shutdown

To disable an interface or Ethernet flow point (EFP) service instance, use the **shutdown** command in interface configuration or service-instance configuration mode. To restart a disabled interface or service instance, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Modes

Interface configuration or service-instance configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **shutdown** command causes a port or service instance to stop forwarding.

The **no shutdown** command has no effect if the port is a static-access port assigned to a VLAN that has been deleted, suspended, or shut down. The port must first be a member of an active VLAN before it can be re-enabled.

The **shutdown** command disables all functions on the specified interface or service instance.

This command also marks the interface. To see if an interface is disabled, use the **show interfaces** privileged EXEC command. An interface that has been shut down is shown as administratively down in the display.

Examples

These examples show how to disable and re-enable a port and a service instance:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# shutdown

Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no shutdown

Switch (config)# interface gigabitethernet0/1
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# shutdown

Switch (config)# interface gigabitethernet0/1
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# no shutdown
```

Related Commands

Command	Description
show interfaces	Displays the statistical information for all interfaces or for a specific interface.

shutdown vlan

To shut down (suspend) local traffic on the specified VLAN, use the **shutdown vlan** command in global configuration mode. To restart local traffic on the VLAN, use the **no** form of this command.

shutdown vlan *vlan-id*

no shutdown vlan *vlan-id*

Syntax Description

vlan-id	ID of the VLAN to be locally shut down. The range is 2 to 1001. VLANs defined as default VLANs (1 and 1002 to 1005), as well as extended-range VLANs (greater than 1005) cannot be shut down.

Defaults

No default is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use the shutdown VLAN configuration command to shut down local traffic on any VLAN, including extended-range VLANs (1006-4094).

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

Examples

This example shows how to shut down traffic on VLAN 2:

```
Switch(config)# shutdown vlan 2
```

Related Commands

Command	Description
shutdown (VLAN configuration)	Shuts down local traffic on the VLAN when in VLAN configuration mode (accessed by the **vlan** *vlan-id* global configuration command).

snmp mib rep trap-rate

To configure the sending of Resilient Ethernet Protocol (REP) SNMP traps when there is a link operational status or port role change, use the **snmp mib rep trap-rate** command in global configuration mode. To disable sending of the REP trap, use the **no** version of the command.

snmp mib rep trap-rate *value*

no snmp mib rep trap-rate

Syntax Description

trap-rate *value*	Sets the number of REP traps sent per second. The range is from 0 to 1000. The default is 0 (no limit imposed; a trap is sent at every occurrence).

Defaults

Sending REP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use this command to enable the switch to send REP specific traps corresponding to link operational status changes and port role changes.

Examples

This example configures the switch to send REP traps at a rate of 10 per second:

```
Switch(config)# snmp mib rep trap-rate 10
```

Related Commands

Command	Description
show running config	Verifies that REP traps are configured.

snmp-server enable traps

To enable the switch to send Simple Network Management Protocol (SNMP) notifications for various traps or inform requests to the network management system (NMS), use the **snmp-server enable traps** command in global configuration mode. To return to the default setting, use the **no** form of this command.

snmp-server enable traps [**alarms** [*severity*] | **auth-framework | bgp | bridge** [**newroot**] [**topologychange**] | **cef | config | copy-config | cpu threshold | entity | envmon** [**fan | shutdown | status | supply | temperature**] | **ethernet | ether oam | flash | hsrp | ipmulticast | mac-notification** [**change**] [**move**] [**threshold**] | **mpls | msdp | ospf** [**cisco-specific | errors | lsa | rate-limit | retransmit | state-change**] | **pim [invalid-pim-message | neighbor-change | rp-mapping-change] | rtr | snmp** [**authentication | coldstart | linkdown | linkup | warmstart**] | **storm-control trap-rate** *value* | **stpx** [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**] | **syslog | transceiver all | tty | vlan-membership | vlancreate | vlandelete**]

no snmp-server enable traps [**alarms** [*severity*] | **auth-framework | bgp | bridge** [**newroot**] [**topologychange**] | **cef | config | copy-config | cpu threshold | entity | envmon** [**fan | shutdown | status | supply | temperature**] | **ethernet | ether oam | flash | hsrp | ipmulticast | mac-notification** [**change**] [**move**] [**threshold**] | **mpls | msdp | ospf** [**cisco-specific | errors | lsa | rate-limit | retransmit | state-change**] | **pim [invalid-pim-message | neighbor-change | rp-mapping-change] | port-security** [**trap-rate** *value*] | **rtr | snmp** [**authentication | coldstart | linkdown | linkup | warmstart**] | **storm-control trap-rate** *value* | **stpx** [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**] | **syslog | transceiver all | tty | vlan-membership | vlancreate | vlandelete**]

Syntax Description

alarms *severity*	(Optional) Enables SNMP alarms traps. For severity, enter number **1** to **4** or enter one of these keywords: • **critical**—Service-affecting condition, severity 1. • **major**—Immediate action needed, severity 2. • **minor**—Minor warning conditions, severity 3. • **informational**—Informational notifications, severity 4.
auth-framework	Enables SNMP CISCO-AUTH-FRAMEWORK-MIB traps
bgp	(Optional) Enables Border Gateway Protocol (BGP) state-change traps. **Note** This keyword is supported only when the metro IP access image is running on the switch.
bridge [**newroot**] [**topologychange**]	(Optional) Generates Spanning Tree Protocol (STP) bridge MIB traps. The keywords have these meanings: • **newroot**—(Optional) Enables SNMP STP bridge MIB new root traps. • **topologychange**—(Optional) Enables SNMP STP bridge MIB topology change traps.

cef *type*	(Optional) Displays Cisco Express Forwarding (CEF) traps. You can optionally enter one of these keywords: • **inconsistency**—Enables SNMP CEF inconsistency traps. • **peer-fib-state-change**—Enables SNMP CEF peer FIB state-change traps. • **peer-state-change**—Enables SNMP CEF peer state-change traps. • **resource-failure**—Enables SNMP CEF resource-failure traps.
config	(Optional) Enables SNMP configuration traps.
copy-config	(Optional) Enable SNMP copy-configuration traps.
cpu threshold	(Optional) Allows CPU-related traps.
entity	(Optional) Enables SNMP entity traps.
envmon [**fan** | **shutdown** | **status** | **supply** | **temperature**]	Optional) Enables SNMP environmental traps. The keywords have these meanings: • **fan**—(Optional) Enables fan traps. • **shutdown**—(Optional) Enables environmental monitor shutdown traps. • **status**—(Optional) Enables SNMP environmental status-change traps. • **supply**—(Optional) Enables environmental monitor power-supply traps. • **temperature**—(Optional) Enables environmental monitor temperature traps.
ether oam	(Optional) Enables Ethernet OAM traps.
ethernet	(Optional) Enables SNMP Ethernet traps.
flash	(Optional) Enables SNMP flash notifications.
hsrp	(Optional) Enables Hot Standby Router Protocol (HSRP) traps.
ipmulticast	(Optional) Enables IP multicast routing traps.
mac-notification	(Optional) Enables MAC address notification traps.
change	(Optional) Enables MAC address change notification traps.
move	(Optional) Enables MAC address move notification traps.
mpls	(Optional) Enables multiprotocol label switching (MPLS) traps.
threshold	(Optional) Enables MAC address table threshold traps.
msdp	(Optional) Enables Multicast Source Discovery Protocol (MSDP) traps.
ospf [**cisco-specific** | **errors** | **lsa** | **rate-limit** | **retransmit** | **state-change**]	(Optional) Enables Open Shortest Path First (OSPF) traps. The keywords have these meanings: • **cisco-specific**—(Optional) Enables Cisco-specific traps. • **errors**—(Optional) Enables error traps. • **lsa**—(Optional) Enables link-state advertisement (LSA) traps. • **rate-limit**—(Optional) Enables rate-limit traps. • **retransmit**—(Optional) Enables packet-retransmit traps. • **state-change**—(Optional) Enables state-change traps.

pim [**invalid-pim-message** | **neighbor-change** | **rp-mapping-change**]	(Optional) Enables Protocol-Independent Multicast (PIM) traps. The keywords have these meanings: • **invalid-pim-message**—(Optional) Enables invalid PIM message traps. • **neighbor-change**—(Optional) Enables PIM neighbor-change traps. • **rp-mapping-change**—(Optional) Enables rendezvous point (RP)-mapping change traps.
rtr	(Optional) Enables SNMP Response Time Reporter traps.
snmp [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]	(Optional) Enables SNMP traps. The keywords have these meanings: • **authentication**—(Optional) Enables authentication trap. • **coldstart**—(Optional) Enables cold-start trap. • **linkdown**—(Optional) Enables linkdown trap. • **linkup**—(Optional) Enables linkup trap. • **warmstart**—(Optional) Enables warm-start trap.
storm-control trap-rate *value*	(Optional) Enables storm-control traps. Use the **trap-rat**e keyword to set the maximum number of storm-control traps sent per minute. The range is from 0 to 1000; the default is 0 (no limit is imposed; a trap is sent at every storm-control occurrence).
stpx [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**]	(Optional) Enables SNMP STPX MIB traps. The keywords have these meanings: • **inconsistency**—(Optional) Enables SNMP STPX MIB inconsistency update traps. • **root-inconsistency**—(Optional) Enables SNMP STPX MIB root inconsistency update traps. • **loop-inconsistency**—(Optional) Enables SNMP STPX MIB loop inconsistency update traps.
syslog	(Optional) Enables SNMP syslog traps.
transceiver all	(Optional) Enables SNMP traps for all supported Digital Optical Monitoring (DoM)-capable transceivers installed on the switch.
tty	(Optional) Sends TCP connection traps. This is enabled by default.
vlan-membership	(Optional) Enables SNMP VLAN membership traps.
vlancreate	(Optional) Enables SNMP VLAN-created traps.
vlandelete	(Optional) Enables SNMP VLAN-deleted traps.

Note Though visible in the command-line help strings, the **dot1x**, **energywise**, **event-manager**, **fru-ctrl insertion** and **removal**, and **vtp** keywords are not supported. The **snmp-server enable informs** global configuration command is not supported. To enable the sending of SNMP inform notifications, use the **snmp-server enable traps** global configuration command combined with the **snmp-server host** *host-addr* **informs** global configuration command.

Defaults

The sending of SNMP traps is disabled.

Command Modes Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

When supported, use the **snmp-server enable traps** command to enable sending of traps or informs.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

SNMP transceiver traps apply to SFPs that support DoM-capable transceivers installed on the switch. The sensor values are polled every 10 minutes, which is how often the user sees traps or alarms.

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

Examples This example shows how to send MPLS traps to the NMS:

```
Switch(config)# snmp-server enable traps mpls
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.
snmp-server host	Specifies the host that receives SNMP traps.

snmp-server host

To specify the recipient (host) of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host, use the **no** form of this command.

snmp-server host *host-addr* [**informs | traps**] [**version** {**1 | 2c | 3** {**auth | noauth| priv**}] [**vrf** *vrf-instance*] {*community-string* [*notification-type*]}

no snmp-server host *host-addr* [**informs | traps**] [**version** {**1 | 2c | 3** {**auth | noauth | priv**}] [**vrf** *vrf-instance*] *community-string*

Syntax Description

host-addr	Name or Internet address of the host (the targeted recipient).
udp-port *port*	(Optional) Configures the User Datagram Protocol (UDP) port number of the host to receive the traps. The range is from 0 to 65535.
informs | traps	(Optional) Sends SNMP traps or informs to this host.
version 1 | 2c | 3	(Optional) Version of the SNMP used to send the traps. These keywords are supported: **1**—SNMPv1. This option is not available with informs. **2c**—SNMPv2C. **3**—SNMPv3. These optional keywords can follow the Version 3 keyword: • **auth** (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. • **noauth** (Default). The noAuthNoPriv security level. This is the default if the [**auth | noauth | priv**] keyword choice is not specified. • **priv** (Optional). Enables Data Encryption Standard (DES) packet encryption (also called *privacy*). **Note** The **priv** keyword is available only when the cryptographic (encrypted) software image is installed.
vrf *vrf-instance*	(Optional) Virtual private network (VPN) routing instance and name for this host.
community-string	Password-like community string sent with the notification operation. Though you can set this string by using the **snmp-server host** command, we recommend that you define this string by using the **snmp-server community** global configuration command before using the **snmp-server host** command. **Note** The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

notification-type (Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent.

