

# shutdown

Use the **shutdown** interface configuration command to disable an interface. Use the **no** form of this command to restart a disabled interface.

**shutdown**

**no shutdown**

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

<b>Defaults</b>	The port is enabled (not shut down).
-----------------	--------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(53)EY	This command was introduced.

<b>Usage Guidelines</b>	<p>The <b>shutdown</b> command causes a port to stop forwarding. You can enable the port with the <b>no shutdown</b> command.</p> <p>The <b>no shutdown</b> 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.</p> <p>The <b>shutdown</b> command disables all functions on the specified interface.</p> <p>This command also marks the interface as unavailable. To see if an interface is disabled, use the <b>show interfaces</b> privileged EXEC command. An interface that has been shut down is shown as administratively down in the display.</p>
-------------------------	---

<b>Examples</b>	These examples show how to disable and re-enable a port:
-----------------	--

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

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

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show interfaces</a>	Displays the statistical information specific to all interfaces or to a specific interface.

# shutdown vlan

Use the **shutdown vlan** global configuration command to shut down (suspend) local traffic on the specified VLAN. Use the **no** form of this command to restart local traffic on the VLAN.

```
shutdown vlan vlan-id

no shutdown vlan vlan-id
```

Syntax Description	<i>vlan-id</i>	ID of the VLAN to be locally shut down. The range is 2 to 1001. VLANs defined as default VLANs under the VLAN Trunking Protocol (VTP), as well as extended-range VLANs (greater than 1005) cannot be shut down. The default VLANs are 1 and 1002 to 1005.
--------------------	----------------	---

Defaults	No default is defined.
----------	------------------------

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

Command History	Release	Modification
	12.2(53)EY	This command was introduced.

Usage Guidelines	The <b>shutdown vlan</b> command does not change the VLAN information in the VTP database. The command shuts down local traffic, but the switch still advertises VTP information.
------------------	---

Examples	<p>This example shows how to shut down traffic on VLAN 2:</p> <pre>Switch(config)# shutdown vlan 2</pre> <p>You can verify your setting by entering the <b>show vlan</b> privileged EXEC command.</p>
----------	---

Related Commands	Command	Description
	<b>shutdown</b> (config-vlan mode)	Shuts down local traffic on the VLAN when in config-VLAN mode (accessed by the <b>vlan <i>vlan-id</i></b> global configuration command).

# small-frame violation rate

Use the **small-frame violation rate** *pps* interface configuration command to configure the rate (threshold) for an interface to be error disabled when it receives VLAN-tagged packets that are small frames (67 bytes or less) at the specified rate. Use the **no** form of this command to return to the default setting.

```
small-frame violation rate pps

no small-frame violation rate pps
```

Syntax Description	<i>pps</i>	Specify the threshold at which an interface receiving small frames will be error disabled. The range is 1 to 10,000 packets per second (pps).
--------------------	------------	---

Defaults	This feature is disabled.
----------	---------------------------

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

Command History	Release	Modification
	12.2(53)EY	This command was introduced.

**Usage Guidelines**

This command enables the rate (threshold) for a port to be error disabled when it receives small frames. Small frames are considered packets that are 67 frames or less.

Use the **errdisable detect cause small-frame** global configuration command to globally enable the small-frames threshold for each port.

You can configure the port to be automatically re-enabled by using the **errdisable recovery cause small-frame** global configuration command. You configure the recovery time by using the **errdisable recovery interval** *interval global configuration command*.

**Examples**

This example shows how to enable the small-frame arrival rate feature so that the port is error disabled if incoming small frames arrived at 10,000 pps.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# small-frame violation rate 10000
```

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

Related Commands	Command	Description
	<b>errdisable detect cause small-frame</b>	Allows any switch port to be put into the error-disabled state if an incoming frame is smaller than the minimum size and arrives at the specified rate (threshold).
	<b>errdisable recovery cause small-frame</b>	<b>Enables the recovery timer.</b>
	<b>show interfaces</b>	Displays the interface settings on the switch, including input and output flow control.

## snmp-server enable traps

Use the **snmp-server enable traps** global configuration command 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 **no** form of this command to return to the default setting.

**snmp-server enable traps** [**bridge** [**newroot**] [**topologychange**] | **cluster** | **config** | **config-copy** | **config-ctid** | **copy-config** | **entity** | **envmon** [**fan** | **shutdown** | **status** | **supply** | **temperature**] | **flash** [**insertion** | **removal**] | **fru-ctrl** | **rep** | **snmp** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] | **storm-control trap-rate** *value* | **stpx** [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**] | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vtp**]

**no snmp-server enable traps** [**bridge** [**newroot**] [**topologychange**] | **cluster** | **config** | **config-copy** | **config-ctid** | **copy-config** | **entity** | **envmon** [**fan** | **shutdown** | **status** | **supply** | **temperature**] | **flash** [**insertion** | **removal**] | **fru-ctrl** | **rep** | **snmp** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] | **storm-control trap-rate** *value* | **stpx** [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**] | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vtp**]

Syntax Description	
<b>bridge</b> [ <b>newroot</b> ] [ <b>topologychange</b> ]	(Optional) Generate STP bridge MIB traps. The keywords have these meanings: <ul style="list-style-type: none"> <li><b>newroot</b>—(Optional) Enable SNMP STP Bridge MIB new root traps.</li> <li><b>topologychange</b>—(Optional) Enable SNMP STP Bridge MIB topology change traps.</li> </ul>
<b>cluster</b>	(Optional) Enable cluster traps.
<b>config</b>	(Optional) Enable SNMP configuration traps.
<b>config-copy</b>	(Optional) Enable SNMP configuration-copy traps.
<b>config-ctid</b>	(Optional) Enable SNMP configuration change tracking identification (config-ctid) traps.
<b>copy-config</b>	(Optional) Enable SNMP copy-configuration traps.
<b>entity</b>	(Optional) Enable SNMP entity traps.
<b>envmon</b> [ <b>fan</b>   <b>shutdown</b>   <b>status</b>   <b>supply</b>   <b>temperature</b> ]	(Optional) Enable SNMP environmental traps. The keywords have these meanings: <ul style="list-style-type: none"> <li><b>fan</b>—(Optional) Enable fan traps.</li> <li><b>shutdown</b>—(Optional) Enable environmental monitor shutdown traps.</li> <li><b>status</b>—(Optional) Enable SNMP environmental status-change traps.</li> <li><b>supply</b>—(Optional) Enable environmental monitor power-supply traps.</li> <li><b>temperature</b>—(Optional) Enable environmental monitor temperature traps.</li> </ul>

<b>flash</b> [ <b>insertion</b>   <b>removal</b> ]	(Optional) Enable SNMP FLASH notifications. The keywords have these meanings:  <b>insertion</b> —(Optional) Generate a trap when a switch (flash) is inserted into a stack, either physically or because of a power cycle or reload.  <b>removal</b> —(Optional) Generate a trap when a switch (flash) is removed from a stack, either physically or because of a power cycle or reload.
<b>fru-ctrl</b>	(Optional) Enable SNMP entity FRU control traps.
<b>rep</b>	(Optional) Enable SNMP Resilient Ethernet Protocol traps.
<b>snmp</b> [ <b>authentication</b>   <b>coldstart</b>   <b>linkdown</b>   <b>linkup</b>   <b>warmstart</b> ]	(Optional) Enable SNMP traps. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>authentication</b>—(Optional) Enable authentication trap.</li> <li>• <b>coldstart</b>—(Optional) Enable cold start trap.</li> <li>• <b>linkdown</b>—(Optional) Enable linkdown trap.</li> <li>• <b>linkup</b>—(Optional) Enable linkup trap.</li> <li>• <b>warmstart</b>—(Optional) Enable warmstart trap.</li> </ul>
<b>storm-control</b> <b>trap-rate</b> <i>value</i>	(Optional) Enable storm-control traps. Use the <b>trap-rate</b> keyword to set the maximum number of storm-control traps sent per minute. The range is 0 to 1000; the default is 0 (no limit is imposed; a trap is sent at every occurrence).
<b>stpx</b>	(Optional) Enable SNMP STPX MIB traps. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>inconsistency</b>—(Optional) Enable SNMP STPX MIB Inconsistency Update traps.</li> <li>• <b>root-inconsistency</b>—(Optional) Enable SNMP STPX MIB Root Inconsistency Update traps.</li> <li>• <b>loop-inconsistency</b>—(Optional) Enable SNMP STPX MIB Loop Inconsistency Update traps.</li> </ul>
<b>syslog</b>	(Optional) Enable SNMP syslog traps.
<b>transceiver</b>	(Optional) Enable SNMP transceiver traps.
<b>tty</b>	(Optional) Send TCP connection traps. This is enabled by default.
<b>vlan-membership</b>	(Optional) Enable SNMP VLAN membership traps.
<b>vlancreate</b>	(Optional) Enable SNMP VLAN-created traps.
<b>vlandelete</b>	(Optional) Enable SNMP VLAN-deleted traps.
<b>vtp</b>	(Optional) Enable VLAN Trunking Protocol (VTP) traps.

**Note**

Though visible in the command-line help strings, the **cpu [threshold]** keyword is 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(53)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.

**Examples** This example shows how to send VTP traps to the NMS:

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

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

Related Commands	Command	Description
	<b>show running-config</b>	Displays the operating configuration.
	<a href="#">snmp-server host</a>	Specifies the host that receives SNMP traps.

# snmp-server host

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

