Commands	Command	Description
	show running-config	Displays the status and configuration of the module or Layer 2 VLAN.
	show spanning-tree mst	Display the information about the MST protocol.

spanning-tree uplinkfast

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

spanning-tree uplinkfast [**max-update-rate** *packets-per-second*]
no spanning-tree uplinkfast [**max-update-rate**]

Syntax Description	max-update-rate <i>packets-per-second</i> (Optional) Specifies the maximum rate (in packets per second) at which update packets are sent. The range is from 0 to 32000.	
Command Default	The defaults are as follows: <ul style="list-style-type: none">• UplinkFast is disabled.• <i>packets-per-second</i> is 150 packets per second.	
Command Modes	Global configuration (config)	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Usage Guidelines	Use the spanning-tree uplinkfast max-update-rate command to enable UplinkFast (if it is not already enabled) and change the rate at which update packets are sent. Use the no form of this command to return to the default rate.	
Examples	This example shows how to enable UplinkFast and set the maximum rate to 200 packets per second: Device(config)# spanning-tree uplinkfast max-update-rate 200 Device(config)#	
Related Commands	Command	Description
	show spanning-tree	Displays information about the spanning-tree state.

spanning-tree vlan

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

spanning-tree vlan *vlan-id* [{ **forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds* | **priority** *priority* | **root** [{ **primary** | **secondary** }]}]
no spanning-tree vlan *vlan-id* [{ **forward-time** | **hello-time** | **max-age** | **priority** | **root** }]

Syntax Description

<i>vlan id</i>	VLAN identification number. The range is from 1 to 4094.
forward-time <i>seconds</i>	(Optional) Sets the STP forward delay time. The range is from 4 to 30 seconds.
hello-time <i>seconds</i>	(Optional) Specifies the duration, in seconds, between the generation of configuration messages by the root switch. The range is from 1 to 10 seconds.
max-age <i>seconds</i>	(Optional) Sets the maximum number of seconds the information in a bridge packet data unit (BPDU) is valid. the range is from 6 to 40 seconds.
priority <i>priority</i>	(Optional) Sets the STP bridge priority. the range is from 0 to 65535.
root primary	(Optional) Forces this switch to be the root bridge.
root secondary	(Optional) Specifies this switch to act as the root switch should the primary root fail.

Command Default

The defaults are:

- **forward-time**: 15 seconds
- **hello-time**: 2 seconds
- **max-age**: 20 seconds
- **priority**: The default with IEEE STP enabled is 32768; the default with STP enabled is 128.
- **root** : No STP root

When you issue the **no spanning-tree vlan** *vlan_id* command, the following parameters are reset to their defaults:

- **priority**: The default with IEEE STP enabled is 32768; the default with STP enabled is 128.
- **hello-time**: 2 seconds
- **forward-time**: 15 seconds
- **max-age**: 20 seconds

Command Modes

Global configuration (config)

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines



Caution

- When disabling spanning tree on a VLAN using the **no spanning-tree vlan *vlan-id*** command, ensure that all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the same VLAN because switches and bridges with spanning tree enabled have incomplete information about the physical topology of the network.
- We do not recommend disabling spanning tree, even in a topology that is free of physical loops. Spanning tree is a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.

When you set the **max-age *seconds*** parameter, if a bridge does not hear bridge protocol data units (BPDUs) from the root bridge within the specified interval, it assumes that the network has changed and recomputes the spanning-tree topology.

The **spanning-tree root primary** command alters this switch's bridge priority to 8192. If you enter the **spanning-tree root primary** command and the switch does not become the root switch, then the bridge priority is changed to 100 less than the bridge priority of the current bridge. If the switch still does not become the root, an error results.

The **spanning-tree root secondary** command alters this switch's bridge priority to 16384. If the root switch should fail, this switch becomes the next root switch.

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

The **spanning-tree etherchannel guard misconfig** command detects two types of errors: misconfiguration and misconnection errors. A misconfiguration error is an error between the port-channel and an individual port. A misconnection error is an error between a switch that is channeling more ports and a switch that is not using enough Spanning Tree Protocol (STP) Bridge Protocol Data Units (BPDUs) to detect the error. In this case, the switch will only error disable an EtherChannel if the switch is a nonroot switch.

Examples

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

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

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

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

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

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


Related Commands

Command	Description
spanning-tree cost	Sets the path cost of the interface for STP calculations.
spanning-tree etherchannel guard misconfig	Displays an error message when a loop due to a channel misconfiguration is detected
spanning-tree port-priority	Sets an interface priority when two bridges tie for position as the root bridge.
spanning-tree uplinkfast	Enables the UplinkFast feature.
show spanning-tree	Displays spanning-tree information for the specified spanning-tree instances.