- **alarms**—Sends SNMP alarms traps.
- **auth-framework**—Sends NMP CISCO-AUTH-FRAMEWORK-MIB traps.
- **bgp**—Sends Border Gateway Protocol (BGP) state change traps. This keyword is valid only when the metro IP access image is installed on the switch.
- **bridge**—Sends SNMP Spanning Tree Protocol (STP) bridge MIB traps.
- **cef**—Sends cef traps.
- **config**—Sends SNMP configuration traps.
- **copy-config**—Sends SNMP copy configuration traps.
- **config-ctid** —Sends SNMP config-ctid traps.
- **cpu threshold**—Allows CPU-related traps.
- **eigrp**—Sends SNMP EIGRP traps
- **entity**— Sends SNMP entity traps.
- **envmon**—Sends environmental monitor traps.
- **ethernet-cfm**—Sends SNMP Ethernet CFM traps.
- **flash**—Sends SNMP FLASH notifications.
- **hsrp—**Sends SNMP Hot Standby Router Protocol (HSRP) traps.
- **ipmulticast—**Sends SNMP IP multicast routing traps.
- **isis**—Sends IS-IS traps.
- **license**—Sends license traps.
- **mac-notification—**Sends SNMP MAC notification traps.
- **mpls-fast-reroute**—Sends SNMP MPLS traffic engineering fast reroute traps.
- **mpls-ldp**—Sends SNMP MPLS label distribution protocol traps.
- **mpls-traffic-eng**—Sends SNMP MPLS traffic engineering traps.
- **mpls-vpn**—Sends SNMP MPLS Virtual Private Network traps.
- **msdp—**Sends SNMP Multicast Source Discovery Protocol (MSDP) traps.
- **ospf—**Sends Open Shortest Path First (OSPF) traps.
- **pim—**Sends SNMP Protocol-Independent Multicast (PIM) traps.
- **rtr—**Sends SNMP Response Time Reporter traps.
- **snmp—**Sends SNMP-type traps.
- **stpx—**Sends SNMP STP extended MIB traps.
- **syslog—**Sends SNMP syslog traps.
- **tty—**Sends TCP connection traps.
- **vlan-membership—** Sends SNMP VLAN membership traps.
- **vlancreate—**Sends SNMP VLAN-created traps.
- **vlandelete—**Sends SNMP VLAN-deleted traps.

Note Though visible in the command-line help strings, the **energywise**, **event manager**, **fru-ctrl**, and **vtp** keywords are not supported.

Defaults

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host.

If no **version** keyword is present, the default is Version 1.

If Version 3 is selected and no authentication keyword is entered, the default is the **noauth** (noAuthNoPriv) security level.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destinations.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Traps are also sent only once, but an inform might be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host. To enable multiple hosts, you must enter a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

If a local user is not associated with a remote host, the switch does not send informs for the **auth** (authNoPriv) and the **priv** (authPriv) authentication levels.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command is in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command replaces the first.

The **snmp-server host** command is used with the **snmp-server enable traps** global configuration command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable traps** command and

the **snmp-server host** command for that host must be enabled. Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled. Other notification types are enabled by a different command.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

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

Examples

This example shows how to configure a unique SNMP community string named *comaccess* for traps and prevent SNMP polling access with this string through access-list 10:

```
Switch(config)# snmp-server community comaccess ro 10
Switch(config)# snmp-server host 172.20.2.160 comaccess
Switch(config)# access-list 10 deny any
```

This example shows how to send the SNMP traps to the host specified by the name *myhost.cisco.com*. The community string is defined as *comaccess*:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com comaccess snmp
```

This example shows how to enable the switch to send all traps to the host *myhost.cisco.com* by using the community string *public*:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.
snmp-server enable traps	Enables SNMP notification for various trap types or inform requests.

snmp trap mac-notification change

To enable the Simple Network Management Protocol (SNMP) MAC address notification trap on a specific Layer 2 interface, use the **snmp trap mac-notification change** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

snmp trap mac-notification change {**added | removed**}

no snmp trap mac-notification change {**added | removed**}

Syntax Description

added	Enables the MAC notification trap whenever a MAC address is added on this interface.
removed	Enables the MAC notification trap whenever a MAC address is removed from this interface.

Defaults

By default, the traps for both address addition and address removal are disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Even though you enable the notification trap for a specific interface by using the **snmp trap mac-notification** command, the trap is generated only when you enable the **snmp-server enable traps mac-notification** and the **mac address-table notification** global configuration commands.

You can verify your settings by entering the **show mac address-table notification change interface** privileged EXEC command.

Examples

This example shows how to enable the MAC notification trap when a MAC address is added to a port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# snmp trap mac-notification change added
```

Related Commands

Command	Description
clear mac address-table notification	Clears the MAC address notification global counters.
mac address-table notification	Enables the MAC address notification feature.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or on the specified interface when the **interface** keyword is appended.
snmp-server enable traps	Sends the SNMP MAC notification traps when the **mac-notification** keyword is appended.

spanning-tree bpdufilter

To prevent an interface from sending or receiving bridge protocol data units (BPDUs), use the **spanning-tree bpdufilter** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree bpdufilter {**disable** | **enable**}

no spanning-tree bpdufilter

Syntax Description

disable	Disables BPDU filtering on the specified STP port.
enable	Enables BPDU filtering on the specified STP port.

Defaults

BPDU filtering is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can enable the BPDU filtering feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

Caution Enabling BPDU filtering on an STP port is the same as disabling spanning tree on it and can result in spanning-tree loops.

You can globally enable BPDU filtering on all Port Fast-enabled STP ports by using the **spanning-tree portfast bpdufilter default** global configuration command.

You can use the **spanning-tree bpdufilter** interface configuration command on an STP port to override the setting of the **spanning-tree portfast bpdufilter default** global configuration command.

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

Examples

This example shows how to enable the BPDU filtering feature on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree bpdufilter enable
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled STP ports or enables the Port Fast feature on all nontrunking STP ports.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an STP port and all its associated VLANs.

spanning-tree bpduguard

To put an interface in the error-disabled state when it receives a bridge protocol data unit (BPDU), use the **spanning-tree bpduguard** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree bpduguard {**disable** | **enable**}

no spanning-tree bpduguard

Syntax Description

disable	Disables BPDU guard on the specified STP port.
enable	Enables BPDU guard on the specified STP port.

Defaults

BPDU guard is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The BPDU guard feature provides a secure response to invalid configurations because you must manually put the STP port back in service. Use the BPDU guard feature in a service-provider network to prevent an interface from being included in the spanning-tree topology.

You can enable the BPDU guard feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), the rapid-PVST+, or the multiple spanning-tree (MST) mode.

You can globally enable BPDU guard on all Port Fast-enabled STP ports by using the **spanning-tree portfast bpduguard default** global configuration command.

You can use the **spanning-tree bpduguard** interface configuration command on an STP port to override the setting of the **spanning-tree portfast bpduguard default** global configuration command.

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

Examples

This example shows how to enable the BPDU guard feature on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree bpduguard enable
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled STP ports or enables the Port Fast feature on all nontrunking STP ports.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an STP port and all its associated VLANs.

spanning-tree cost

To set the path cost for spanning-tree calculations. use the **spanning-tree cost** command in interface configuration mode. If a loop occurs, spanning tree considers the path cost when selecting an interface to place in the forwarding state. To return to the default setting, use the **no** form of this command.

spanning-tree [**vlan** *vlan-id*] **cost** *cost*

no spanning-tree [**vlan** *vlan-id*] **cost**

Syntax Description

vlan *vlan-id*	(Optional) VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
cost	Path cost. The range is 1 to 200000000, with higher values meaning higher costs.

Defaults

The default path cost is computed from the STP interface bandwidth setting. These are the IEEE default path cost values:

- 1000 Mbps—1
- 100 Mbps—10
- 10 Mbps—100

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When you configure the cost, higher values represent higher costs.

If you configure an STP port with both the **spanning-tree vlan** *vlan-id* **cost** *cost* command and the **spanning-tree cost** *cost* command, the **spanning-tree vlan** *vlan-id* **cost** *cost* command takes effect.

You can verify your settings by entering the **show spanning-tree interface** *interface-id* privileged EXEC command.

Examples

This example shows how to set the path cost to 250 on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree cost 250
```

This example shows how to set a path cost to 300 for VLANs 10, 12 to 15, and 20:

```
Switch(config-if)# spanning-tree vlan 10,12-15,20 cost 300
```

Related Commands

Command	Description
show spanning-tree interface *interface-id*	Displays spanning-tree information for the specified interface.
spanning-tree port-priority	Configures an STP port priority.
spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree etherchannel guard misconfig

To display an error message when the switch detects an EtherChannel misconfiguration, use the **spanning-tree etherchannel guard misconfig** command in global configuration mode. To disable the feature, 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.

Defaults

EtherChannel guard is enabled on the switch.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When the switch detects an EtherChannel misconfiguration, this error message appears:

```
PM-4-ERR_DISABLE: Channel-misconfig error detected on [chars], putting [chars] in
err-disable state.
```

To show switch ports that are in the misconfigured EtherChannel, use the **show interfaces status err-disabled** privileged EXEC command. To verify the EtherChannel configuration on a remote device, use the **show etherchannel summary** privileged EXEC command on the remote device.

When a port is in the error-disabled state because of an EtherChannel misconfiguration, you can bring it out of this state by entering the **errdisable recovery cause channel-misconfig** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands.

You can verify your settings by entering the **show spanning-tree summary** privileged EXEC command.

Examples

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

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

Related Commands

Command	Description
errdisable recovery cause channel-misconfig	Enables the timer to recover from the EtherChannel misconfiguration error-disable state.
show etherchannel summary	Displays EtherChannel information for a channel as a one-line summary per channel-group.
show interfaces status err-disabled	Displays the interfaces in the error-disabled state.

spanning-tree extend system-id

To enable the extended system ID feature, use the **spanning-tree extend system-id** global configuration command.

spanning-tree extend system-id

Note Though visible in the command-line help strings, the **no** version of this command is not supported. You cannot disable the extended system ID feature.

Syntax Description

This command has no arguments or keywords.

Defaults

The extended system ID is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The switch supports the IEEE 802.1t spanning-tree extensions. Some of the bits previously used for the switch priority are now used for the extended system ID (VLAN identifier for the per-VLAN spanning-tree plus [PVST+] and rapid PVST+ or as an instance identifier for the multiple spanning tree [MST]).

The spanning tree uses the extended system ID, the switch priority, and the allocated spanning-tree MAC address to make the bridge ID unique for each VLAN or multiple spanning-tree instance.

Support for the extended system ID affects how you manually configure the root switch, the secondary root switch, and the switch priority of a VLAN. For more information, see the "spanning-tree mst root" and the "spanning-tree vlan" sections.

If your network consists of switches that do not support the extended system ID and switches that do support it, it is unlikely that the switch with the extended system ID support will become the root switch. The extended system ID increases the switch priority value every time the VLAN number is greater than the priority of the connected switches.

Related Commands

Command	Description
show spanning-tree summary	Displays a summary of spanning-tree interface states.
spanning-tree mst root	Configures the MST root switch priority and timers based on the network diameter.
spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree guard

To enable root guard or loop guard on all the VLANs associated with the selected port, use the **spanning-tree guard** command in interface configuration mode. Root guard restricts which interface is allowed to be the spanning-tree root port or the path-to-the root for the switch. Loop guard prevents alternate or root ports from becoming designated ports when a failure creates a unidirectional link. To return to the default setting, use the **no** form of this command.

spanning-tree guard {**loop** | **none** | **root**}

no spanning-tree guard

Syntax Description

loop	Enabled loop guard.
none	Disabled root guard or loop guard.
root	Enabled root guard.

Defaults

Root guard is disabled.

Loop guard is configured according to the **spanning-tree loopguard default** global configuration command (globally disabled).

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can enable root guard or loop guard when the switch is operating in the per-VLAN spanning-tree plus (PVST+), the rapid-PVST+, or the multiple spanning-tree (MST) mode.

When root guard is enabled, if spanning-tree calculations cause an interface to be selected as the root port, the interface transitions to the root-inconsistent (blocked) state to prevent the customer's switch from becoming the root switch or being in the path to the root. The root port provides the best path from the switch to the root switch.

When the **no spanning-tree guard** or the **no spanning-tree guard none** command is entered, root guard is disabled for all VLANs on the selected NNI. If this interface is in the root-inconsistent (blocked) state, it automatically transitions to the listening state.

Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send bridge protocol data units (BPDUs) on root or alternate ports. When the switch is operating in MST mode, BPDUs are not sent on nonboundary interfaces if the interface is blocked by loop guard in all MST instances. On a boundary interface, loop guard blocks the interface in all MST instances.

To disable root guard or loop guard, use the **spanning-tree guard none** interface configuration command on an STP interface. You cannot enable both root guard and loop guard at the same time.

You can override the setting of the **spanning-tree loopguard default** global configuration command by using the **spanning-tree guard loop** interface configuration command on an STP interface.

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

Examples

This example shows how to enable root guard on all the VLANs associated with the specified port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree guard root
```

This example shows how to enable loop guard on all the VLANs associated with the specified port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree guard loop
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree loopguard default	Prevents alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link.
spanning-tree mst cost	Configures the path cost for MST calculations.
spanning-tree mst port-priority	Configures an STP MST port priority.
spanning-tree mst root	Configures the MST root switch priority and timers based on the network diameter.
spanning-tree port-priority	Configures an STP port priority.
spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree link-type

To override the default link-type setting, which is determined by the duplex mode of the Spanning Tree Protocol (STP) port, and to enable rapid spanning-tree transitions to the forwarding state, use the **spanning-tree link-type** command in interface configuration mode. To return to the default setting, 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 link type of an STP port is point-to-point.
shared	Specifies that the link type of an STP port is shared.