```
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	<div> <div>host-addr</div> <div>Name or Internet address of the host (the targeted recipient).</div> </div>
udp-port port	<div> <div></div> <div>(Optional) Configure the User Datagram Protocol (UDP) port number of the host to receive the traps. The range is 0 to 65535.</div> </div>
informs   traps	<div> <div></div> <div>(Optional) Send SNMP traps or informs to this host.</div> </div>
version 1   2c   3	<div> <div></div> <div>(Optional) Version of the SNMP used to send the traps.</div> <div>These keywords are supported:</div> <div>1—SNMPv1. This option is not available with informs.</div> <div>2c—SNMPv2C.</div> <div>3—SNMPv3. These optional keywords can follow the Version 3 keyword:</div> <div> <ul style="list-style-type: none"> <li>auth (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication.</li> <li>noauth (Default). The noAuthNoPriv security level. This is the default if the [auth   noauth   priv] keyword choice is not specified.</li> <li>priv (Optional). Enables Data Encryption Standard (DES) packet encryption (also called <i>privacy</i>).</li> </ul> </div> <div>Note The priv keyword is available only when the cryptographic (encrypted) software image is installed.</div> </div>
vrf vrf-instance	<div> <div></div> <div>(Optional) Virtual private network (VPN) routing instance and name for this host.</div> </div>
community-string	<div> <div></div> <div>Password-like community string sent with the notification operation. Though you can set this string by using the <b>snmp-server host</b> command, we recommend that you define this string by using the <b>snmp-server community</b> global configuration command before using the <b>snmp-server host</b> command.</div> <div>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.</div> </div>



<i>notification-type</i>	<p>(Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the these keywords:</p> <ul style="list-style-type: none"> <li>• <b>bridge</b>—Send SNMP Spanning Tree Protocol (STP) bridge MIB traps.</li> <li>• <b>cluster</b>—Send cluster member status traps.</li> <li>• <b>config</b>—Send SNMP configuration traps.</li> <li>• <b>copy-config</b>—Send SNMP copy configuration traps.</li> <li>• <b>entity</b>— Send SNMP entity traps.</li> <li>• <b>envmon</b>—Send environmental monitor traps.</li> <li>• <b>flash</b>—Send SNMP FLASH notifications.</li> <li>• <b>fru-ctrl</b>—Send entity FRU control traps.</li> <li>• <b>snmp</b>—Send SNMP-type traps.</li> <li>• <b>storm-control</b>—Send SNMP storm-control traps.</li> <li>• <b>stpx</b>—Send SNMP STP extended MIB traps.</li> <li>• <b>syslog</b>—Send SNMP syslog traps.</li> <li>• <b>tty</b>—Send TCP connection traps.</li> <li>• <b>udp-port</b> <i>port</i>—Configure the User Datagram Protocol (UDP) port number of the host to receive the traps. The range is from 0 to 65535.</li> <li>• <b>vlan-membership</b>— Send SNMP VLAN membership traps.</li> <li>• <b>vlancreate</b>—Send SNMP VLAN-created traps.</li> <li>• <b>vlandelete</b>—Send SNMP VLAN-deleted traps.</li> <li>• <b>vtp</b>—Send SNMP VLAN Trunking Protocol (VTP) traps.</li> </ul>
--------------------------	---

### 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(53)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.

## 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
```

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

**Related Commands**

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

# snmp trap mac-notification

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

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

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

## Syntax Description

<b>added</b>	Enable the MAC notification trap whenever a MAC address is added on this interface.
<b>removed</b>	Enable 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(53)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.

## 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 added
```

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

**Related Commands**

Command	Description
<a href="#">snmp-server enable traps</a>	Sends the SNMP MAC notification traps when the <b>mac-notification</b> keyword is appended.

# spanning-tree backbonefast

Use the **spanning-tree backbonefast** global configuration command to enable the BackboneFast feature. Use the **no** form of the command to return to the default setting.

**spanning-tree backbonefast**

**no spanning-tree backbonefast**

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

**Defaults** BackboneFast is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(53)EY	This command was introduced.

**Usage Guidelines** You can configure the BackboneFast feature for rapid PVST+ or for multiple spanning-tree (MST) mode, but the feature remains disabled (inactive) until you change the spanning-tree mode to PVST+.

BackboneFast starts when a root port or blocked port on a switch receives inferior BPDUs from its designated switch. An inferior BPDU identifies a switch that declares itself as both the root bridge and the designated switch. When a switch receives an inferior BPDU, it means that a link to which the switch is not directly connected (an *indirect* link) has failed (that is, the designated switch has lost its connection to the root switch. If there are alternate paths to the root switch, BackboneFast causes the maximum aging time on the interfaces on which it received the inferior BPDU to expire and allows a blocked port to move immediately to the listening state. BackboneFast then transitions the interface to the forwarding state. For more information, see the software configuration guide for this release.

Enable BackboneFast on all supported switches to allow the detection of indirect link failures and to start the spanning-tree reconfiguration sooner.

**Examples** This example shows how to enable BackboneFast on the switch:

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

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

Related Commands	Command	Description
	<a href="#">show spanning-tree summary</a>	Displays a summary of the spanning-tree interface states.

# spanning-tree bpdupfilter

Use the **spanning-tree bpdupfilter** interface configuration command to prevent an interface from sending or receiving bridge protocol data units (BPDUs). Use the **no** form of this command to return to the default setting.

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

**no spanning-tree bpdupfilter**

## Syntax Description

<b>disable</b>	Disable BPDU filtering on the specified interface.
<b>enable</b>	Enable BPDU filtering on the specified interface.

## Defaults

BPDU filtering is disabled.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(53)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 interface 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 interfaces by using the **spanning-tree portfast bpdupfilter default** global configuration command.