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

Command Default	By default, all interfaces are in Layer 2 mode.	
Command Modes	Interface configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	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.

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> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
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> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
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* }
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 Everest 16.5.1a	This command was introduced.

Usage Guidelines

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

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

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

Examples

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

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport access vlan 2
```

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}
no switchport 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 switches or between a switch and a router.

Command Default The default mode is **dynamic auto**.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	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** command in interface configuration mode to disable trunking.
- To enable trunking to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** commands in interface configuration mode 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** command in privileged EXEC mode and examining information in the *Administrative Mode* and *Operational Mode* rows.

Examples

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

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

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

```
Device> enable
Device# configure terminal
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> enable
Device# configure terminal
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

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 Everest 16.5.1a	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> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport nonegotiate
```

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

switchport trunk

To set the trunk characteristics when the interface is in trunking mode, use the **switchport trunk** command in interface configuration mode. To reset a trunking characteristic to the default, use the **no** form of this command.



Note The keyword **native vlan tag** is supported only on Cisco Catalyst 9500 Series Switches - High Performance.

switchport trunk {**allowed vlan** *vlan-list* | **native vlan** {**tag** | *vlan-id*} | **pruning vlan** *vlan-list*}
no switchport trunk {**allowed vlan** | **native vlan** [**tag**] | **pruning vlan**}

Syntax Description

allowed vlan <i>vlan-list</i>	Sets the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. See the Usage Guidelines for the <i>vlan-list</i> choices.
native vlan <i>vlan-id</i>	Sets the native VLAN for sending and receiving untagged traffic when the interface is in IEEE 802.1Q trunking mode. The range is 1 to 4094.
native vlan tag	Enables native VLAN tagging on a particular trunk port.
pruning vlan <i>vlan-list</i>	Sets the list of VLANs that are eligible for VTP pruning when in trunking mode. See the Usage Guidelines for the <i>vlan-list</i> choices.

Command Default

VLAN 1 is the default native VLAN ID on the port.
 The default for all VLAN lists is to include all VLANs.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.
Cisco IOS XE Gibraltar 16.11.1	This command was modified. The keyword native vlan tag was added for Cisco Catalyst 9500 High Performance series of switches.

Usage Guidelines

The *vlan-list* format is **all** | **none** | [**add** | **remove** | **except**] *vlan-atom* [,*vlan-atom*...]:

- **all** specifies all VLANs from 1 to 4094. This is the default. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
- **none** specifies an empty list. This keyword is not allowed on commands that require certain VLANs to be set or at least one VLAN to be set.
- **add** adds the defined list of VLANs to those currently set instead of replacing the list. Valid IDs are from 1 to 1005; extended-range VLANs (VLAN IDs greater than 1005) are valid in some cases.



Note You can add extended-range VLANs to the allowed VLAN list, but not to the pruning-eligible VLAN list.

Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.

- **remove** removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 1 to 1005; extended-range VLAN IDs are valid in some cases.



Note You can remove extended-range VLANs from the allowed VLAN list, but you cannot remove them from the pruning-eligible list.

- **except** lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.) Valid IDs are from 1 to 1005. Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- *vlan-atom* is either a single VLAN number from 1 to 4094 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.

Native VLANs:

- All untagged traffic received on an IEEE 802.1Q trunk port is forwarded with the native VLAN configured for the port.
- If a packet has a VLAN ID that is the same as the sending-port native VLAN ID, the packet is sent without a tag; otherwise, the switch sends the packet with a tag.
- **vlan dot1q tag native** global command needs to be enabled to execute the **switchport trunk native vlan tag** command.
- The **no** form of the **native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.

Allowed VLAN:

- To reduce the risk of spanning-tree loops or storms, you can disable VLAN 1 on any individual VLAN trunk port by removing VLAN 1 from the allowed list. When you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), Dynamic Trunking Protocol (DTP), and VLAN Trunking Protocol (VTP) in VLAN 1.
- The **no** form of the **allowed vlan** command resets the list to the default list, which allows all VLANs.

Trunk pruning:

- The pruning-eligible list applies only to trunk ports.
- Each trunk port has its own eligibility list.
- If you do not want a VLAN to be pruned, remove it from the pruning-eligible list. VLANs that are pruning-ineligible receive flooded traffic.
- VLAN 1, VLANs 1002 to 1005, and extended-range VLANs (VLANs 1006 to 4094) cannot be pruned.

This example shows how to enable native VLAN tagging on a trunk port:

```
Device> enable
Device(config)# interface HundredGigE 1/0/45
Device(config-if)# switchport trunk native vlan tag
```

This example shows how to configure VLAN 3 as the default for the port to send all untagged traffic:

```
Device> enable
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport trunk native vlan 3
```

This example shows how to add VLANs 1, 2, 5, and 6 to the allowed list:

```
Device> enable
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

This example shows how to remove VLANs 3 and 10 to 15 from the pruning-eligible list:

```
Device> enable
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport trunk pruning vlan remove 3,10-15
```

You can verify your settings 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 Everest 16.5.1a	This command was introduced.