Defaults

The switch derives the link type of an interface from the duplex mode. A full-duplex interface is considered a point-to-point link, and a half-duplex interface is considered a shared link.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can override the default setting of the link type by using the **spanning-tree link-type** command. For example, a half-duplex link can be physically connected point-to-point to a single interface on a remote switch running the Multiple Spanning Tree Protocol (MSTP) or the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol and be enabled for rapid transitions.

You can verify your setting by entering the **show spanning-tree mst interface** *interface-id* or the show **spanning-tree interface** *interface-id* privileged EXEC command.

Examples

This example shows how to specify the link type as shared (regardless of the duplex setting) and to prevent rapid transitions to the forwarding state:

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

Related Commands

Command	Description
clear spanning-tree counters	Restarts the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface.
show spanning-tree interface *interface-id*	Displays spanning-tree state information for the specified interface.
show spanning-tree mst interface *interface-id*	Displays MST information for the specified interface.

spanning-tree loopguard default

To enable loopguard by default on all interfaces with STP enabled, use the **spanning-tree loopguard default** command in global configuration mode. Enabling loopguard prevents alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. To return to the default setting, 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.

Defaults

Loop guard is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.252)EY	This command was introduced.

Usage Guidelines

You can enable the loop guard feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send bridge protocol data units (BPDUs) on root or alternate ports. When the switch is operating in MST mode, BPDUs are not sent on nonboundary interfaces if the interface is blocked by loop guard in all MST instances. On a boundary interface, loop guard blocks the interface in all MST instances.

Loop guard operates only on STP ports that the spanning tree identifies as point-to-point.

You can override the setting of the **spanning-tree loopguard default** global configuration command by using the **spanning-tree guard loop** interface configuration command.

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

Examples

This example shows how to globally enable loop guard:

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

Related Commands

Command	Description
show running-config	Displays the operating configuration.
spanning-tree guard loop	Enables the loop guard feature on all the VLANs associated with the specified STP port.

spanning-tree mode

To enable per-VLAN spanning-tree plus (PVST+), rapid PVST+, or multiple spanning tree (MST), use the **spanning-tree mode** command in global configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree mode {**mst** | **pvst** | **rapid-pvst**}

no spanning-tree mode

Syntax Description

mst	Enables MST and Rapid Spanning Tree Protocol (RSTP) (based on IEEE 802.1s and IEEE 802.1w).
pvst	Enables PVST+ (based on IEEE 802.1D).
rapid-pvst	Enables rapid PVST+ (based on IEEE 802.1w).

Defaults

The default mode is rapid PVST+.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The switch supports PVST+, rapid PVST+, and MSTP, but only one version can be active at any time: All VLANs run PVST+, all VLANs run rapid PVST+, or all VLANs run MSTP.

When you enable the MST mode, RSTP is automatically enabled.

Caution Changing spanning-tree modes can disrupt traffic because all spanning-tree instances are stopped for the previous mode and restarted in the new mode.

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

Examples

This example shows to enable MST and RSTP on the switch:

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

This example shows to enable PVST+ on the switch:

```
Switch(config)# spanning-tree mode pvst
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.

spanning-tree mst configuration

To enter multiple spanning-tree (MST) configuration mode through which you configure the MST region, 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.

Defaults

The default mapping is that all VLANs are mapped to the common and internal spanning-tree (CIST) instance (instance 0).

The default name is an empty string.

The revision number is 0.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **spanning-tree mst configuration** command enables the MST configuration mode. These configuration commands are available:

- **abort**: exits the MST region configuration mode without applying configuration changes.
- **exit**: exits the MST region configuration mode and applies all configuration changes.
- **instance** *instance-id* **vlan** *vlan-range*: maps VLANs to an MST instance. The range for the *instance-id* is 0 to 4094. The range for *vlan-range* is 1 to 4094. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.
- **name** *name*: sets the configuration name. The *name* string has a maximum length of 32 characters and is case sensitive.
- **no**: negates the **instance**, **name**, and **revision** commands or sets them to their defaults.
- **private-vlan**: Although visible in the command-line help strings, this command is not supported.
- **revision** *version*: sets the configuration revision number. The range is 0 to 65535.
- **show** [**current** | **pending**]: displays the current or pending MST region configuration.

In MST mode, the switch supports up to 16 MST instances. The number of VLANs that can be mapped to a particular MST instance is unlimited.

When you map VLANs to an MST instance, the mapping is incremental, and VLANs specified in the command are added to or removed from the VLANs that were previously mapped. To specify a range, use a hyphen; for example, **instance 1 vlan 1-63** maps VLANs 1 to 63 to MST instance 1. To specify a series, use a comma; for example, **instance 1 vlan 10, 20, 30** maps VLANs 10, 20, and 30 to MST instance 1.

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST by using the **no** form of the command.

For two or more switches to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

You can verify your settings by entering the **show pending** MST configuration command.

Examples

This example shows how to enter MST configuration mode, map VLANs 10 to 20 to MST instance 1, name the region *region1*, set the configuration revision to 1, display the pending configuration, apply the changes, and return to global configuration mode:

```
Switch# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
--------  ---------------------
0         1-9,21-4094
1         10-20
-------------------------------

Switch(config-mst)# exit
Switch(config)#
```

This example shows how to add VLANs 1 to 100 to the ones already mapped (if any) to instance 2, to move VLANs 40 to 60 that were previously mapped to instance 2 to the CIST instance, to add VLAN 10 to instance 10, and to remove all the VLANs mapped to instance 2 and map them to the CIST instance:

```
Switch(config-mst)# instance 2 vlan 1-100
Switch(config-mst)# no instance 2 vlan 40-60
Switch(config-mst)# instance 10 vlan 10
Switch(config-mst)# no instance 2
```

Related Commands

Command	Description
show spanning-tree mst configuration	Displays the MST region configuration.

spanning-tree mst cost

To set the path cost for multiple spanning-tree (MST) calculations, use the **spanning-tree mst cost** command in interface configuration mode. If a loop occurs, spanning tree considers the path cost when selecting an interface to put in the forwarding state. To return to the default setting, use the **no** form of this command.

spanning-tree mst *instance-id* **cost** *cost*

no spanning-tree mst *instance-id* **cost**

Syntax Description

instance-id	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.
cost	Path cost is 1 to 200000000, with higher values meaning higher costs.

Defaults

The default path cost is computed from the interface speed. Faster speeds have smaller costs.

- 10 Gb/s—2000
- 1000 Mb/s—20000
- 100 Mb/s—200000
- 10 Mbp\/s—2000000

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When you configure the cost, higher values represent higher costs.

You can verify your settings by entering the **show spanning-tree mst interface** *interface-id* privileged EXEC command.

Examples

This example shows how to set a path cost of 250 on a port associated with instances 2 and 4:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree mst 2,4 cost 250
```

Related Commands

Command	Description
show spanning-tree mst interface *interface-id*	Displays MST information for the specified interface.
spanning-tree mst port-priority	Configures an interface priority.
spanning-tree mst priority	Configures the switch priority for the specified spanning-tree instance.

spanning-tree mst forward-time

To set the forward-delay time for all multiple spanning-tree (MST) instances, use the **spanning-tree mst forward-time** command in global configuration mode. The forwarding time specifies how long each of the listening and learning states last before the interface begins forwarding. To return to the default setting, use the **no** form of this command.

spanning-tree mst forward-time *seconds*

no spanning-tree mst forward-time

Syntax Description

seconds	Length of the listening and learning states. The range is 4 to 30 seconds.

Defaults

The default is 15 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Changing the **spanning-tree mst forward-time** command affects all spanning-tree instances.

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Examples

This example shows how to set the spanning-tree forwarding time to 18 seconds for all MST instances:

```
Switch(config)# spanning-tree mst forward-time 18
```

Related Commands

Command	Description
show spanning-tree mst	Displays MST information.
spanning-tree mst hello-time	Sets the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree mst hello-time

To set the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages, use the **spanning-tree mst hello-time** command in global configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree mst hello-time *seconds*

no spanning-tree mst hello-time

Syntax Description

seconds	Interval between hello BPDUs sent by root switch configuration messages. The range is 1 to 10 seconds.

Defaults

The default is 2 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

After you set the **spanning-tree mst max-age** *seconds* global configuration command, if a switch does not receive BPDUs from the root switch within the specified interval, the switch recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

Changing the **spanning-tree mst hello-time** command affects all spanning-tree instances.

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Examples

This example shows how to set the spanning-tree hello time to 3 seconds for all multiple spanning-tree (MST) instances:

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

Related Commands

Command	Description
show spanning-tree mst	Displays MST information.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree mst max-age

To set the interval between messages that the spanning tree receives from the root switch, use the **spanning-tree mst max-age** command in global configuration mode. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputes the spanning-tree topology. To return to the default setting, use the **no** form of this command.

spanning-tree mst max-age *seconds*

no spanning-tree mst max-age

Syntax Description

seconds	Interval between messages the spanning tree receives from the root switch. The range is 6 to 40 seconds.

Defaults

The default is 20 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

After you set the **spanning-tree mst max-age** *seconds* global configuration command, if a switch does not receive BPDUs from the root switch within the specified interval, the switch recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

Changing the **spanning-tree mst max-age** command affects all spanning-tree instances.

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Examples

This example shows how to set the spanning-tree max-age to 30 seconds for all multiple spanning-tree (MST) instances:

```
Switch(config)# spanning-tree mst max-age 30
```

Related Commands

Command	Description
show spanning-tree mst	Displays MST information.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree mst max-hops

To set the number of hops in a region before the bridge protocol data unit (BPDU) is discarded and the information held for an interface is aged, use the **spanning-tree mst max-hops** command in global configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree mst max-hops *hop-count*

no spanning-tree mst max-hops

Syntax Description

hop-count	Number of hops in a region before the BPDU is discarded. The range is 1 to 255 hops.

Defaults

The default is 20 hops.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The root switch of the instance always sends a BPDU (or M-record) with a cost of 0 and the hop count set to the maximum value. When a switch receives this BPDU, it decrements the received remaining hop count by one and propagates the decremented count as the remaining hop count in the generated M-records. A switch discards the BPDU and ages the information held for the interface when the count reaches 0.

Changing the **spanning-tree mst max-hops** command affects all spanning-tree instances.

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Examples

This example shows how to set the spanning-tree max-hops to 10 for all multiple spanning-tree (MST) instances:

```
Switch(config)# spanning-tree mst max-hops 10
```

Related Commands

Command	Description
show spanning-tree mst	Displays MST information.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.

spanning-tree mst port-priority

To configure an interface priority, use the **spanning-tree mst port-priority** command in interface configuration mode. If a loop occurs, the Multiple Spanning Tree Protocol (MSTP) can find the interface to put in the forwarding state. To return to the default setting, use the **no** form of this command.

spanning-tree mst *instance-id* **port-priority** *priority*

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

Syntax Description

instance-id	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.
priority	The range is 0 to 240 in increments of 16. Valid priority values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority.

Defaults

The default is 128.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can assign higher priority values (lower numerical values) to STP port that you want selected first and lower priority values (higher numerical values) that you want selected last. If all STP ports have the same priority value, the multiple spanning tree (MST) puts the interface with the lowest interface number in the forwarding state and blocks other interfaces.

You can verify your settings by entering the **show spanning-tree mst interface** *interface-id* privileged EXEC command.