You can use the **spanning-tree bpdupfilter** interface configuration command to override the setting of the **spanning-tree portfast bpdupfilter default** global configuration 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 bpdupfilter enable
```

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

Related Commands	Command	Description
	<b>show running-config</b>	Displays the operating configuration.
	<b>spanning-tree portfast (global configuration)</b>	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interface or enables the Port Fast feature on all nontrunking interfaces.
	<b>spanning-tree portfast (interface configuration)</b>	Enables the Port Fast feature on an interface and all its associated VLANs.



# spanning-tree bpduguard

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

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

**no spanning-tree bpduguard**

## Syntax Description

<b>disable</b>	Disable BPDU guard on the specified interface.
<b>enable</b>	Enable BPDU guard on the specified interface.

## Defaults

BPDU guard is disabled.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(53)EY	This command was introduced.

## Usage Guidelines

The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface 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+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

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

You can use the **spanning-tree bpduguard** interface configuration command to override the setting of the **spanning-tree portfast bpduguard default** global configuration 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
```

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

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 interfaces or enables the Port Fast feature on all nontrunking interfaces.
	spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface and all its associated VLANs.

## spanning-tree cost

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

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

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

### Syntax Description

<b>vlan</b> <i>vlan-id</i>	(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.
<i>cost</i>	Path cost. The range is 1 to 200000000, with higher values meaning higher costs.

### Defaults

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

- 1000 Mb/s—4
- 100 Mb/s—19
- 10 Mb/s—100

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(53)EY	This command was introduced.

### Usage Guidelines

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

If you configure an interface 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.

### 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
```

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

Related Commands	Command	Description
	<code>show spanning-tree interface <i>interface-id</i></code>	Displays spanning-tree information for the specified interface.
	<code>spanning-tree port-priority</code>	Configures an interface priority.
	<code>spanning-tree vlan <i>vlan-id</i> priority</code>	Sets the switch priority for the specified spanning-tree instance.

# spanning-tree etherchannel guard misconfig

Use the **spanning-tree etherchannel guard misconfig** global configuration command to display an error message when the switch detects an EtherChannel misconfiguration. Use the **no** form of this command to disable the feature.

**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(53)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.

## Examples

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

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

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

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

# spanning-tree extend system-id

Use the **spanning-tree extend system-id** global configuration command to enable the extended system ID feature.

## 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(53)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
	<code>show spanning-tree summary</code>	Displays a summary of spanning-tree interface states.
	<code>spanning-tree mst root</code>	Configures the MST root switch priority and timers based on the network diameter.
	<code>spanning-tree vlan priority</code>	Sets the switch priority for the specified spanning-tree instance.



# spanning-tree guard

Use the **spanning-tree guard** interface configuration command to enable root guard or loop guard on all the VLANs associated with the selected interface. 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. Use the **no** form of this command to return to the default setting.

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

**no spanning-tree guard**

## Syntax Description

<b>loop</b>	Enable loop guard.
<b>none</b>	Disable root guard or loop guard.
<b>root</b>	Enable 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(53)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+), 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 interface. If this interface is in the root-inconsistent (blocked) state, it automatically transitions to the listening state.

Do not enable root guard on interfaces that will be used by the UplinkFast feature. With UplinkFast, the backup interfaces (in the blocked state) replace the root port in the case of a failure. However, if root guard is also enabled, all the backup interfaces used by the UplinkFast feature are placed in the root-inconsistent state (blocked) and prevented from reaching the forwarding state. The UplinkFast feature is not available when the switch is operating in the rapid-PVST+ or 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.

To disable root guard or loop guard, use the **spanning-tree guard none** interface configuration command. 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.

### 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
```

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

### Related Commands

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

# spanning-tree link-type

Use the **spanning-tree link-type** interface configuration command to override the default link-type setting, which is determined by the duplex mode of the interface, and to enable rapid spanning-tree transitions to the forwarding state. Use the **no** form of this command to return to the default setting.

**spanning-tree link-type {point-to-point | shared}**

**no spanning-tree link-type**

## Syntax Description

<b>point-to-point</b>	Specify that the link type of an interface is point-to-point.
<b>shared</b>	Specify that the link type of an interface 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(53)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.

## 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
```

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.

Related Commands	Command	Description
	<b>clear spanning-tree detected-protocols</b>	Restarts the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface.
	<b>show spanning-tree interface</b> <i>interface-id</i>	Displays spanning-tree state information for the specified interface.
	<b>show spanning-tree mst interface</b> <i>interface-id</i>	Displays MST information for the specified interface.

# spanning-tree loopguard default

Use the **spanning-tree loopguard default** global configuration command to prevent alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. Use the **no** form of this command to return to the default setting.

**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

Release	Modification
12.2(53)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 interfaces 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.

**Examples** This example shows how to globally enable loop guard:

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

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

Related Commands	Command	Description
	<b>show running-config</b>	Displays the operating configuration.
	<b>spanning-tree guard loop</b>	Enables the loop guard feature on all the VLANs associated with the specified interface.

■ spanning-tree loopguard default

# spanning-tree mode

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

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

**no spanning-tree mode**

<b>Syntax Description</b>	<b>mst</b>	Enable MST and Rapid Spanning Tree Protocol (RSTP) (based on IEEE 802.1s and IEEE 802.1w).
	<b>pvst</b>	Enable PVST+ (based on IEEE 802.1D).
	<b>rapid-pvst</b>	Enable rapid PVST+ (based on IEEE 802.1w).

**Defaults** The default mode is PVST+.

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(53)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.

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

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

This example shows to enable rapid PVST+ on the switch:

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

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

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

■ spanning-tree mode



# spanning-tree mst configuration

Use the **spanning-tree mst configuration** global configuration command to enter multiple spanning-tree (MST) configuration mode through which you configure the MST region. Use the **no** form of this command to return to the default settings.

**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(53)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 1 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**: Though 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 65 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.

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  Vlan  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
```

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

Related Commands

Command	Description
<a href="#">show spanning-tree mst configuration</a>	Displays the MST region configuration.

# spanning-tree mst cost

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

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

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

## Syntax Description

<i>instance-id</i>	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.
<i>cost</i>	Path cost is 1 to 200000000, with higher values meaning higher costs.

## Defaults

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

- 1000 Mb/s—20000
- 100 Mb/s—200000
- 10 Mb/s—2000000

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(53)EY	This command was introduced.