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.

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

Part 2 - Checking the VLAN database:

```
Device> enable
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> enable
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> enable
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> enable
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
```

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** | **fast-hello error-reporting** | **message time** *message-timer-interval* | **recovery interval** *recovery-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.
	fast-hello error-reporting	Reports link failure on the console instead of err-disabling the affected Fast UDLD port.
	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.
	recovery interval <i>recovery-timer-interval</i>	Configures the error disable recovery timer value.

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 Everest 16.5.1a	This command was introduced.
	Cisco IOS XE Fuji 16.9.1	The fast-hello error-reporting keyword was added to the command. The recovery interval <i>recovery-timer-interval</i> keyword 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 *Software Configuration Guide (Catalyst 9500 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 reenabling UDLD globally.
- The **no udld port** interface configuration command followed by the **udld port** or **udld port aggressive** interface configuration command to reenabling 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> enable
Device# configure terminal
Device(config)# udld enable
```

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

udld fast-hello

To enable Fast UniDirectional Link Detection (UDLD) on an individual interface which has UDLD configured on it, use the **udld fast-hello** command in interface configuration mode.

udld fast-hello *message-timer-interval*

Syntax Description	<i>message-timer-interval</i> Configures time in milliseconds between sending of messages in steady state. The range is from 200 to 1000 milliseconds.	
Command Default	Fast UDLD is disabled by default.	
Command Modes	Interface configuration	
Command History	Release	Modification
	Cisco IOS XE Fuji 16.9.1	This command was introduced.
Usage Guidelines	<p>A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another device.</p> <p>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.</p> <p>Fast UDLD enables detection of unidirectional links within the span of a few hundred milliseconds to a second. Fast UDLD runs on top of the UDLD process without interrupting it. To configure a port in Fast UDLD mode, it must first be configured in UDLD mode.</p> <p>To enable Fast UDLD mode on a port, use the udld fast-hello<i>message-timer-interval</i> interface configuration command.</p>	

Examples

This example shows how to enable Fast UDLD on an port:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet6/0/1
Device(config-if)# udld fast-hello 200
```

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

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** command in global configuration mode, use the **udld port** command in interface configuration mode.

udld port [**aggressive** | **disable**]
no udld port [**aggressive**]

Syntax Description	<p>aggressive (Optional) Enables UDLD in aggressive mode on the specified interface.</p> <p>disable (Optional) Disables UDLD on the specified interface despite the global UDLD configuration.</p>						
Command Default	<p>On fiber-optic interfaces, UDLD is disabled and fiber-optic interfaces enable UDLD according to the state of the udld enable or udld aggressive command in global configuration mode.</p> <p>On nonfiber-optic interfaces, UDLD is disabled.</p>						
Command Modes	Interface configuration						
Command History	<table> <tr> <th data-bbox="342 921 1101 961">Release</th><th data-bbox="1101 921 1508 961">Modification</th></tr> <tr> <td data-bbox="342 982 1101 1022">Cisco IOS XE Everest 16.5.1a</td><td data-bbox="1101 982 1508 1022">This command was introduced.</td></tr> <tr> <td data-bbox="342 1043 1101 1083">Cisco IOS XE Fuji 16.9.1</td><td data-bbox="1101 1043 1508 1123">The disable keyword was introduced.</td></tr> </table>	Release	Modification	Cisco IOS XE Everest 16.5.1a	This command was introduced.	Cisco IOS XE Fuji 16.9.1	The disable keyword was introduced.
Release	Modification						
Cisco IOS XE Everest 16.5.1a	This command was introduced.						
Cisco IOS XE Fuji 16.9.1	The disable keyword was introduced.						
Usage Guidelines	<p>A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another device.</p> <p>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.</p> <p>To enable UDLD in normal mode, use the udld port command in interface configuration mode. To enable UDLD in aggressive mode, use the udld port aggressive command in interface configuration mode.</p> <p>Use the udld port disable command on fiber-optic ports to return control of UDLD to the udld enable command in global configuration mode or to disable UDLD on nonfiber-optic ports.</p> <p>Use the udld port aggressive command on fiber-optic ports to override the setting of the udld enable or udld aggressive command in global configuration mode. Use the udld port disable command on fiber-optic ports to remove this setting and to return control of UDLD enabling to the udld command in global configuration mode or to disable UDLD on nonfiber-optic ports.</p> <p>You can use these commands to reset an interface shut down by UDLD:</p> <ul style="list-style-type: none"> • The udld reset command in privileged EXEC mode resets all interfaces shut down by UDLD. • The shutdown and no shutdown command in interface configuration mode 						