Examples

This example shows how to increase the likelihood that the interface associated with spanning-tree instances 20 and 22 is placed into the forwarding state if a loop occurs:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree mst 20,22 port-priority 0
```

Related Commands

Command	Description
show spanning-tree mst interface *interface-id*	Displays MST information for the specified interface.
spanning-tree mst cost	Sets the path cost for MST calculations.
spanning-tree mst priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree mst pre-standard

To configure a port to send only prestandard bridge protocol data units (BPDUs), use the **spanning-tree mst pre-standard** command in interface configuration command. To return to the default setting, 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 state is automatic detection of prestandard neighbors.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The port can accept both prestandard and standard BPDUs. If the neighbor types are mismatched, only the common and internal spanning tree (CIST) runs on this interface.

Note If a switch port is connected to a switch running prestandard Cisco IOS software, you *must* use the **spanning-tree mst pre-standard** interface configuration command on the port. If you do not configure the port to send only prestandard BPDUs, the Multiple STP (MSTP) performance might diminish.

When the port is configured to automatically detect prestandard neighbors, the *prestandard* flag always appears in the **show spanning-tree mst** commands.

You can verify your settings by entering the **show spanning-tree mst** privileged EXEC command.

Examples

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

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

Related Commands

Command	Description
show spanning-tree mst *instance-id*	Displays multiple spanning-tree (MST) information, including the *prestandard* flag, for the specified interface.

spanning-tree mst priority

To set the switch priority for the specified spanning-tree 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-id* **priority** *priority*

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

Syntax Description

instance-id	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.
priority	Sets the switch priority for the specified spanning-tree instance. This setting affects the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch. The range is 0 to 61440 in increments of 4096. Valid priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.

Defaults

The default is 32768.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Examples

This example shows how to set the spanning-tree priority to 8192 for multiple spanning-tree instances (MST) 20 to 21:

```
Switch(config)# spanning-tree mst 20-21 priority 8192
```

Related Commands

Command	Description
show spanning-tree mst *instance-id*	Displays MST information for the specified interface.
spanning-tree mst cost	Sets the path cost for MST calculations.
spanning-tree mst port-priority	Configures an interface priority.

spanning-tree mst root

Use the **spanning-tree mst root** global configuration command to configure the multiple spanning-tree (MST) root switch priority and timers based on the network diameter. Use the **no** form of this command to return to the default settings.

spanning-tree mst *instance-id* **root** {**primary** | **secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]

no spanning-tree mst *instance-id* **root**

Syntax Description

instance-id	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.
root primary	Forces this switch to be the root switch.
root secondary	Sets this switch to be the root switch should the primary root switch fail.
diameter *net-diameter*	(Optional) Sets the maximum number of switches between any two end stations. The range is 2 to 7. This keyword is available only for MST instance 0.
hello-time *seconds*	(Optional) Sets the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds. This keyword is available only for MST instance 0.

Defaults

The primary root switch priority is 24576.

The secondary root switch priority is 28672.

The hello time is 2 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use the **spanning-tree mst** *instance-id* **root** command only on backbone switches.

When you enter the **spanning-tree mst** *instance-id* **root** command, the software tries to set a high enough priority to make this switch the root of the spanning-tree instance. Because of the extended system ID support, the switch sets the switch priority for the instance to 24576 if this value will cause this switch to become the root for the specified instance. If any root switch for the specified instance has a switch priority lower than 24576, the switch sets its own priority to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree mst** *instance-id* **root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch fails, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768 and are therefore unlikely to become the root switch).

You can verify your settings by entering the **show spanning-tree mst** *instance-id* privileged EXEC command.

Examples

This example shows how to configure the switch as the root switch for instance 10 with a network diameter of 4:

```
Switch(config)# spanning-tree mst 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for instance 10 with a network diameter of 4:

```
Switch(config)# spanning-tree mst 10 root secondary diameter 4
```

Related Commands

Command	Description
show spanning-tree mst *instance-id*	Displays MST information for the specified instance.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree port-priority

To configure an interface priority, use the **spanning-tree port-priority** command in interface configuration mode. If a loop occurs, spanning tree can find the interface to put in the forwarding state. To return to the default setting, use the **no** form of this command.

spanning-tree [**vlan** *vlan-id*] **port-priority** *priority*

no spanning-tree [**vlan** *vlan-id*] **port-priority**

Syntax Description

vlan *vlan-id*	(Optional) VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
priority	Number from 0 to 240, in increments of 16. Valid values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority.

Defaults

The default is 128.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If the variable *vlan-id* is omitted, the command applies to the spanning-tree instance associated with VLAN 1.

You can set the priority on a VLAN that has no interfaces assigned to it. The setting takes effect when you assign the STP port to the VLAN.

If you configure an STP port with both the **spanning-tree vlan** *vlan-id* **port-priority** *priority* command and the **spanning-tree port-priority** *priority* command, the **spanning-tree vlan** *vlan-id* **port-priority** *priority* command takes effect.

You can verify your settings by entering the **show spanning-tree interface** *interface-id* privileged EXEC command.

Examples

This example shows how to increase the likelihood that a port will be put in the forwarding state if a loop occurs:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree vlan 20 port-priority 0
```

This example shows how to set the port-priority value on VLANs 20 to 25:

```
Switch(config-if)# spanning-tree vlan 20-25 port-priority 0
```

Related Commands

Command	Description
show spanning-tree interface *interface-id*	Displays spanning-tree information for the specified interface.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree portfast (global configuration)

To globally enable bridge protocol data unit (BPDU) filtering on Port Fast-enabled interfaces, the BPDU guard feature on Port Fast-enabled STP ports, or the Port Fast feature on all nontrunking STP ports., use the **spanning-tree portfast** command in global configuration mode. The BPDU filtering feature prevents the switch STP port from sending or receiving BPDUs. The BPDU guard feature puts Port Fast-enabled STP ports that receive BPDUs in an error-disabled state. To return to the default settings, use the **no** form of this command.

spanning-tree portfast {**bpdufilter default** | **bpduguard default** | **default**}

no spanning-tree portfast {**bpdufilter default** | **bpduguard default** | **default**}

Syntax Description

bpdufilter default	Globally enables BPDU filtering on Port Fast-enabled STP ports, and prevent the switch STP port connected to end stations from sending or receiving BPDUs.
bpduguard default	Globally enables the BPDU guard feature on Port Fast-enabled STP ports, and place the STP ports that receive BPDUs in an error-disabled state.
default	Globally enables the Port Fast feature on all nontrunking STP ports. When the Port Fast feature is enabled, the STP port changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes.

Defaults

The BPDU filtering, the BPDU guard, and the Port Fast features are disabled on all NNIs or ENIs unless they are individually configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can enable these features when the switch is operating in the per-VLAN spanning-tree plus (PVST+), the rapid-PVST+, or the multiple spanning-tree (MST) mode.

Use the **spanning-tree portfast bpdufilter default** global configuration command to globally enable BPDU filtering on STP ports that are Port Fast-enabled. The STP ports still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs. You should globally enable BPDU filtering on a switch so that hosts connected to switch STP ports do not receive BPDUs. If a BPDU is received on a Port Fast-enabled STP port, the interface loses its Port Fast-operational status and BPDU filtering is disabled.

You can override the **spanning-tree portfast bpdufilter default** global configuration command on an STP port by using the **spanning-tree bdpufilter** interface configuration command.

Caution Enabling BPDU filtering on an STP port is the same as disabling spanning tree on it and can result in spanning-tree loops.

Use the **spanning-tree portfast bpduguard default** global configuration command to globally enable BPDU guard on STP ports that are in a Port Fast-operational state. In a valid configuration, Port Fast-enabled STP ports do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled STP port signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the STP port in the error-disabled state. The BPDU guard feature provides a secure response to invalid configurations because you must manually put the STP port back in service. Use the BPDU guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

You can override the **spanning-tree portfast bpduguard default** global configuration command by using the **spanning-tree bdpuguard** interface configuration command on an STP port.

Use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking STP ports. Configure Port Fast only on STP ports that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation. A Port Fast-enabled STP port moves directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-delay time.

You can override the **spanning-tree portfast default** global configuration command by using the **spanning-tree portfast** interface configuration command on an STP port. You can use the **no spanning-tree portfast default** global configuration command to disable Port Fast on all STP ports unless they are individually configured with the **spanning-tree portfast** interface configuration command.

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

Examples

This example shows how to globally enable the BPDU filtering feature:

```
Switch(config)# spanning-tree portfast bpdufilter default
```

This example shows how to globally enable the BPDU guard feature:

```
Switch(config)# spanning-tree portfast bpduguard default
```

This example shows how to globally enable the Port Fast feature on all nontrunking interfaces:

```
Switch(config)# spanning-tree portfast default
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.
spanning-tree bpdufilter	Prevents an interface from sending or receiving BPDUs.
spanning-tree bpduguard	Puts an STP port in the error-disabled state when it receives a BPDU.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an STP port in all its associated VLANs.

spanning-tree portfast (interface configuration)

To enable the Port Fast feature on an STP port in all its associated VLANs, use the **spanning-tree portfast** command in interface configuration mode. When the Port Fast feature is enabled, the STP port changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes. To return to the default setting, use the **no** form of this command.

spanning-tree portfast [**disable** | **trunk**]

no spanning-tree portfast

Syntax Description

disable	(Optional) Disables the Port Fast feature on the specified interface.
trunk	(Optional) Enables the Port Fast feature on a trunking interface.

Defaults

The Port Fast feature is disabled on all ports.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use this feature only on STP ports that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation.

To enable Port Fast on trunk ports, you must use the **spanning-tree portfast trunk** interface configuration command. The **spanning-tree portfast** command is not supported on trunk ports.

You can enable this feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), the rapid-PVST+, or the multiple spanning-tree (MST) mode.

This feature affects all VLANs on the STP port.

An interface with the Port Fast feature enabled is moved directly to the spanning-tree forwarding state without the standard forward-time delay.

You can use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking interfaces. However, the **spanning-tree portfast** interface configuration command can override the global setting.

If you configure the **spanning-tree portfast default** global configuration command, you can disable Port Fast on an STP port that is not a trunk interface by using the **spanning-tree portfast disable** interface configuration command.

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

Examples

This example shows how to enable the Port Fast feature on a port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree portfast
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.
spanning-tree bpdufilter	Prevents an interface from sending or receiving bridge protocol data units (BPDUs).
spanning-tree bpduguard	Puts an interface in the error-disabled state when it receives a BPDU.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled STP ports or enables the Port Fast feature on all nontrunking STP ports.

spanning-tree vlan

To configure spanning tree on a per-VLAN basis, use the **spanning-tree vlan** command in global configuration mode. To return to the default setting, 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**} [**diameter** *net-diameter* [**hello-time** *seconds*]]]

no spanning-tree vlan *vlan-id* [**forward-time** | **hello-time** | **max-age** | **priority** | **root**]

Syntax Description

vlan-id	VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
forward-time *seconds*	(Optional) Sets the forward-delay time for the specified spanning-tree instance. The forwarding time specifies how long each of the listening and learning states last before the interface begins forwarding. The range is 4 to 30 seconds.
hello-time *seconds*	(Optional) Sets the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds.
max-age *seconds*	(Optional) Sets the interval between messages the spanning tree receives from the root switch. If a switch does not receive a BPDU message from the root switch within this interval, it recomputes the spanning-tree topology. The range is 6 to 40 seconds.
priority *priority*	(Optional) Sets the switch priority for the specified spanning-tree instance. This setting affects the likelihood that this switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch. The range is 0 to 61440 in increments of 4096. Valid priority values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.
root primary	(Optional) Forces this switch to be the root switch.
root secondary	(Optional) Sets this switch to be the root switch should the primary root switch fail.
diameter *net-diameter*	(Optional) Sets the maximum number of switches between any two end stations. The range is 2 to 7.

Defaults

Spanning tree is enabled on all VLANs.

The forward-delay time is 15 seconds.

The hello time is 2 seconds.

The max-age is 20 seconds.

The primary root switch priority is 24576.

The secondary root switch priority is 28672.

Command Modes Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines Disabling the STP causes the VLAN to stop participating in the spanning-tree topology. STP ports that are administratively down remain down. Received BPDUs are forwarded like other multicast frames. The VLAN does not detect and prevent loops when STP is disabled.

You can disable the STP on a VLAN that is not currently active and verify the change by using the **show running-config** or the **show spanning-tree vlan** *vlan-id* privileged EXEC command. The setting takes effect when the VLAN is activated.

When disabling or re-enabling the STP, you can specify a range of VLANs that you want to disable or enable.

When a VLAN is disabled and then enabled, all assigned VLANs continue to be its members. However, all spanning-tree bridge parameters are returned to their previous settings (the last setting before the VLAN was disabled).

You can enable spanning-tree options on a VLAN that has no STP ports assigned to it. The setting takes effect when you assign interfaces to it.

When setting the **max-age** *seconds,* if a switch does not receive BPDUs from the root switch within the specified interval, it recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

The **spanning-tree vlan** *vlan-id* **root** command should be used only on backbone switches.

When you enter the **spanning-tree vlan** *vlan-id* **root** command, the software checks the switch priority of the current root switch for each VLAN. Because of the extended system ID support, the switch sets the switch priority for the specified VLAN to 24576 if this value will cause this switch to become the root for the specified VLAN. If any root switch for the specified VLAN has a switch priority lower than 24576, the switch sets its own priority for the specified VLAN to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree vlan** *vlan-id* **root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch should fail, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768, and therefore, are unlikely to become the root switch).

You can verify your settings by entering the **show spanning-tree vlan** *vlan-id* privileged EXEC command.

Examples This example shows how to disable the STP on VLAN 5:

```
Switch(config)# no spanning-tree vlan 5
```

You can verify your setting by entering the **show spanning-tree** privileged EXEC command. In this instance, VLAN 5 does not appear in the list.