## Usage Guidelines

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

## 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
```

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

Related Commands

Command	Description
<code>show spanning-tree mst interface <i>interface-id</i></code>	Displays MST information for the specified interface.
<code>spanning-tree mst port-priority</code>	Configures an interface priority.
<code>spanning-tree mst priority</code>	Configures the switch priority for the specified spanning-tree instance.

# spanning-tree mst forward-time

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

**spanning-tree mst forward-time** *seconds*

**no spanning-tree mst forward-time**

<b>Syntax Description</b>	<i>seconds</i>	Length of the listening and learning states. The range is 4 to 30 seconds.
---------------------------	----------------	--

<b>Defaults</b>	The default is 15 seconds.
-----------------	----------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(53)EY	This command was introduced.

<b>Usage Guidelines</b>	Changing the <b>spanning-tree mst forward-time</b> command affects all spanning-tree instances.
-------------------------	---

<b>Examples</b>	This example shows how to set the spanning-tree forwarding time to 18 seconds for all MST instances: <pre>Switch(config)# <b>spanning-tree mst forward-time 18</b></pre>
	You can verify your setting by entering the <b>show spanning-tree mst</b> privileged EXEC command.

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

# spanning-tree mst hello-time

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

**spanning-tree mst hello-time** *seconds*

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

<b>Syntax Description</b>	<i>seconds</i>	Interval between hello BPDUs sent by root switch configuration messages. The range is 1 to 10 seconds.
---------------------------	----------------	--

<b>Defaults</b>	The default is 2 seconds.	
-----------------	---------------------------	--

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(46)EY	This command was introduced.

<b>Usage Guidelines</b>	<p>After you set the <b>spanning-tree mst max-age</b> <i>seconds</i> 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 <b>max-age</b> setting must be greater than the <b>hello-time</b> setting.</p> <p>Changing the <b>spanning-tree mst hello-time</b> command affects all spanning-tree instances.</p>	
-------------------------	---	--

<b>Examples</b>	<p>This example shows how to set the spanning-tree hello time to 3 seconds for all multiple spanning-tree (MST) instances:</p> <pre>Switch(config)# spanning-tree mst hello-time 3</pre> <p>You can verify your setting by entering the <b>show spanning-tree mst</b> privileged EXEC command.</p>	
-----------------	--	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show spanning-tree mst</a>	Displays MST information.
	<a href="#">spanning-tree mst forward-time</a>	Sets the forward-delay time for all MST instances.
	<a href="#">spanning-tree mst max-age</a>	Sets the interval between messages that the spanning tree receives from the root switch.
	<a href="#">spanning-tree mst max-hops</a>	Sets the number of hops in a region before the BPDU is discarded.

# spanning-tree mst max-age

Use the **spanning-tree mst max-age** global configuration command to set the interval between messages that the spanning tree receives from the root switch. 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. Use the **no** form of this command to return to the default setting.

**spanning-tree mst max-age** *seconds*

**no spanning-tree mst max-age**

<b>Syntax Description</b>	<i>seconds</i>	Interval between messages the spanning tree receives from the root switch. The range is 6 to 40 seconds.
---------------------------	----------------	--

<b>Defaults</b>	The default is 20 seconds.
-----------------	----------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(53)EY	This command was introduced.

<b>Usage Guidelines</b>	<p>After you set the <b>spanning-tree mst max-age</b> <i>seconds</i> 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 <b>max-age</b> setting must be greater than the <b>hello-time</b> setting.</p> <p>Changing the <b>spanning-tree mst max-age</b> command affects all spanning-tree instances.</p>
-------------------------	--

<b>Examples</b>	<p>This example shows how to set the spanning-tree max-age to 30 seconds for all multiple spanning-tree (MST) instances:</p>
-----------------	--

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

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

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

# spanning-tree mst max-hops

Use the **spanning-tree mst max-hops** global configuration command 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 **no** form of this command to return to the default setting.

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

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

<b>Syntax Description</b>	<i>hop-count</i> Number of hops in a region before the BPDU is discarded. The range is 1 to 255 hops.
---------------------------	---

<b>Defaults</b>	The default is 20 hops.
-----------------	-------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(53)EY	This command was introduced.

<b>Usage Guidelines</b>	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 <b>spanning-tree mst max-hops</b> command affects all spanning-tree instances.

<b>Examples</b>	This example shows how to set the spanning-tree max-hops to 10 for all multiple spanning-tree (MST) instances:
	Switch(config)# <b>spanning-tree mst max-hops 10</b>
	You can verify your setting by entering the <b>show spanning-tree mst</b> privileged EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show spanning-tree mst</a>	Displays MST information.
	<a href="#">spanning-tree mst forward-time</a>	Sets the forward-delay time for all MST instances.
	<a href="#">spanning-tree mst hello-time</a>	Sets the interval between hello BPDU sent by root switch configuration messages.
	<a href="#">spanning-tree mst max-age</a>	Sets the interval between messages that the spanning tree receives from the root switch.



# spanning-tree mst port-priority

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

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

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

## Syntax Description

<i>instance-id</i>	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.
<i>priority</i>	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(53)EY	This command was introduced.

## Usage Guidelines

You can assign higher priority values (lower numerical values) to interfaces that you want selected first and lower priority values (higher numerical values) that you want selected last. If all interfaces 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.

## 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
```

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

## Related Commands

Command	Description
<b>show spanning-tree mst interface</b> <i>interface-id</i>	Displays MST information for the specified interface.

Command	Description
<a href="#">spanning-tree mst cost</a>	Sets the path cost for MST calculations.
<a href="#">spanning-tree mst priority</a>	Sets the switch priority for the specified spanning-tree instance.

# spanning-tree mst pre-standard

Use the **spanning-tree mst pre-standard** interface configuration command to configure a port to send only prestandard bridge protocol data units (BPDUs).

**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(53)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.

## Examples

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

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

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

## Related Commands

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

# spanning-tree mst priority

Use the **spanning-tree mst priority** global configuration command to set the switch priority for the specified spanning-tree instance. Use the **no** form of this command to return to the default setting.

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

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

Syntax Description

<i>instance-id</i>	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.
<b>priority</b>	<p>Set 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.</p> <p>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.</p>

Defaults

The default is 32768.

Command Modes

Global configuration

Command History

Release	Modification
12.2(46)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**

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

Related Commands

Command	Description
<b>show spanning-tree mst</b> <i>instance-id</i>	Displays MST information for the specified interface.
<b>spanning-tree mst cost</b>	Sets the path cost for MST calculations.
<b>spanning-tree mst port-priority</b>	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

<i>instance-id</i>	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.
<b>root primary</b>	Force this switch to be the root switch.
<b>root secondary</b>	Set this switch to be the root switch should the primary root switch fail.
<b>diameter</b> <i>net-diameter</i>	(Optional) Set 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.
<b>hello-time</b> <i>seconds</i>	(Optional) Set 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(53)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).

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
```

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

Related Commands

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

# spanning-tree port-priority

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

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

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

## Syntax Description

<b>vlan</b> <i>vlan-id</i>	(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.
<i>priority</i>	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(53)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 interface to the VLAN.

If you configure an interface 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.

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
```

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

Related Commands

Command	Description
<b>show spanning-tree interface <i>interface-id</i></b>	Displays spanning-tree information for the specified interface.
<b>spanning-tree cost</b>	Sets the path cost for spanning-tree calculations.
<b>spanning-tree vlan priority</b>	Sets the switch priority for the specified spanning-tree instance.



## spanning-tree portfast (global configuration)

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

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

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

Syntax Description		
	<b>bpdupfilter default</b>	Globally enable BPDU filtering on Port Fast-enabled interfaces and prevent the switch interface connected to end stations from sending or receiving BPDUs.
	<b>bpduguard default</b>	Globally enable the BPDU guard feature on Port Fast-enabled interfaces and place the interfaces that receive BPDUs in an error-disabled state.
	<b>default</b>	Globally enable the Port Fast feature on all nontrunking interfaces. When the Port Fast feature is enabled, the interface changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes.

<b>Defaults</b>	The BPDU filtering, the BPDU guard, and the Port Fast features are disabled on all interfaces unless they are individually configured.
-----------------	--

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

Command History	Release	Modification
	12.2(53)EY	This command was introduced.

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

Use the **spanning-tree portfast bpdupfilter default** global configuration command to globally enable BPDU filtering on interfaces that are Port Fast-enabled (the interfaces are in a Port Fast-operational state). The interfaces 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 interfaces do not receive BPDUs. If a BPDU is received on a Port Fast-enabled interface, the interface loses its Port Fast-operational status and BPDU filtering is disabled.

You can override the **spanning-tree portfast bpdupfilter default** global configuration command by using the **spanning-tree bdpupfilter** interface configuration command.

**Caution**

Enabling BPDU filtering on an interface 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 interfaces that are in a Port Fast-operational state. In a valid configuration, Port Fast-enabled interfaces do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled interface signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the interface in the error-disabled state. The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface 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.

Use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking interfaces. Configure Port Fast only on interfaces 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 interface 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. You can use the **no spanning-tree portfast default** global configuration command to disable Port Fast on all interfaces unless they are individually configured with the **spanning-tree portfast** interface configuration command.

**Examples**

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

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

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

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

# spanning-tree portfast (interface configuration)

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

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

**no spanning-tree portfast**

Syntax Description	<b>disable</b>	(Optional) Disable the Port Fast feature on the specified interface.
	<b>trunk</b>	(Optional) Enable the Port Fast feature on a trunking interface.