- The **no udld enable** command in global configuration mode, followed by the **udld {aggressive | enable}** command in global configuration mode reenables UDLD globally.
- The **udld port disable** command in interface configuration mode, followed by the **udld port** or **udld port aggressive** command in interface configuration mode reenables UDLD on the specified interface.
- The **errdisable recovery cause udld** and **errdisable recovery interval *interval*** command in global configuration mode automatically recover from the UDLD error-disabled state.

This example shows how to enable UDLD on an port:

```
Device> enable
Device# configure terminal
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> enable
Device# configure terminal
Device(config)# interface gigabitethernet6/0/1
Device(config-if)# udld port disable
```

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

udd 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 **udd reset** command in privileged EXEC mode.

udd reset

Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Usage Guidelines	<p>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.</p> <p>This example shows how to reset all interfaces disabled by UDLD:</p> <pre>Device> enable Device# udd reset 1 ports shutdown by UDLD were reset.</pre>	

vtp mode

To configure the VLAN Trunking Protocol (VTP) device mode, use the **vtp mode** command. To revert to the default server mode, use the **no** form of this command.

vtp mode {**client** | **off** | **transparent**}
no vtp mode

Syntax Description		
client		Specifies the device as a client.
off		Specifies the device mode as off.
server		Specifies the device as a server.
transparent		Specifies the device mode as transparent.

Command Default	Server.
------------------------	---------

Command History	Release	Modification
	Cisco IOS XE Fuji 16.8.1a	This command was introduced.

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

Usage Guidelines VLAN Trunking Protocol (VTP) is a Cisco Proprietary Layer 2 messaging protocol used to distribute the VLAN configuration information across multiple devices within a VTP domain. Without VTP, you must configure VLANs in each device in the network. Using VTP, you configure VLANs on a VTP server and then distribute the configuration to other VTP devices in the VTP domain.

In VTP transparent mode, you can configure VLANs (add, delete, or modify) and private VLANs. VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. The VTP configuration revision number is always set to zero (0). Transparent switches do forward VTP advertisements that they receive out their trunk ports in VTP version 2.

A VTP device mode can be one of the following:

- **server** —You can create, modify, and delete VLANs and specify other configuration parameters, such as VTP version, for the entire VTP domain. VTP servers advertise their VLAN configuration to other switches in the same VTP domain and synchronize their VLAN configuration with other switches based on advertisements received over trunk links. VTP server is the default mode.



Note You can configure VLANs 1 to 1005. VLANs 1002 to 1005 are reserved for token ring in VTP version 2.

- **client** —VTP clients behave the same way as VTP servers, but you cannot create, change, or delete VLANs on a VTP client.

- transparent —You can configure VLANs (add, delete, or modify) and private VLANs. VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. Because of this, the VTP configuration revision number is always set to zero (0). Transparent switches do forward VTP advertisements that they receive out their trunk ports in VTP version 2.
- off —In the above three described modes, VTP advertisements are received and transmitted as soon as the switch enters the management domain state. In the VTP off mode, switches behave the same as in VTP transparent mode with the exception that VTP advertisements are not forwarded. You can use this VTP device to monitor the VLANs.



Note If you use the `no vtp mode` command to remove a VTP device, the device will be configured as a VTP server. Use the `vtp mode off` command to remove a VTP device.

Example

This example shows how to configure a VTP device in transparent mode and add VLANs 2, 3, and 4:

```
Device> enable
Device(config)#vtp mode transparent
Device(config)# vlan 2-4
```

Example

This example shows how to remove a device configured as a VTP device:

```
Device> enable
Device(config)# vtp mode off
```

Example

This example shows how to configure a VTP device as a VTP server and adds VLANs 2 and 3:

```
Device> enable
Device# vtp mode server
Device(config)# vlan 2,3
```

Example

This example shows how to configure a VTP device as a client:

```
Device> enable
Device# vtp mode client
```