This example shows how to set the spanning-tree forwarding time to 18 seconds for VLANs 20 and 25:

```
Switch(config)# spanning-tree vlan 20,25 forward-time 18
```

This example shows how to set the spanning-tree hello-delay time to 3 seconds for VLANs 20 to 24:

```
Switch(config)# spanning-tree vlan 20-24 hello-time 3
```

This example shows how to set spanning-tree max-age to 30 seconds for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 max-age 30
```

This example shows how to reset the **max-age** parameter to the default value for spanning-tree instance 100 and 105 to 108:

```
Switch(config)# no spanning-tree vlan 100, 105-108 max-age
```

This example shows how to set the spanning-tree priority to 8192 for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 priority 8192
```

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

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

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

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

Related Commands

Command	Description
show spanning-tree vlan	Displays spanning-tree information.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree guard	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
spanning-tree port-priority	Sets an interface priority.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled STP ports or enables the Port Fast feature on all nontrunking STP ports.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an STP port in all its associated VLANs.

speed

To specify the speed of a 10/100/1000 Mbps port, use the **speed** interface configuration command. To return the port to its default value, use the **no** or **default** form of this command.

speed {**10** | **100** | **1000** | **auto** [**10** | **100** | **1000**] | **nonegotiate**}

no speed

Note You cannot configure the speed on small form-factor pluggable (SFP) module ports or on 10 Gigabit Ethernet ports, but you can configure the speed to not negotiate (**nonegotiate**) if they are connected to a device that does not support autonegotiation. See "Usage Guidelines" for exceptions when a 1000BASE-T SFP module is in the SFP module slot.

Syntax Description

10	Port runs at 10 Mbps.
100	Port runs at 100 Mbps.
1000	Port runs at 1000 Mbps. This option is valid and visible only on 10/100/1000 Mbps-ports.
auto	Port automatically detects the speed it should run at based on the port at the other end of the link. If you use the **10**, **100**, or **1000** keywords with the **auto** keyword, the port only autonegotiates at the specified speeds.
nonegotiate	Autonegotiation is disabled, and the port runs at 1000 Mbps. (The 1000BASE-T SFP does not support the **nonegotiate** keyword.)

Defaults

The default is **auto**.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can configure the Gigabit Ethernet port speed as 10, 100, or 1000 Mbps.

You cannot configure the speed on 10 Gigabit Ethernet ports, but you can configure the speed to not negotiate (**nonegotiate**) if they are connected to a device that does not support autonegotiation.

When a 1000BASE-T SFP module is in the SFP module slot, you can configure the speed as **10**, **100**, **1000**, or auto but not to **nonegotiate**.

Except for the 1000BASE-T SFP modules, if an SFP module port is connected to a device that does not support autonegotiation, you can configure the speed to not negotiate (**nonegotiate**).

If the speed is set to **auto**, the switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The duplex setting remains as configured on each end of the link, which could result in a duplex setting mismatch.

If both ends of the line support autonegotiation, we highly recommend the default autonegotiation settings. If one interface supports autonegotiation and the other end does not, do use the **auto** setting on the supported side, but set the duplex and speed on the other side.

Caution Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.

Note For guidelines on setting the switch speed and duplex parameters, see the software configuration guide for this release.

You can verify the configuration by entering the **show interfaces** privileged EXEC command.

Examples

This example shows how to set speed on a port to 100 Mbps:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed 100
```

This example shows how to set a port to autonegotiate at only 10 Mbps:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto 10
```

This example shows how to set a port to autonegotiate at only 10 or 100 Mbps:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto 10 100
```

Related Commands

Command	Description
duplex	Specifies the duplex mode of operation.
show interfaces	Displays the statistical information specific to all interfaces or to a specific interface.

storm-control

To enable broadcast, multicast, or unicast storm control and to set threshold levels on an interface, use the **storm-control** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

storm-control {{**broadcast** | **multicast** | **unicast**} **level** {*rising_level* [*falling_level*]} | **bps** *bps* [*bps-low*] | **pps** *pps* [*pps-low*]}} | {**action** {**shutdown** | **trap**}}

no storm-control {{**broadcast** | **multicast** | **unicast**} **level**} | {**action** {**shutdown** | **trap**}}

Syntax Description

broadcast	Enables broadcast storm control on the interface.
multicast	Enables multicast storm control on the interface.
unicast	Enables unicast storm control on the interface.
level *rising_level* [*falling_level*]	Specifies the rising and falling suppression levels as a percentage of total bandwidth of the port. • *rising_level*—The rising threshold level for broadcast, multicast, or unicast traffic as a percentage (up to two decimal places) of the bandwidth. The port blocks traffic when the rising threshold is reached. The range is 0.00 to 100.00. • (Optional) *falling_level—T*he falling threshold level as a percentage (up to two decimal places) of the bandwidth. *This value must be less than or equal to the rising suppression value.* The port forwards traffic when traffic drops below this level. If you do not configure a falling suppression level, it is set to the rising suppression level. The range is 0.00 to 100.00. If you set the threshold to the maximum value (100 percent), no limit is placed on the traffic. If you set the threshold to 0.0, all broadcast, multicast, and unicast traffic on that port is blocked.
level bps *bps* [*bps-low*]	Specifies the rising and falling suppression levels as a rate in bits per second at which traffic is received on the port. • **bps** *bps*—The rising threshold level for broadcast, multicast, or unicast traffic in bits per second (up to one decimal place). The port blocks traffic when the rising threshold is reached. The range is 0.0 to 10000000000.0. • (Optional) *bps-low*—The falling threshold level in bits per second (up to one decimal place). It can be less than or equal to the rising threshold level. The port forwards traffic when traffic drops below this level. The range is 0.0 to 10000000000.0. For **bps** settings, you can use metric suffixes such as k, m, and g for large number thresholds.

level pps *pps* [*pps-low*]	Specifies the rising and falling suppression levels as a rate in packets per second at which traffic is received on the port. • **pps** *pps*—The rising threshold level for broadcast, multicast, or unicast traffic in packets per second (up to one decimal place). The port blocks traffic when the rising threshold is reached. The range is 0.0 to 10000000000.0. • (Optional) *pps-low*,—The falling threshold level in packets per second (up to one decimal place). It can be less than or equal to the rising threshold level. The port forwards traffic when traffic drops below this level. The range is 0.0 to 10000000000.0. For **pps** settings, you can use metric suffixes such as k, m, and g for large number thresholds.\
action {**shutdown** | **trap**}	Specifies the action to be taken when a storm is detected. The default action is to filter traffic and to not send an Simple Network Management Protocol (SNMP) trap. The keywords have these meanings: • **shutdown**—Error-disables the port during a storm. • **trap**—Sends an SNMP trap when a storm occurs.

Defaults

Broadcast, multicast, and unicast storm control are disabled.

The default action is to filter traffic and to not send an SNMP trap.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Storm control is supported on physical interfaces. When you configure storm control on an interface, it also affects traffic on Ethernet Flow Points (EFPs) configured on the interface.

You can also configure storm control on an EtherChannel. When storm control is configured on an EtherChannel, the storm control settings propagate to the EtherChannel physical interfaces.

The storm-control suppression level can be entered as a percentage of total bandwidth of the port, as a rate in packets per second at which traffic is received, or as a rate in bits per second at which traffic is received.

When specified as a percentage of total bandwidth, a suppression value of 100 percent means that no limit is placed on the specified traffic type. A value of **level 0 0** means that all broadcast, multicast, or unicast traffic on that port is blocked. Storm control is enabled only when the rising suppression level is less than 100 percent. If no other storm-control configuration is specified, the default action is to filter the traffic causing the storm and to send no SNMP traps.

Note When the storm control threshold for multicast traffic is reached, all multicast traffic except control traffic, such as bridge protocol data unit (BDPU) and Cisco Discovery Protocol (CDP) frames, are blocked. However, the switch does not differentiate between routing updates, such as Open Shortest Path First (OSPF) and regular multicast data traffic, so both types of traffic are blocked.

The **trap** and **shutdown** options are independent of each other.

If you configure the action to be taken as shutdown (the port is error-disabled during a storm) when a packet storm is detected, you must use the **no shutdown** interface configuration command to bring the interface out of this state. If you do not specify the **shutdown** action, specify the action as **trap** (the switch generates a trap when a storm is detected).

When a storm occurs and the action is to filter traffic, if the falling suppression level is not specified, the switch blocks all traffic until the traffic rate drops below the rising suppression level. If the falling suppression level is specified, the switch blocks traffic until the traffic rate drops below this level.

When a broadcast storm occurs and the action is to filter traffic, the switch blocks only broadcast traffic.

You can verify the configuration by entering the **show storm-control** privileged EXEC command.

For more information, see the software configuration guide for this release.

Examples

This example shows how to enable broadcast storm control with a 75.5-percent rising suppression level:

This example shows how to enable unicast storm control on a port with an 87-percent rising suppression level and a 65-percent falling suppression level:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# storm-control unicast level 87 65
```

This example shows how to enable broadcast address storm control on a port to a level of 20 percent. When the broadcast traffic exceeds the configured level of 20 percent of the total available bandwidth of the port within the traffic-storm-control interval, the switch drops all broadcast traffic until the end of the traffic-storm-control interval:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# storm-control broadcast level 20
```

Related Commands

Command	Description
show storm-control	Displays broadcast, multicast, or unicast storm control settings on all interfaces or on a specified interface.

switchport

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

switchport

no switchport

Note The **switchport** commands are not available on interfaces with service instances configured.

Syntax Description

This command has no arguments or keywords.

Defaults

By default, all interfaces are in Layer 2 (switching) mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	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 enter the **no switchport** command and then assign an IP address to the routed port.

If an interface is configured as a Layer 3 interface, to process traffic through the CPU, you must first enter the **switchport** command with no keywords before configuring switching characteristics on the port. Then you can enter additional **switchport** commands with keywords, as shown on the pages that follow.

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

When you enter the **switchport** (or **no switchport**) command without keywords on an interface, the configuration information for the affected interface might be lost, and the interface returned to its default configuration.

The **switchport** commands are not available on interfaces with service instances configured.

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

Examples

This example shows how to change an interface from a Layer 2 (switching) port to a Layer 3 (routed) port.

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

This example shows how to return the port to switching mode:

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

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
show running-config	Displays the operating configuration.

switchport access vlan

To configure a port as a static-access port, use the **switchport access vlan** command in interface configuration mode. If the switchport mode is set to **access** (by using the **switchport mode** interface configuration command), use this command to set the port to operate as a member of the specified VLAN. To reset the access VLAN mode to the default VLAN for the switch, use the **no** form of this command.

switchport access vlan {*vlan-id* | **dynamic**}

no switchport access vlan

Note This command is not available on interfaces with service instances configured.

Syntax Description

vlan-id	Configure the interface as a static access port with the VLAN ID of the access mode VLAN; the range is 1 to 4094.

Note Although visible in the command-line help, the **dynamic** keyword is not supported.

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

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

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

An access port can be assigned to only one VLAN.

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

Examples

This example shows how to change a Layer 2 interface in access mode to operate in VLAN 2 instead of the default VLAN.

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

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
switchport mode	Configures the VLAN membership mode of a port.

switchport backup interface

To configure Flex Links, a pair of interfaces that provide backup to each other, use the **switchport backup interface** command in interface configuration mode on a Layer 2 interface. To remove the Flex Links configuration, use the **no** form of this command.

switchport backup interface [*interface-id* | **GigabitEthernet** *interface-id* | **Port-channel** *interface-id*] {**mmu primary vlan** *interface-id* | **multicast fast-convergence** | **preemption** {**delay** *delay-time* | **mode**} | **prefer vlan** *vlan-id*}

no switchport backup interface [**GigabitEthernet** *interface-id* | **Port-channel** *interface-id*] {**mmu primary vlan** *interface-id* | **multicast fast-convergence** | **preemption** {**delay** *delay-time* | **mode**} | **prefer vlan** *vlan-id*}

Note This command is not available on interfaces with service instances configured.

Syntax Description

GigabitEthernet	GigabitEthernet port name.
Port-channel	Ethernet Channel interface.
interface-id	Specifies that the Layer 2 interface to act as a backup link to the interface being configured. The interface can be a physical interface or port channel. The port-channel range is 1 to 26.
mmu primary vlan *vlan-id*	MAC-address move update. Configure the MAC move update (MMU) for a backup interface pair, using the MAC-address move update primary VLAN ID. The VLAN range is 1 to 4094.
multicast fast-convergence	Enables multicast Fast-convergence.
preemption	Configures a preemption scheme for a backup interface pair.
delay *delay-time*	(Optional) Specifies a preemption delay; the valid values are 1 to 300 seconds.
mode	Specifies a preemption mode as bandwidth, forced, or off.
prefer vlan *vlan-id*	Specifies that VLANs are carried on the backup interfaces of a Flex Link pair. VLAN ID range is 1 to 4,094.
off	(Optional) Specifies that no preemption occurs from backup to active.
delay *delay-time*	(Optional) Specifies a preemption delay; the valid values are 1 to 300 seconds.

Defaults

The default is to have no Flex Links defined. Preemption mode is off. No preemption occurs. Preemption delay is set to 35 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

With Flex Links configured, one link acts as the primary interface and forwards traffic, while the other interface is in standby mode, ready to begin forwarding traffic if the primary link shuts down. The interface being configured is referred to as the active link; the specified interface is identified as the backup link. The feature provides an alternative to the Spanning Tree Protocol (STP), allowing users to turn off STP and still retain basic link redundancy.

- This command is available only for Layer 2 interfaces.
- You can configure only one Flex Link backup link for any active link, and it must be a different interface from the active interface.
- An interface can belong to only one Flex Link pair. An interface can be a backup link for only one active link. An active link cannot belong to another Flex Link pair.
- A backup link does not have to be the same type (Fast Ethernet or Gigabit Ethernet, for instance) as the active link. However, you should configure both Flex Links with similar characteristics so that there are no loops or changes in behavior if the standby link begins to forward traffic.
- Neither of the links can be a port that belongs to an EtherChannel. However, you can configure two port channels (EtherChannel logical interfaces) as Flex Links, and you can configure a port channel and a physical interface as Flex Links, with either the port channel or the physical interface as the active link.
- If STP is configured on the switch, Flex Links do not participate in STP in all valid VLANs. If STP is not running, be sure that there are no loops in the configured topology.

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

Examples

This example shows how to configure two interfaces as Flex Links:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport backup interface gigabitethernet0/2
Switch(config-if)# end
```