Defaults	The Port Fast feature is disabled on all interfaces; however, it is automatically enabled on dynamic-access ports.
----------	--

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

Command History	Release	Modification
	12.2(53)EY	This command was introduced.

Usage Guidelines	Use this feature only on interfaces 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 <b>spanning-tree portfast trunk</b> interface configuration command. The <b>spanning-tree portfast</b> 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+), rapid-PVST+, or the multiple spanning-tree (MST) mode.
	This feature affects all VLANs on the interface.
	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 <b>spanning-tree portfast default</b> global configuration command to globally enable the Port Fast feature on all nontrunking interfaces. However, the <b>spanning-tree portfast</b> interface configuration command can override the global setting.
	If you configure the <b>spanning-tree portfast default</b> global configuration command, you can disable Port Fast on an interface that is not a trunk interface by using the <b>spanning-tree portfast disable</b> interface configuration 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
```

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

### Related Commands

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

# spanning-tree transmit hold-count

Use the **spanning-tree transmit hold-count** global configuration command to configure the number of bridge protocol data units (BPDUs) sent every second. Use the **no** form of this command to return to the default setting.

```
spanning-tree transmit hold-count [value]

no spanning-tree transmit hold-count [value]
```

Syntax Description	<i>value</i> (Optional) Number of BPDUs sent every second. The range is 1 to 20.
--------------------	--

Defaults	The default is 6.
----------	-------------------

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

Command History	Release	Modification
	12.2(53)EY	This command was introduced.

Usage Guidelines	Increasing the transmit hold-count value can have a significant impact on CPU utilization when the switch is in rapid-per-VLAN spanning-tree plus (rapid-PVST+) mode. Decreasing this value might slow down convergence. We recommend using the default setting.
------------------	--

Examples	<p>This example shows how to set the transmit hold count to 8:</p> <pre>Switch(config)# spanning-tree transmit hold-count 8</pre> <p>You can verify your setting by entering the <b>show spanning-tree mst</b> privileged EXEC command.</p>
----------	---

Related Commands	Command	Description
	<a href="#">show spanning-tree mst</a>	Displays the multiple spanning-tree (MST) region configuration and status, including the transmit hold count.

# spanning-tree uplinkfast

Use the **spanning-tree uplinkfast** global configuration command to accelerate the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself. Use the **no** form of this command to return to the default setting.

**spanning-tree uplinkfast** [**max-update-rate** *pkts-per-second*]

**no spanning-tree uplinkfast** [**max-update-rate**]

## Syntax Description

<b>max-update-rate</b> <i>pkts-per-second</i>	(Optional) The number of packets per second at which update packets are sent. The range is 0 to 32000.
---	--

## Defaults

UplinkFast is disabled.  
The update rate is 150 packets per second.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(53)EY	This command was introduced.

## Usage Guidelines

Use this command only on access switches.

You can configure the UplinkFast feature for rapid PVST+ or for multiple spanning-tree (MST) mode, but the feature remains disabled (inactive) until you change the spanning-tree mode to PVST+.

When you enable UplinkFast, it is enabled for the entire switch and cannot be enabled for individual VLANs.

When UplinkFast is enabled, the switch priority of all VLANs is set to 49152. If you change the path cost to a value less than 3000 and you enable UplinkFast or UplinkFast is already enabled, the path cost of all interfaces and VLAN trunks is increased by 3000 (if you change the path cost to 3000 or above, the path cost is not altered). The changes to the switch priority and the path cost reduces the chance that a switch will become the root switch.

When UplinkFast is disabled, the switch priorities of all VLANs and path costs of all interfaces are set to default values if you did not modify them from their defaults.

When spanning tree detects that the root port has failed, UplinkFast immediately changes to an alternate root port, changing the new root port directly to forwarding state. During this time, a topology change notification is sent.

Do not enable the root guard on interfaces that will be used by the UplinkFast feature. With UplinkFast, the backup interfaces (in the blocked state) replace the root port in the case of a failure. However, if root guard is also enabled, all the backup interfaces used by the UplinkFast feature are placed in the root-inconsistent state (blocked) and prevented from reaching the forwarding state.

If you set the max-update-rate to 0, station-learning frames are not generated, so the spanning-tree topology converges more slowly after a loss of connectivity.

Examples

This example shows how to enable UplinkFast:

```
Switch(config)# spanning-tree uplinkfast
```

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

Related Commands

Command	Description
<a href="#">show spanning-tree summary</a>	Displays a summary of the spanning-tree interface states.
<a href="#">spanning-tree vlan root primary</a>	Forces this switch to be the root switch.



# spanning-tree vlan

Use the **spanning-tree vlan** global configuration command to configure spanning tree on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

**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		
<i>vlan-id</i>		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.
<b>forward-time</b> <i>seconds</i>		(Optional) Set 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.
<b>hello-time</b> <i>seconds</i>		(Optional) Set the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds.
<b>max-age</b> <i>seconds</i>		(Optional) Set 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.
<b>priority</b> <i>priority</i>		(Optional) Set 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 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.
<b>root primary</b>		(Optional) Force this switch to be the root switch.
<b>root secondary</b>		(Optional) Set this switch to be the root switch should the primary root switch fail.
<b>diameter</b> <i>net-diameter</i>		(Optional) Set 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(53)EY	This command was introduced.

**Usage Guidelines**

Disabling the STP causes the VLAN to stop participating in the spanning-tree topology. Interfaces 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 interfaces 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).

**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
```

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

#### Related Commands

Command	Description
<a href="#">show spanning-tree vlan</a>	Displays spanning-tree information.
<a href="#">spanning-tree cost</a>	Sets the path cost for spanning-tree calculations.
<a href="#">spanning-tree guard</a>	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
<a href="#">spanning-tree port-priority</a>	Sets an interface priority.
<a href="#">spanning-tree portfast (global configuration)</a>	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interfaces or enables the Port Fast feature on all nontrunking interfaces.
<a href="#">spanning-tree portfast (interface configuration)</a>	Enables the Port Fast feature on an interface in all its associated VLANs.
<a href="#">spanning-tree uplinkfast</a>	Enables the UplinkFast feature, which accelerates the choice of a new root port.

# speed

Use the **speed** interface configuration command to specify the speed of a 10/100 Mb/s or 10/100/1000 Mb/s port. Use the **no** or **default** form of this command to return the port to its default value.

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

**no speed**

Syntax Description

<b>10</b>	Port runs at 10 Mb/s.
<b>100</b>	Port runs at 100 Mb/s.
<b>1000</b>	Port runs at 1000 Mb/s. This option is valid and visible only on 10/100/1000 Mb/s-ports.
<b>auto</b>	Port automatically detects the speed it should run at based on the port at the other end of the link. If you use the <b>10</b> , <b>100</b> , or <b>1000</b> keywords with the <b>auto</b> keyword, the port only autonegotiates at the specified speeds.
<b>nonegotiate</b>	Autonegotiation is disabled, and the port runs at 1000 Mb/s.

Defaults

The default is **auto**.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You cannot configure speed on the 10-Gigabit Ethernet ports.

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

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.

For guidelines on setting the switch speed and duplex parameters, see the “Configuring Interface Characteristics” chapter in the software configuration guide for this release.

### Examples

This example shows how to set speed on a port to 100 Mb/s:

```
Switch(config)# interface gigabitethernet0/17  
Switch(config-if)# speed 100
```

This example shows how to set a port to autonegotiate at only 10 Mb/s:

```
Switch(config)# interface gigabitethernet0/18  
Switch(config-if)# speed auto 10
```

This example shows how to set a port to autonegotiate at only 10 or 100 Mb/s:

```
Switch(config)# interface gigabitethernet0/17  
Switch(config-if)# speed auto 10 100
```

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

### Related Commands

Command	Description
<a href="#">duplex</a>	Specifies the duplex mode of operation.
<a href="#">show interfaces</a>	Displays the statistical information specific to all interfaces or to a specific interface.