This example shows how to configure the interface to always preempt the backup:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport backup interface gigabitethernet0/2 preemption forced
Switch(config-if)# end
```

This example shows how to configure the interface preemption delay time:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport backup interface gigabitethernet0/2 preemption delay 150
Switch(config-if)# end
```

This example shows how to configure the interface as the MMU primary VLAN:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport backup interface gigabitethernet0/2 mmu primary vlan 1021
Switch(config-if)# end
```

This example shows how to configure preferred VLANs:

```
Switch(config)# interface gigabitethernet 0/6
Switch(config-if)# switchport backup interface gigabitethernet 0/8 prefer vlan 60,100-120
```

In this example, VLANs 60, and 100 to 120 are configured on the switch:

```
Switch(config)# interface gigabitEthernet 0/6
Switch(config-if)# switchport backup interface gigabitEthernet 0/8 prefer vlan 60,100-120
```

When both interfaces are up, Gi0/6 forwards traffic for VLANs 1 to 50, and Gi0/8 forwards traffic for VLANs 60 and 100 to 120.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/6    GigabitEthernet0/8    Active Up/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

When a Flex Link interface goes down (LINK_DOWN), VLANs preferred on this interface are moved to the peer interface of the Flex Link pair. In this example, if interface Gi0/6 goes down, Gi0/8 carries all VLANs of the Flex Link pair.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/6    GigabitEthernet0/8    Active Down/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

When a Flex Link interface comes up, VLANs preferred on this interface are blocked on the peer interface and moved to the forwarding state on the interface that has just come up. In this example, if interface Gi0/6 comes up, VLANs preferred on this interface are blocked on the peer interface Gi0/8 and forwarded on Gi0/6.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/6    GigabitEthernet0/8    Active Up/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

This example shows how to configure multicast fast-convergence on interface Gi0/11:

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 0/11
Switch(config-if)# switchport backup interface gigabitEthernet 0/12 multicast
fast-convergence
Switch(config-if)# end
```

```
Switch# show interfaces switchport backup detail

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/11   GigabitEthernet0/12   Active Up/Backup Standby
        Preemption Mode  : off
        Multicast Fast Convergence  : On
        Bandwidth : 1000000 Kbit (Gi0/11), 1000000 Kbit (Gi0/12)
        Mac Address Move Update Vlan : auto
```

Related Commands

Command	Description
show interfaces [*interface-id*] **switchport backup**	Displays the configured Flex Links and their status on the switch or for the specified interface.

switchport block

To prevent unknown multicast or unicast packets from being forwarded, use the **switchport block** command in interface configuration mode. To allow forwarding unknown multicast or unicast packets, use the **no** form of this command.

switchport block {**multicast | unicast**}

no switchport block {**multicast | unicast**}

Note This command is not available on interfaces with service instances configured.

Syntax Description

multicast	Specifies that unknown multicast traffic should be blocked. **Note** Only pure Layer 2 multicast traffic is blocked. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.
unicast	Specifies that unknown unicast traffic should be blocked.

Defaults

Unknown multicast and unicast traffic is not blocked.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

By default, all traffic with unknown MAC addresses is sent to all ports. You can block unknown multicast or unicast traffic on protected or nonprotected ports. If unknown multicast or unicast traffic is not blocked on a protected port, there could be security issues.

With multicast traffic, the port blocking feature blocks only pure Layer 2 packets. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.

Blocking unknown multicast or unicast traffic is not automatically enabled on protected ports; you must explicitly configure it.

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

For more information about blocking packets, see the software configuration guide for this release.

Examples

This example shows how to block unknown multicast traffic on an interface:

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

Related Commands

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

switchport host

To optimize a Layer 2 port for a host connection, use the **switchport host** command in interface configuration mode. The **no** form of this command has no affect on the system.

switchport host

Note This command is not available on interfaces with service instances configured.

Syntax Description

This command has no arguments or keywords.

Defaults

The default is for the port to not be optimized for a host connection.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

To optimize the port for a host connection, the **switchport host** command sets switch port mode to access, enables spanning tree Port Fast, and disables channel grouping. Only an end station can accept this configuration.

Because spanning tree Port Fast is enabled, you should enter the **switchport host** command only on ports that are connected to a single host. Connecting other switches, hubs, concentrators, or bridges to a fast-start port can cause temporary spanning-tree loops.

Enable the **switchport host** command to decrease the time that it takes to start up packet forwarding.

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

Examples

This example shows how to optimize the port configuration for a host connection:

```
Switch(config-if)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
Switch(config-if)#
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including switchport mode.

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 default, use the **no** form of this command.

switchport mode {**access** | **trunk**}

no switchport mode

Note This command is not available on interfaces with service instances configured.

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 unencapsulated (nontagged) frames. An access port can be assigned to only one VLAN.
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.

Defaults

The default mode is **access**.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	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. If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.

Access ports and trunk ports are mutually exclusive.

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

Examples

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

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode access
```

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

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode trunk
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport access vlan	Configures a port as a static-access or dynamic-access port.
switchport trunk	Configures the trunk characteristics when an interface is in trunking 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.

switchport trunk {**allowed vlan** *vlan-list* | **native vlan** *vlan-id*}

no switchport trunk {**allowed vlan | native vlan**}

Note This command is not available on interfaces with service instances configured.

Syntax Description

allowed vlan *vlan-list*	Sets the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. See the following *vlan-list* format. The **none** keyword is not valid. The default is **all**.
native vlan *vlan-id*	Sets the native VLAN for sending and receiving untagged traffic when the interface is in 802.1Q trunking mode. The range is 1 to 4094.

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

- **all** specifies all VLANs from 1 to 4094. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
- **none** means 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 4094. You can add extended-range VLANs (VLAN IDs greater than 1005) to the allowed 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 4094; extended-range VLAN IDs are valid.

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

Defaults

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
12.2(52)EY	This command was introduced.

Usage Guidelines

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.
- 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), and Link Aggregation Control Protocol (LACP) in VLAN 1.
- The **no** form of the **allowed vlan** command resets the list to the default list, which allows all VLANs.

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

Examples

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

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk native vlan 3
```

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

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport mode	Configures the VLAN membership mode of a port.

system env temperature threshold alert

To configure the delta value from the shutdown threshold for a high or low alert to be generated, use the **system env temperature threshold alert** command in global configuration mode. To return to the default, use the **no** form of this command.

system env temperature threshold alert {**high | low**} *value*

no system env temperature threshold alert {**high | low**}

Syntax Description

high	Configures the high temperature threshold when an alert should be sent.
low	Configures the low temperature threshold when an alert should be sent.
value	Specifies the delta value in degrees Celsius from the shutdown threshold for an high or low alert to be generated. The range is from 20 to 40 degrees Celcius.

Defaults

The default value is 10 degrees Celcius. An alert is sent when the temperature is 10 degrees higher or lower than the shutdown threshold.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Examples

This example sets 15 degrees Celcius as the high value delta from the shutdown threshold so that an alert is sent if the temperature is 15 degrees higher than the shutdown threshold:

```
Switch(config)# system env temperature threshold alert high 15
Switch(config)#
```

Related Commands

Command	Description
show env temperature status	Displays the switch temperature status and thresholds.

test cable-diagnostics tdr

To run the Time Domain Reflector (TDR) feature on an interface, use the **test cable-diagnostics tdr** command in privileged EXEC mode.

test cable-diagnostics tdr interface *interface-id*

Note TDR is supported only on GigabitEthernet 10/100/100 ports.

interface-id	Specifies the interface on which to run TDR.

Defaults

There is no default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can use the TDR feature to diagnose and resolve cabling problems. TDR is supported only on copper Ethernet 10/100 or 10/100/1000 ports. It is not supported on small form-factor pluggable (SFP) module ports or on 10 Gigabit Ethernet ports. For more information about TDR, see the software configuration guide for this release.

After you run TDR by using the **test cable-diagnostics tdr interface** *interface-id* command, use the **show cable-diagnostics tdr interface** *interface-id* privileged EXEC command to display the results.

Examples

This example shows how to run TDR on an interface:

```
Switch# test cable-diagnostics tdr interface gigabitethernet0/2
TDR test started on interface Gi0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

If you enter the **test cable-diagnostics tdr interface** *interface-id* command on an interface that has a link status of up and a speed of 10 or 100 Mbps, these messages appear:

```
Switch# test cable-diagnostics tdr interface gigabitethernet0/3
TDR test on Gi0/9 will affect link state and traffic
TDR test started on interface Gi0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

Related Commands

Command	Description
show cable-diagnostics tdr	Displays the TDR results.

traceroute mac

To display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address, use the **traceroute mac** command in privileged EXEC mode.

traceroute mac [**interface** *interface-id*] {*source-mac-address*} **[interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]

Syntax Description

interface *interface-id*	(Optional) Specifies an interface on the source or destination switch.
source-mac-address	Specifies the MAC address of the source switch in hexadecimal format.
destination-mac-address	Specifies the MAC address of the destination switch in hexadecimal format.
vlan *vlan-id*	(Optional) Specifies the VLAN on which to trace the Layer 2 path that the packets take from the source switch to the destination switch. Valid VLAN IDs are 1 to 4094.
detail	(Optional) Specifies that detailed information appears.

Defaults

There is no default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all the switches in the network. Do not disable CDP.

When the switch detects a device in the Layer 2 path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and an error message appears.

The **traceroute mac** command output shows the Layer 2 path when the specified source and destination addresses belong to the same VLAN. If you specify source and destination addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.

If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination MAC addresses:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Source 0000.0201.0601 found on con6[ME-3400-24TS] (2.2.6.6)
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5                 (2.2.5.5        )  :    Gi0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows how to display the Layer 2 path by using the **detail** keyword:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[ME-3400-24TS] (2.2.6.6)
ME-3400-24TS / 2.2.6.6 :
        Gi0/2 [auto, auto] => Gi0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination switches:

```
Switch# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
0000.0201.0201
Source 0000.0201.0601 found on con6[ME-3400-24TS] (2.2.6.6)
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5                 (2.2.5.5        )  :    Gi0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows the Layer 2 path when the switch is not connected to the source switch:

```
Switch# traceroute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source .....
Source 0000.0201.0501 found on con5[ME-3400-24TS] (2.2.5.5)
con5 / ME-3400-24TS/ 2.2.5.5 :
        Gi0/1 [auto, auto] => Gi0/3 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows the Layer 2 path when the switch cannot find the destination port for the source MAC address:

```
Switch# traceroute mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
```

This example shows the Layer 2 path when the source and destination devices are in different VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace aborted.
```

This example shows the Layer 2 path when the destination MAC address is a multicast address:

```
Switch# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
```

This example shows the Layer 2 path when source and destination switches belong to multiple VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
```

Related Commands

Command	Description
traceroute mac ip	Displays the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname.

traceroute mac ip

To display the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname, use the **traceroute mac ip** command in privileged EXEC mode.

traceroute mac ip {*source-ip-address* | *source-hostname*} {*destination-ip-address* | *destination-hostname*} [**detail**]

Syntax Description

source-ip-address	Specifies the IP address of the source switch as a 32-bit quantity in dotted-decimal format.
destination-ip-address	Specifies the IP address of the destination switch as a 32-bit quantity in dotted-decimal format.
source-hostname	Specifies the IP hostname of the source switch.
destination-hostname	Specifies the IP hostname of the destination switch.
detail	(Optional) Specifies that detailed information appears.

Defaults

There is no default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all the switches in the network. Do not disable CDP.

When the switch detects an device in the Layer 2 path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

The **traceroute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses are in the same subnet. When you specify the IP addresses, the switch uses Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.

- If an ARP entry exists for the specified IP address, the switch uses the associated MAC address and identifies the physical path.
- If an ARP entry does not exist, the switch sends an ARP query and tries to resolve the IP address. The IP addresses must be in the same subnet. If the IP address is not resolved, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the **detail** keyword:

```
Switch# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / ME-3400-24TS-/ 2.2.6.6 :
        Gi0/1 [auto, auto] => Gi0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the source and destination hostnames:

```
Switch# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5                 (2.2.5.5        )  :    Gi0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

This example shows the Layer 2 path when ARP cannot associate the source IP address with the corresponding MAC address:

```
Switch# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

Related Commands

Command	Description
shutdown	Displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.

udld

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

udld {**aggressive** | **enable** | **message time** *message-timer-interval*}

no udld {**aggressive** | **enable** | **message**}

Syntax Description

aggressive	Enables UDLD in aggressive mode on all fiber-optic interfaces.
enable	Enables UDLD in normal mode on all fiber-optic interfaces.
message time *message-timer-interval*	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 7 to 90 seconds.

Defaults

UDLD is disabled on all interfaces.

The message timer is set at 60 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links. For information about normal and aggressive modes, see the "Understanding UDLD" section in the software configuration guide for this release.

If you change the message time between probe packets, you are making a trade-off 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 re-enable UDLD globally

- The **no udld port** interface configuration command followed by the **udld port** or **udld port aggressive** interface configuration command to re-enable 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

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

Examples

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

```
Switch(config)# udld enable
```

Related Commands

Command	Description
show udld	Displays UDLD administrative and operational status for all ports or the specified port.
udld port	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command.
udld reset	Resets all interfaces shut down by UDLD and permits traffic to again pass through.

udld port

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

udld port [**aggressive | disable**]

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

Syntax Description

aggressive	Enables UDLD in aggressive mode on the specified interface.
disable	Disables UDLD on this interface despite the global UDLD setting.

Defaults

On fiber-optic interfaces, UDLD is not enabled, not in aggressive mode, and not disabled. For this reason, fiber-optic interfaces enable UDLD according to the state of the **udld enable** or **udld aggressive** global configuration command.

On nonfiber-optic interfaces, UDLD is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52EY	This command was introduced.

Usage Guidelines

A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch. If the port is a user network interface (UNI) or enhanced network interface (ENI), you must use the **no shutdown** interface configuration command to enable it before using the **udld port** command. UNIs and ENIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

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 “Configuring UDLD” chapter in the software configuration guide for this release.

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

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

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

For UDLD to peer with a neighbor on a port that has an Ethernet Virtual Connection (EVC) EFP service instance configured, you need to enter the **l2 protocol peer udld** service-instance configuration command on the service instance.

If the switch software detects a small form-factor pluggable (SFP) module change and the port changes from fiber optic to nonfiber optic or the reverse, all configurations are maintained.

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 re-enable UDLD globally.
- The **no udld port** interface configuration command followed by the **udld port or udld port aggressive** interface configuration command to re-enable 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.

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

Examples

This example shows how to enable UDLD on an port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# udld port
```

This example shows how to configure UDLD peering on an EFP service instance:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# udld port
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan none
Switch(config-if)# service instance 1 Ethernet
Switch(config-if-srv)# encapsulation untagged
Switch(config-if-srv)# l2protocol peer udld
Switch(config-if-srv)# bridge-domain 10
Switch(config-if-srv)# end
```

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

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no udld port
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.
show udld	Displays UDLD administrative and operational status for all ports or the specified port.
udld	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
udld reset	Resets all interfaces shut down by UDLD and permits traffic to again pass through.

udld reset

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

udld reset

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If the interface configuration is still enabled for UDLD, these ports begin to run UDLD again and are disabled for the same reason if the problem has not been corrected.

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

Examples

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

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

Related Commands

Command	Description
show running-config	Displays the operating configuration.
show udld	Displays UDLD administrative and operational status for all ports or the specified port.
udld	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
udld port	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command.

uni count

To set the user-network interface (UNI) count for an Ethernet virtual connection (EVC), use the **uni count** command in EVC configuration mode. To return to the default setting, use the **no** form of this command.

uni count *value* [**multipoint**]

no uni count

Syntax Description

value	Sets the number of UNIs in the EVC. The range is from 2 to 1024. The default is 2.
multipoint	(Optional) Selects point-to-multipoint service. This keyword is visible only when you enter a **uni count** value of 2. • If you do not enter a value or if you enter 1 or 2, the service defaults to point-to-point service. If you enter 2, you can configure point-to-multipoint service. • If you enter a **uni count** value of 3 or greater, the service is point-to-multipoint.

Defaults

The default UNI count is 2. The default service, if you do not enter a UNI count, is point-to-multipoint.

Command Modes

EVC configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The UNI count determines the type of service in the EVC.

- If the command is not entered, the UNI count defaults to 2 and the service defaults to point-to-point service.
- If you manually enter a value of 2, you can leave the service at the default or can configure point-to-multipoint service by entering the **multipoint** keyword.
- If you enter a value of 3 or greater, the service is point-to-multipoint.

You should know the correct number of maintenance end points (MEPs) in the domain. If you enter a UNI count value greater than the actual number of endpoints, the UNI status shows as partially active even if all endpoints are up. If you enter a UNI count less than the actual number of endpoints, UNI status shows as active, even if all endpoints are not up.

Caution Configuring a UNI count does not prevent you from configuring more endpoints than the configured count. For example, if you configure a UNI count of five, but you create ten MEPs, any five MEPs in the domain can go down without the status changing to Partially Active.

Examples

This example shows how to a UNI count of two with point-to-multipoint service:

```
Switch(config)# ethernet evc test1
Switch(config-evc)# uni count 2 multipoint
```

Related Commands

Command	Description
ethernet evc *evc-id*	Defines an EVC and enters EVC configuration mode.

uni-vlan

To configure a VLAN as a user network interface (UNI) community or isolated VLAN, use the **uni-vlan** command in VLAN configuration mode. UNIs on a switch that are assigned to a community VLAN can exchange packets with one another.

uni-vlan {**community** | **isolated**}

no uni-vlan

Note This command has no effect on the switch. All ports on the switch are network node interfaces (NNIs), which can always exchange packets with one another.

Syntax Description

community	Designate the UNI-ENI VLAN as a community VLAN.
isolated	Designate the UNI-ENI VLAN as an isolated VLAN.

Defaults

The default VLAN configuration is UNI-ENI isolated VLAN.

Command Modes

VLAN configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

This command has no effect on the switch because all ports on the switch are NNIs.

Related Commands

Command	Description
show interfaces status	Displays the status of interfaces, including the VLANs to which they belong.

violate-action

To set actions for a policy-map class for packets that exceed the peak information rate (PIR), use the **violate-action** command in policy-map class police configuration mode. To cancel the action or to return to the default action, use the **no** form of this command.

violate-action {**drop** | **set-cos-transmit** *new cos-value* | **set-discard-class-transmit** *new discard-value* | **set-dscp-transmit** *new dscp-value* | **set-mpls-exp-imposition-transmit** *new-imposition-exp-value* | **set-mpls-exp-topmost transmit** *new-topmost-exp-value* | **set-prec-transmit value** *new prec-value* | **set-qos-transmit value** *new qos-value*| **transmit**}

no violate-action {**drop** | **set-cos-transmit** *new cos-value* | **set-discard-class-transmit** *new discard-value* | **set-dscp-transmit** *new dscp-value* | **set-mpls-exp-imposition-transmit** *new-imposition-exp-value* | **set-mpls-exp-topmost transmit** *new-topmost-exp-value* | **set-prec-transmit value** *new prec-value* | **set-qos-transmit value** *new qos-value*| **transmit**}

Syntax Description

drop	Drops the packet.
set-cos-transmit *new-cos-value*	Sets a new class of service (CoS) value for the packet and send the packet. The range for the new CoS value is 0 to 7.
set-discard-class-transmit *new discard-value*	Sets a new discard-class value for the packet and send the packet. The range for the value is 0 to 7.
set-dscp-transmit *new-dscp-value*	Sets a new Differentiated Services Code Point (DSCP) value for the packet and send the packet. The range for the new DCSP value is 0 to 63.
set-mpls-exp-imposition transmit *new-imposition-exp-value*	Sets an MPLS label using the new MPLS EXP value at tag imposition, and send the packet. The range is 0 to 7.
set-mpls-exp-topmost transmit *new-topmost-exp-value*	Sets an MPLS label using the new MPLS EXP value for the topmost (outer) MPLS label, and send the packet. The range is 0 to 7.
set-prec-transmit *new-precedence-value*	Sets a new IP precedence value for the packet and send the packet. The range for the new IP precedence value is 0 to 7.
set-qos-transmit *qos-group-value*	Sets a new quality of service (QoS) group value for the packet and send the packet. The range for the new QoS value is 0 to 99.
transmit	(Optional) Sends the packet unmodified.

Defaults

The default action is to drop the packet.

Command Modes

Policy-map class police configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You configure violate actions for packets that exceed the peak information rate (PIR).

The switch also supports marking multiple QoS parameters for the same class and simultaneously configuring conform-action, exceed action, and violate-action marking.

Access policy-map class police configuration mode by entering the **police** policy-map class command. See the **police** command for more information.

You can use this command to set one or more violate actions for a traffic class.

For both individual and aggregate policers, if you do not configure a violate action, by default the violate class is assigned the same action as the exceed action.

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Examples

This example shows how configure multiple actions in a policy map that sets a committed information rate of 5000000 bits per second (b/s) and a peak rate of 8000000 b/s:

```
Switch(config)# policy-map map1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police cir 5000000 pir 8000000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-dscp-transmit 24
Switch(config-pmap-c-police)# violate-action drop
Switch(config-pmap-c-police)# end
```

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
conform-action	Defines the action to take on traffic that conforms to the CIR.
exceed-action	Defines the action to take on traffic between the conform rate and the conform rate plus the exceed burst.
police	Defines a policer for classified traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays quality of service (QoS) policy maps.

vlan

To create a VLAN and to enter VLAN configuration mode, use the **vlan** command with a VLAN ID in global configuration mode. To delete the VLAN, use the **no** form of this command. Configuration information for normal-range VLANs (VLAN IDs 1 to 1005) is always saved in the VLAN database as well as in the switch running configuration file. Configuration information for extended-range VLANs (VLAN IDs greater than 1005), are saved only in the switch running configuration file. You can save configurations in the switch startup configuration file by entering the **copy running-config startup-config** privileged EXEC command.

vlan *vlan-id*

no vlan *vlan-id*

Syntax Description

vlan-id	ID of the VLAN to be added and configured. For *vlan-id*, the range is 1 to 4094. You can enter a single VLAN ID, a series of VLAN IDs separated by commas, or a range of VLAN IDs separated by hyphens.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Extended-range VLANs (VLAN IDs 1006 to 4094) are not added to the VLAN database, but all VLAN configurations are saved in the running configuration, and you can save them in the switch startup configuration file.

Entering the **vlan** command with a VLAN ID enables VLAN configuration mode. If you enter an invalid VLAN ID, you receive an error message and do not enter VLAN configuration mode.

When you enter the VLAN ID of an existing VLAN, you do not create a new VLAN, but you can modify VLAN parameters for that VLAN. The specified VLANs are added or modified when you exit VLAN configuration mode. Only the **shutdown** command (for VLANs 1 to 1005) takes effect immediately.

These configuration commands are available in VLAN configuration mode. The **no** form of each command returns the characteristic to its default state.

Note Although all commands are visible, the only VLAN configuration command that is supported on extended-range VLANs is **mtu** *mtu-size*. For extended-range VLANs, all other characteristics must remain at the default state.

Note The switch supports only Ethernet VLANs. You can configure parameters for FDDI and Token Ring VLANs and view the results in the vlan.dat file, but these parameters are not used.

- **are** *are-number*: defines the maximum number of all-routes explorer (ARE) hops for TrCRF VLANs. The range is 0 to 13. The default is 7.
- **backupcrf {enable | disable}**: specifies the backup CRF mode for TrCRF VLANs.
- **bridge** {*bridge-number*| **type**}: specifies the logical distributed source-routing bridge, the bridge that interconnects all logical rings having this VLAN as a parent VLAN in FDDI-NET, Token Ring-NET, and TrBRF VLANs. The range is 0 to 15. The default bridge number is 0.
- **exit**: applies changes, increments the VLAN database revision number (VLANs 1 to 1005 only), and exits VLAN configuration mode.
- **media**: defines the VLAN media type.
  - **ethernet** is Ethernet media type (the default).
  - **fddi** is FDDI media type.
  - **fd-net** is FDDI network entity title (NET) media type.
  - **tokenring** is Token Ring media type or TrCRF.
  - **tr-net** is Token Ring network entity title (NET) media type or TrBRF media type.
- **mtu** *mtu-size*: specifies the maximum transmission unit (MTU) (packet size in bytes). The range is 1500 to 18190. The default is 1500 bytes.
- **name** *vlan-name*: names the VLAN with an ASCII string from 1 to 32 characters that must be unique within the administrative domain. The default is *VLANxxxx* where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number.
- **no**: negates a command or returns it to the default setting.
- **parent** *parent-vlan-id*: specifies the parent VLAN of an existing FDDI, Token Ring, or TrCRF VLAN. The range is 0 to 1005. The default parent VLAN ID is 0 (no parent VLAN).
- **ring** *ring-number*: defines the logical ring for an FDDI, Token Ring, or TrCRF VLAN. The range is 1 to 4095.
- **said** *said-value*: specifies the security association identifier (SAID) as documented in IEEE 802.10. The range is 1 to 4294967294, and the number must be unique within the administrative domain. The default value is 100000 plus the VLAN ID number.
- **shutdown**: shuts down VLAN switching on the VLAN. This command takes effect immediately. Other commands take effect when you exit VLAN configuration mode.
- **state**: specifies the VLAN state:
  - **active** means the VLAN is operational (the default).
  - **suspend** means the VLAN is suspended. Suspended VLANs do not pass packets.
- **ste** *ste-number*: defines the maximum number of spanning-tree explorer (STE) hops for TrCRF VLANs. The range is 0 to 13. The default is 7.
- **stp type**: defines the spanning-tree type for FDDI-NET, Token Ring-NET, or TrBRF VLANs.
  - **ieee** for IEEE Ethernet STP running source-route transparent (SRT) bridging.
  - **ibm** for IBM STP running source-route bridging (SRB).