# srr-queue bandwidth limit

Use the **srr-queue bandwidth limit** interface configuration command to limit the maximum output on a port. Use the **no** form of this command to return to the default setting.

```
srr-queue bandwidth limit weight1

no srr-queue bandwidth limit
```


Syntax Description	<i>weight1</i> Percentage of the port speed to which the port should be limited. The range is 10 to 90.
--------------------	---

Defaults	The port is not rate limited and is set to 100 percent.
----------	---

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

Command History	Release	Modification
	12.2(53)EY	This command was introduced.

Usage Guidelines	If you configure this command to 80 percent, the port is idle 20 percent of the time. The line rate drops to 80 percent of the connected speed. These values are not exact because the hardware adjusts the line rate in increments of six.
------------------	---



Note

The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your quality of service (QoS) solution.

Examples	<p>This example shows how to limit a port to 800 Mb/s:</p> <pre>Switch(config)# interface gigabitethernet0/1 Switch(config-if)# srr-queue bandwidth limit 80</pre> <p>You can verify your settings by entering the <b>show mls qos interface</b> <i>[interface-id]</i> <b>queueing</b> privileged EXEC command.</p>
----------	---

## Related Commands

Command	Description
<a href="#">mls qos queue-set output buffers</a>	Allocates buffers to the queue-set.
<a href="#">mls qos srr-queue output cos-map</a>	Maps class of service (CoS) values to egress queue or maps CoS values to a queue and to a threshold ID.
<a href="#">mls qos trust</a>	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
<a href="#">mls qos queue-set output threshold</a>	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation for the queue-set.
<a href="#">radius-server dead-criteria</a>	Maps a port to a queue-set.
<a href="#">show mls qos interface queueing</a>	Displays QoS information.
<a href="#">srr-queue bandwidth shape</a>	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.
<a href="#">srr-queue bandwidth share</a>	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

# srr-queue bandwidth shape

Use the **srr-queue bandwidth shape** interface configuration command to assign the shaped weights and to enable bandwidth shaping on the four egress queues mapped to a port. Use the **no** form of this command to return to the default setting.

```
srr-queue bandwidth shape weight1 weight2 weight3 weight4
```

```
no srr-queue bandwidth shape
```

Syntax Description	<i>weight1 weight2 weight3 weight4</i>	Specify the weights to specify the percentage of the port that is shaped. The inverse ratio (1/ <i>weight</i> ) specifies the shaping bandwidth for this queue. Separate each value with a space. The range is 0 to 65535.
--------------------	--	--

Defaults	Weight1 is set to 25. Weight2, weight3, and weight4 are set to 0, and these queues are in shared mode.
----------	--

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

Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.2(53)EY</td><td>This command was introduced.</td></tr></table>	Release	Modification	12.2(53)EY	This command was introduced.
Release	Modification				
12.2(53)EY	This command was introduced.				

Usage Guidelines	<p>In shaped mode, the queues are guaranteed a percentage of the bandwidth, and they are rate-limited to that amount. Shaped traffic does not use more than the allocated bandwidth even if the link is idle. Use shaping to smooth bursty traffic or to provide a smoother output over time.</p> <p>The shaped mode overrides the shared mode.</p> <p>If you configure a shaped queue weight to 0 by using the <b>srr-queue bandwidth shape</b> interface configuration command, this queue participates in shared mode. The weight specified with the <b>srr-queue bandwidth shape</b> command is ignored, and the weights specified with the <b>srr-queue bandwidth share</b> interface configuration command for a queue come into effect.</p> <p>When configuring queues for the same port for both shaping and sharing, make sure that you configure the lowest numbered queue for shaping.</p>
------------------	---



Note

The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.



## Examples

This example shows how to configure the queues for the same port for both shaping and sharing. Because the weight ratios for queues 2, 3, and 4 are set to 0, these queues operate in shared mode. The bandwidth weight for queue 1 is 1/8, which is 12.5 percent. Queue 1 is guaranteed this bandwidth and limited to it; it does not extend its slot to the other queues even if the other queues have no traffic and are idle. Queues 2, 3, and 4 are in shared mode, and the setting for queue 1 is ignored. The bandwidth ratio allocated for the queues in shared mode is  $4/(4+4+4)$ , which is 33 percent:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
Switch(config-if)# srr-queue bandwidth share 4 4 4 4
```

You can verify your settings by entering the **show mls qos interface** *[interface-id]* **queueing** privileged EXEC command.

## Related Commands

Command	Description
<a href="#">mls qos queue-set output buffers</a>	Allocates buffers to a queue-set.
<a href="#">mls qos srr-queue output cos-map</a>	Maps class of service (CoS) values to an egress queue or maps CoS values to a queue and to a threshold ID.
<a href="#">mls qos trust</a>	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
<a href="#">mls qos queue-set output threshold</a>	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
<a href="#">priority-queue</a>	Enables the egress expedite queue on a port.
<a href="#">radius-server dead-criteria</a>	Maps a port to a queue-set.
<a href="#">show mls qos interface queueing</a>	Displays quality of service (QoS) information.
<a href="#">srr-queue bandwidth share</a>	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

# srr-queue bandwidth share

Use the **srr-queue bandwidth share** interface configuration command to assign the shared weights and to enable bandwidth sharing on the four egress queues mapped to a port. The ratio of the weights is the ratio of frequency in which the shaped round robin (SRR) scheduler dequeues packets from each queue. Use the **no** form of this command to return to the default setting.