  - **auto** for STP running a combination of source-route transparent bridging (IEEE) and source-route bridging (IBM).

- **tb-vlan1** *tb-vlan1-id* and **tb-vlan2** *tb-vlan2-id*: specifies the first and second VLAN to which this VLAN is translationally bridged. Translational VLANs translate FDDI or Token Ring to Ethernet, for example. The range is 0 to 1005. If no value is specified, 0 (no transitional bridging) is assumed.

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

Examples

This example shows how to add an Ethernet VLAN with default media characteristics. The default includes a *vlan-name* of *VLANxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number. The default **media** option is **ethernet**; the **state** option is **active**. The default *said-value* variable is 100000 plus the VLAN ID; the *mtu-size* variable is 1500; the **stp-type** option is **ieee**. When you enter the **exit** VLAN configuration command, the VLAN is added if it did not already exist; otherwise, this command does has no affect.

This example shows how to create a new VLAN with all default characteristics and enter config-vlan mode:

```
Switch(config)# vlan 200
Switch(config-vlan)# exit
```

Related Commands

Command	Description
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified).

vlan access-map

To create or modify a VLAN map entry for VLAN packet filtering and to enter VLAN access-map configuration mode, use the **vlan access-map** command in global configuration mode. To delete a VLAN map entry, use the **no** form of this command. Use the **vlan filter** interface configuration command to apply a VLAN map to one or more VLANs.

vlan access-map *name* [*number*]

no vlan access-map *name* [*number*]

Syntax Description

name	Name of the VLAN map.
number	(Optional) The sequence number of the map entry that you want to create or modify (0 to 65535). If you are creating a VLAN map and the sequence number is not specified, it is automatically assigned in increments of 10, starting from 10. This number is the sequence to insert to, or delete from, a VLAN access-map entry.

Defaults

There are no VLAN map entries and no VLAN maps applied to a VLAN.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

In global configuration mode, use this command to create or modify a VLAN map. This entry changes the mode to VLAN access-map configuration, where you can use the **match** access-map configuration command to specify the access lists for IP or non-IP traffic to match and use the **action** command to set whether a match causes the packet to be forwarded or dropped.

In VLAN access-map configuration mode, these commands are available:

- **action**: sets the action to be taken (forward or drop).
- **default**: sets a command to its defaults
- **exit**: exits from VLAN access-map configuration mode
- **match**: sets the values to match (IP address or MAC address).
- **no**: negates a command or set its defaults

When you do not specify an entry number (sequence number), it is added to the end of the map.

There can be only one VLAN map per VLAN and it is applied as packets are received by a VLAN.

You can use the **no vlan access-map** *name* [*number*] command with a sequence number to delete a single entry.

In global configuration mode, use the **vlan filter** interface configuration command to apply the map to one or more VLANs.

Note For more information about VLAN map entries, see the software configuration guide for this release.

Examples

This example shows how to create a VLAN map named *vac1* and apply matching conditions and actions to it. If no other entries already exist in the map, this will be entry 10.

```
Switch(config)# vlan access-map vac1
Switch(config-access-map)# match ip address acl1
Switch(config-access-map)# action forward
```

This example shows how to delete VLAN map *vac1*:

```
Switch(config)# no vlan access-map vac1
```

Related Commands

Command	Description
action	Sets the action for the VLAN access map entry.
match (access-map configuration)	Sets the VLAN map to match packets against one or more access lists.
show vlan access-map	Displays information about a particular VLAN access map or all VLAN access maps.
vlan filter	Applies the VLAN access map to one or more VLANs.

vlan dot1q tag native

To enable tagging of native VLAN frames on all IEEE 802.1Q trunk ports, use the **vlan dot1q tag native** command in global configuration mode. To return to the default setting, use the **no** form of this command.

vlan dot1q tag native

no vlan dot1q tag native

Syntax Description

This command has no arguments or keywords.

Defaults

IEEE 802.1Q native VLAN tagging is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When enabled, native VLAN packets going out all 802.1Q trunk ports are tagged.

When disabled, native VLAN packets going out all 802.1Q trunk ports are not tagged.

Layer 2 control packets that are normally untagged, such as MSTP and CDP, are still sent out untagged.

Examples

This example shows how to enable 802.1Q tagging on native VLAN frames:

```
Switch# configure terminal
Switch (config)# vlan dot1q tag native
Switch (config)# end
```

You can verify your settings by entering the **show vlan dot1q tag native** privileged EXEC command.

Related Commands

Command	Description
show vlan dot1q tag native	Displays 802.1Q native VLAN tagging status.

vlan filter

To apply a VLAN map to one or more VLANs, use the **vlan filter** command in global configuration mode. To remove the map, use the **no** form of this command.

vlan filter *mapname* **vlan-list** {*list* | **all**}

no vlan filter *mapname* **vlan-list** {*list* | **all**}

Syntax Description

mapname	Name of the VLAN map entry.
list	The list of one or more VLANs in the form tt, uu-vv, xx, yy-zz, where spaces around commas and dashes are optional. The range is 1 to 4094.
all	Removes the filter from all VLANs.

Defaults

There are no VLAN filters.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

To avoid accidentally dropping too many packets and disabling connectivity in the middle of the configuration process, we recommend that you completely define the VLAN access map before applying it to a VLAN.

You can verify your settings by entering the **show vlan filter** privileged EXEC command.

For more information about VLAN map entries, see the software configuration guide for this release.

Examples

This example applies VLAN map entry *map1* to VLANs 20 and 30:

```
Switch(config)# vlan filter map1 vlan-list 20, 30
```

This example shows how to delete VLAN map entry *mac1* from VLAN 20:

```
Switch(config)# no vlan filter map1 vlan-list 20
```

Related Commands

Command	Description
show vlan access-map	Displays information about a particular VLAN access map or all VLAN access maps.
show vlan filter	Displays information about all VLAN filters or about a particular VLAN or VLAN access map.
vlan access-map	Creates a VLAN map entry for VLAN packet filtering.

vpn id

To configure the virtual private network (VPN) number for a virtual forwarding infrastructure (VFI) interface, use the **vpn id** command in VFI configuration mode. To remove the VPN ID from the VFI, use the **no** form of this command.

vpn id *vpn-number*

no vpn id *vpn-number*

Syntax Description

vpn-number	The VPN ID for the VFI interface to use. The range is from 1 to 4294967295.

Defaults

The VPN ID is not configured.

Command Modes

VFI configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You create a VFI and enter VFI configuration mode by entering the **l2 vfi** global configuration command.

You must enter a VPN ID to configure the VFI. Some VFI configuration mode keywords are not visible until you enter a VPN ID. When you enter a **vpn id** *vpn-number,* these additional VFI configuration commands are available:

- **neighbor** *remote-peer-IP-address* **encapsulation mpls**: configures the IP address of the remote peer to become a member of the VPLS configured by the VFI and sets the MPLS encapsulation type.
- **shutdown**: shuts down the VFI interface.

The switch supports a total of 26 VFIs.

You can verify the configuration by entering the **show vfi** user EXEC command.

Examples

This example shows how to configure a VPLS (VFI *abc*) on a provider edge (PE) switch and assign it to VPN *123*:

```
Switch(config)# l2 vfi abc manual
Switch(config-vfi)# vpn id 123
Switch(config-vfi)# neighbor 20.0.0.1 encapsulation mpls
Switch(config-vfi)# exit
```

Related Commands

Command	Description
l2 vfi	Creates a VFI and enters VFI configuration mode.
show vfi	Displays information about a VFI.

xconnect

to route a Layer 2 packets over a specified point-to-point VC by using Ethernet over multiprotocol label switching (EoMPLS), use the **xconnect** command in interface configuration mode at customer-edge or service provider-edge ingress and egress Ethernet ports or on VLAN interfaces with a destination and virtual-connection (VC) ID. You can also bind the VC to a pseudowire. To route Layer 2 packets over a hierarchical virtual private LAN switching (H-VPLS) VFI between the edge devices, use the command with a virtual forwarding infrastructure (VFI) name. To delete the VC or VFI connection, use the **no** form of this command on both edge devices.

xconnect *destination vc-id* {**encapsuluation mpls** [**pw-class** *pw-class-name*]}

no xconnect

Syntax Description

destination	The destination label distribution protocol (LDP) IP address of the remote provider edge device. The IP address cannot be an IP address on the route on which the command is entered.
vc-id	Assigns a virtual connection identifier (VC ID) for the virtual connection between the two peer provider edge devices. The range is 1 to 4294967295.
encapsuluation mpls	Specifies the MPLS data encapsulation method.
pw-class *pw-class-name*	(Optional) Specifies the pseudowire class for advanced configuration.

Defaults

There are no point-to-point connections configured.

When configured, the attachment circuit is not bound to the pseudowire.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

An MPLS VC runs across an MPLS cloud to connect Ethernet interfaces on two provider edge devices at each edge of the service provider network. You must enter the command at the PE device at each edge of the service provider network to establish a bidirectional virtual connection, which consists of two unidirectional label-switched paths (LSPs). A VC is not established if not properly defined from both ends.

For the *destination* parameter, specify the LDP IP address of the other PE device; do not specify the IP address of the device on which you are entering the command.

The *vc-id* must be unique for each pair of provider edge devices. Therefore, in large networks, you should keep track of the VC ID assignments to ensure that a VC ID is not assigned more than once.

For H-VPLS, you create the VFI and enter VFI configuration mode by entering the **l2 vfi** *vfi-name* global configuration command.

You can attach a VFI to a VLAN or to multiple Ethernet ports. The switch does not allow switching VLAN and port interfaces through the same VFI.

The **pw-class** keyword with the *pw-class-name* value binds the xconnect configuration of an attachment circuit to a specific pseudowire class. In this way, the pseudowire class configuration serves as a template that contains settings used by all attachment circuits bound to it with the xconnect command.

To configure the pseudowire class, use the **pseudowire-class** global configuration command to enter pseudo-wire class configuration mode. See the IOS documentation for this command.

http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_m4.html#wp1015442

The switch supports only the **encapsulation mpls** and **preferred-path** options in pseudo-wire configuration mode.

You can verify the configuration by entering the **show mplsl2 transport vc** privileged EXEC command.

Examples

This example shows how to establish an Ethernet over MPLS (EoMPLS) tunnel between the PE1 VLAN 3 interface and the PE2 VLAN 4 interface. PE1 has IP address 10.0.0.1/32 that PE2 discovers through routing and PE2 has IP address 20.0.0.1/32 that PE1 discovers through routing.

At the PE1 interface:

```
Switch(config)# interface vlan 3
Switch(config-if)# xconnect 20.0.0.1 123 encapsulation mpls
```

At the PE2 interface:

```
Switch(config)# interface vlan 4
Switch(config-if)# xconnect 10.0.0.1 123 encapsulation mpls
```

This example shows how to configure a pseudowire class named *vc-class* and then configure xconnect service for an interface by binding the interface to the pseudowire named *123* with a remote peer *10.0.3.201*. The configuration uses the settings in the pseudowire class.

```
Switch (config)# pseudowire-class vc-class
Switch (config-pw-class)# encapsulation mpls
Switch (config-pw-class)# preferred-path interface tunnel 100
Switch (config-pw-class)# exit
Switch(config)# interface Gigabit Ethernet 1/0/1
Switch(config-if)# xconnect 10.0.3.201 123 pw-class vc-class
```

This example shows how to create VFI *abc* and attach it to a VLAN interface. You need to configure the PE devices at both edges of the MPLS network this way:

```
Switch(config)# l2 vfi abc manual
Switch(config-vfi)# vpn id 123
Switch(config-vfi)# neighbor 10.0.0.1 encapsulation mpls
Switch(config-vfi)# exit
Switch(config)# interface vlan 4
Switch(config-if)# xconnect vfi abc encapsulation mpls
```

Related Commands

Command	Description
l2 vfi	Configures a VFI for implementing VPLS over an MPLS backbone.
show mpls l2transport vc	Displays information about the EoMPLS VCs that have been enabled to route Layer 2 packets on a device.