```
srr-queue bandwidth share weight1 weight2 weight3 weight4
```

```
no srr-queue bandwidth share
```

Syntax Description	<i>weight1 weight2 weight3 weight4</i>	The ratios of <i>weight1</i> , <i>weight2</i> , <i>weight3</i> , and <i>weight4</i> specify the ratio of the frequency in which the SRR scheduler dequeues packets. Separate each value with a space. The range is 1 to 255.
--------------------	--	--

Defaults	Weight1, weight2, weight3, and weight4 are 25 (1/4 of the bandwidth is allocated to each queue).
----------	--

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

Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.2(53)EY</td><td>This command was introduced.</td></tr></table>	Release	Modification	12.2(53)EY	This command was introduced.
Release	Modification				
12.2(53)EY	This command was introduced.				

**Usage Guidelines**

The absolute value of each weight is meaningless, and only the ratio of parameters is used.

In shared mode, the queues share the bandwidth among them according to the configured weights. The bandwidth is guaranteed at this level but not limited to it. For example, if a queue empties and does not require a share of the link, the remaining queues can expand into the unused bandwidth and share it among themselves.

If you configure a shaped queue weight to 0 by using the **srr-queue bandwidth shape** interface configuration command, this queue participates in SRR shared mode. The weight specified with the **srr-queue bandwidth shape** command is ignored, and the weights specified with the **srr-queue bandwidth share** interface configuration command for a queue take effect.

When configuring queues for the same port for both shaping and sharing, make sure that you configure the lowest numbered queue for shaping.



**Note**

The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

**Examples**

This example shows how to configure the weight ratio of the SRR scheduler running on an egress port. Four queues are used. The bandwidth ratio allocated for each queue in shared mode is  $1/(1+2+3+4)$ ,  $2/(1+2+3+4)$ ,  $3/(1+2+3+4)$ , and  $4/(1+2+3+4)$ , which is 10 percent, 20 percent, 30 percent, and 40 percent for queues 1, 2, 3, and 4. This means that queue 4 has four times the bandwidth of queue 1, twice the bandwidth of queue 2, and one-and-a-third times the bandwidth of queue 3.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```

You can verify your settings by entering the **show mls qos interface** *[interface-id]* **queueing** privileged EXEC command.

**Related Commands**

Command	Description
<a href="#">mls qos queue-set output buffers</a>	Allocates buffers to a queue-set.
<a href="#">mls qos srr-queue output cos-map</a>	Maps class of service (CoS) values to an egress queue or maps CoS values to a queue and to a threshold ID.
<a href="#">mls qos trust</a>	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
<a href="#">mls qos queue-set output threshold</a>	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
<a href="#">priority-queue</a>	Enables the egress expedite queue on a port.
<a href="#">radius-server dead-criteria</a>	Maps a port to a queue-set.
<a href="#">show mls qos interface queueing</a>	Displays quality of service (QoS) information.
<a href="#">srr-queue bandwidth shape</a>	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.

# switchport access

Use the **switchport access** interface configuration command to configure a port as a static-access port. If the switchport mode is set to **access**, the port operates as a member of the specified VLAN.

**switchport access vlan** *vlan-id*

**no switchport access vlan**

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **no switchport access** 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.

Examples

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

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

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

Related Commands

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

# switchport autostate exclude

Use the **switchport autostate exclude** interface configuration command to exclude an interface from the VLAN interface (switch virtual interface) line-state up or down calculation. Use the **no** form of this command to return to the default setting.

**switchport autostate exclude**

**no switchport autostate exclude**

## Syntax Description

This command has no arguments or keywords.

## Defaults

All ports in the VLAN are included in the VLAN interface link-up calculation.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(53)EY	This command was introduced.

## Usage Guidelines

Enter the **switchport autostate exclude** command on a Layer 2 access or trunk port belonging to an SVI.

A VLAN interface (SVI) is up if ports are forwarding traffic in the associated VLAN. When all ports on a VLAN are down or blocking, the SVI is down. For the SVI to be up, at least one port in the VLAN must be up and forwarding. You can use the **switchport autostate exclude** command to exclude a port from the SVI interface line-state up-or-down calculation. For example, you might exclude a monitoring port from the calculations so that the VLAN is not considered up when only the monitoring port is active.

When you enter the **switchport autostate exclude** command on a port, the command applies to all VLANs that are enabled on the port.

You can verify the autostate mode of an interface by entering the **show interface interface-id switchport** privileged EXEC command. If the mode has not been set, the autostate mode does not appear.

## Examples

This example shows how to configure autostate exclude on an interface and to verify the configuration:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport autostate exclude
Switch(config-if)# end
Switch# show interface gigabitethernet0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
```

switchport autostate exclude

Voice VLAN: none  
Administrative private-vlan host-association: none  
Administrative private-vlan mapping: none  
Administrative private-vlan trunk native VLAN: none  
Administrative private-vlan trunk Native VLAN tagging: enabled  
Administrative private-vlan trunk encapsulation: dot1q  
Administrative private-vlan trunk normal VLANs: none  
Administrative private-vlan trunk associations: none  
Administrative private-vlan trunk mappings: none  
Operational private-vlan: none  
Trunking VLANs Enabled: ALL  
Pruning VLANs Enabled: 2-1001  
Capture Mode Disabled  
Capture VLANs Allowed: ALL  
Autostate mode exclude

Related Commands	Command	Description
	<a href="#">show interfaces</a>	Displays the administrative and operational status of a switching (nonrouting) port, including autostate mode, if set.
	<code>[interface-id] switchport</code>	
	<code>show running-config</code>	Displays the current operating configuration.

# switchport host

Use the **switchport host** interface configuration command to optimize a Layer 2 port for a host connection. The **no** form of this command has no affect on the system.

## switchport host

### 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(53)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.

### 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)#
```

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

### Related Commands

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

# switchport mode

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

```
switchport mode { access | dynamic { auto | desirable } | trunk }  
  
no switchport mode { access | dynamic | trunk }
```

Syntax Description

access	Set the port to access mode (either static-access or dynamic-access depending on the setting of the <b>switchport access vlan</b> interface configuration command). The port is set to access unconditionally and operates as a nontrunking, single VLAN interface that sends and receives nonencapsulated (non-tagged) frames. An access port can be assigned to only one VLAN.
dynamic auto	Set the interface trunking mode dynamic parameter to auto to specify that the interface convert the link to a trunk link. This is the default switchport mode.
dynamic desirable	Set the interface trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link.
trunk	Set 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 **dynamic auto**.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)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.

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

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



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

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

Access ports and trunk ports are mutually exclusive.

### 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 set the port to dynamic desirable mode:

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

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

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

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.

### Related Commands

Command	Description
<b>show interfaces switchport</b>	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
<b>switchport access</b>	Configures a port as a static-access or dynamic-access port.
<b>switchport trunk</b>	Configures the trunk characteristics when an interface is in trunking mode.

# switchport nonegotiate

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

**switchport nonegotiate**

**no switchport nonegotiate**

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

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

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(53)EY	This command was introduced.

**Usage Guidelines**

The **no** form of the **switchport nonegotiate** command removes **nonegotiate** status.

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

Internetworking devices that do not support DTP might forward DTP frames improperly and cause misconfigurations. To avoid this, you should turn off DTP by using the **switchport no negotiate** command to configure the interfaces connected to devices that do not support DTP to not forward DTP frames.

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

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

## Examples

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

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

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

## Related Commands

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

# switchport trunk

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

```
switchport trunk {allowed vlan vlan-list |native vlan vlan-id | pruning vlan vlan-list}
```

```
no switchport trunk {allowed vlan | native vlan | pruning vlan}
```

Syntax Description	<b>allowed vlan <i>vlan-list</i></b>	Set the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. See the following <i>vlan-list</i> format. The <b>none</b> keyword is not valid. The default is <b>all</b> .
	<b>native vlan <i>vlan-id</i></b>	Set the native VLAN for sending and receiving untagged traffic when the interface is in IEEE 802.1Q trunking mode. The range is 1 to 4094.
	<b>pruning vlan <i>vlan-list</i></b>	Set the list of VLANs that are eligible for VTP pruning when in trunking mode. The <b>all</b> keyword is not valid.

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 1005; extended-range VLANs (VLAN IDs greater than 1005) are valid in some cases.



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

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

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



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

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**

The default encapsulation is negotiate.

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

Trunk pruning:

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

**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
```

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

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk pruning vlan remove 3,10-15
```

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

Related Commands	Command	Description
	<a href="#">show interfaces switchport</a>	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
	<a href="#">switchport mode</a>	Configures the VLAN membership mode of a port.

# system env temperature threshold yellow

Use the **system env temperature threshold yellow** global configuration command to configure the difference between the yellow and red temperature thresholds that determines the value of yellow threshold. Use the **no** form of this command to return to the default value.

**system env temperature threshold yellow** *value*

**no system env temperature threshold yellow** *value*

<b>Syntax Description</b>	<i>value</i>	Specify the difference between the yellow and red threshold values (in Celsius). The range is 10 to 25. The default value is 10.
---------------------------	--------------	--

<b>Defaults</b>	Difference between Yellow and Red threshold values: Red threshold value:
-----------------	---

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(53)EY	This command was introduced.

<b>Usage Guidelines</b>	<p>You cannot configure the green and red thresholds but can configure the yellow threshold.</p> <p>Use the <b>system env temperature threshold yellow</b> <i>value</i> global configuration command to specify the difference between the yellow and red thresholds and to configure the yellow threshold. For example, if the red threshold is 66 degrees C and you want to configure the yellow threshold as 51 degrees C, set the difference between the thresholds as 15 by using the <b>system env temperature threshold yellow 15</b> command.</p>
-------------------------	---



<b>Note</b>	The internal temperature sensor in the switch measures the internal system temperature and might vary $\pm 5$ degrees C.
-------------	--

<b>Examples</b>	<p>This example sets 15 as the difference between the yellow and red thresholds:</p> <pre>Switch(config)# system env temperature threshold yellow 15 Switch(config)#</pre>
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show env temperature status</b>	Displays the temperature status and threshold levels.

# system mtu

Use the **system mtu** global configuration command to set the maximum packet size or maximum transmission unit (MTU) size for Gigabit Ethernet (10/100/1000) ports, or for 10-Gigabit ports, or for routed ports. Use the **no** form of this command to restore the global MTU value to its default value

**system mtu** {*bytes* | **jumbo** *bytes*}

**no system mtu** [*jumbo*]

Syntax Description	<i>bytes</i>	Change the MTU size for all Fast Ethernet interfaces.
	<b>jumbo</b> <i>bytes</i>	Set the system MTU for Gigabit Ethernet ports and 10-Gigabit Ethernet ports. The system jumbo MTU is the maximum MTU received at the Gigabit Ethernet and 10-Gigabit Ethernet ports.  The range is from 1500 to 9198 bytes.

**Defaults**

The default MTU size for all ports is 1500 bytes.

The default value for the system routing MTU is the system MTU value.

**Command Modes**

Global configuration

Command History	<b>Release</b>	<b>Modification</b>
	12.2(53)EY	This command was introduced.

**Usage Guidelines**

The switch does not support the MTU on a per-interface basis.

If you enter the **system mtu bytes** global configuration command or the **system mtu routing** command on the switch, the commands have no effect.

When you use the **system mtu jumbo bytes** command to change the system jumbo MTU size, you must reset the switch before the new configuration takes effect.

The system MTU setting is saved in the switch environmental variable in NVRAM and becomes effective when the switch reloads. The MTU settings that you enter with the **system mtu jumbo** command are not saved in the switch Cisco IOS configuration file, even if you enter the **copy running-config startup-config** privileged EXEC command. Therefore, if you use TFTP to configure a new switch by using a backup configuration file and want the system MTU to be other than the default, you must explicitly configure the **system mtu jumbo** settings on the new switch and then reload the switch.



---

**Examples**

This example shows how to set the maximum jumbo packet size for Gigabit Ethernet ports to 6000 bytes:

```
Switch(config)# system mtu jumbo 6000  
Switch(config)# exit  
Switch# reload
```

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

---

**Related Commands**

Command	Description
<a href="#">show system mtu</a>	Displays the packet size set for Gigabit Ethernet and 10-Gigabit Ethernet ports.

# tracert mac

Use the **tracert mac** privileged EXEC command to display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.

```
tracert mac [interface interface-id] {source-mac-address} [interface interface-id]
           {destination-mac-address} [vlan vlan-id] [detail]
```

Syntax Description	interface interface-id	(Optional) Specify an interface on the source or destination switch.
	source-mac-address	Specify the MAC address of the source switch in hexadecimal format.
	destination-mac-address	Specify the MAC address of the destination switch in hexadecimal format.
	vlan vlan-id	(Optional) Specify 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) Specify that detailed information appears.

Defaults There is no default.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(53)EY	This command was introduced.

**Usage Guidelines**

For Layer 2 tracert 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 tracert, 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 tracert 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 **tracert 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[WS-C2360-48TD-SD] (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[WS-C2360-48TD-SD] (2.2.6.6)
con6 / WS-C2360-48TD-SD / 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[WS-C2360-48TD-SD] (2.2.6.6)
con6 (2.2.6.6) :Gi00/1 => Gi0/3
con5          (2.2.5.5       ) :   Gi0/3 => Gi00/1
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[WS-C2360-48TD-SD] (2.2.5.5)
con5 / WS-C2360-48TD-SD / 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# tracroute 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# tracroute 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# tracroute 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# tracroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
```

Related Commands	Command	Description
	<b>tracroute mac ip</b>	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

Use the **traceroute mac ip** privileged EXEC command 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.

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

<b>Syntax Description</b>	<i>source-ip-address</i>	Specify the IP address of the source switch as a 32-bit quantity in dotted-decimal format.
	<i>destination-ip-address</i>	Specify the IP address of the destination switch as a 32-bit quantity in dotted-decimal format.
	<i>source-hostname</i>	Specify the IP hostname of the source switch.
	<i>destination-hostname</i>	Specify the IP hostname of the destination switch.
	<b>detail</b>	(Optional) Specify that detailed information appears.

<b>Defaults</b>	There is no default.
-----------------	----------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(53)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 tracroute 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# tracroute 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 / WS-C3750E-24TD / 2.2.6.6 :
    Gi0/0/1 [auto, auto] => Gi0/0/3 [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# tracroute 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) :Gi0/0/1 => Gi0/0/3
con5           (2.2.5.5       ) :   Gi0/0/3 => Gi0/1
con1           (2.2.1.1       ) :   Gi0/0/1 => Gi0/2
con2           (2.2.2.2       ) :   Gi0/0/2 => 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# tracroute 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
<b>tracroute mac</b>	Displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.

# udld

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

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

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

## Syntax Description

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

## 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(53)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

Examples

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

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

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

Related Commands

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



# udld port

Use the **udld port** interface configuration command 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 **no** form of this command to return to the **udld** global configuration command setting or to disable UDLD if entered for a nonfiber-optic port.

**udld port [aggressive]**

**no udld port [aggressive]**

<b>Syntax Description</b>	<b>aggressive</b>	Enable UDLD in aggressive mode on the specified interface.
---------------------------	-------------------	--

<b>Defaults</b>	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 <b>udld enable</b> or <b>udld aggressive</b> global configuration command.  On nonfiber-optic interfaces, UDLD is disabled.
-----------------	---

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(53)EY	This command was introduced.

<b>Usage Guidelines</b>	<p>A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch.</p> <p>UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links. For information about normal and aggressive modes, see the “Configuring UDLD” chapter in the software configuration guide for this release.</p> <p>To enable UDLD in normal mode, use the <b>udld port</b> interface configuration command. To enable UDLD in aggressive mode, use the <b>udld port aggressive</b> interface configuration command.</p> <p>Use the <b>no udld port</b> command on fiber-optic ports to return control of UDLD to the <b>udld enable</b> global configuration command or to disable UDLD on nonfiber-optic ports.</p> <p>Use the <b>udld port aggressive</b> command on fiber-optic ports to override the setting of the <b>udld enable</b> or <b>udld aggressive</b> global configuration command. Use the <b>no</b> form on fiber-optic ports to remove this setting and to return control of UDLD enabling to the <b>udld</b> global configuration command or to disable UDLD on nonfiber-optic ports.</p>
-------------------------	--

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

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 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
```

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

Related Commands

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

# udld reset

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

## udld reset

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

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(53)EY	This command was introduced.

<b>Usage Guidelines</b>	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.
-------------------------	---

<b>Examples</b>	This example shows how to reset all interfaces disabled by UDLD:
-----------------	--

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

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

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

# usb-inactivity-timeout

To configure an inactivity timeout on the USB console, use the **usb-inactivity-timeout** command in console line configuration mode. To remove the inactivity timeout use the **no** form of this command.

**usb-inactivity-timeout** *minutes*

**no usb-inactivity-timeout** *minutes*

Syntax Description	<i>minutes</i>	Time, in minutes, before the console port changes to the RJ-45 port due to inactivity on the USB console. The range is 1 to 240. The default is no timeout.
--------------------	----------------	---

Defaults	Inactivity timeout is not configured.
----------	---------------------------------------

Command Modes	Line configuration
---------------	--------------------

Command History	Release	Modification
	12.2(53)EY	This command was introduced.

Usage Guidelines	The switch has a configurable timeout inactivity that activates the RJ-45 console if the USB console has been activated but no input activity has occurred on the USB console for a specified time period. When the USB console is deactivated due to an inactivity timeout, you can restore its operation by disconnecting and reconnecting the USB cable.
------------------	---

Examples	This example shows how to configure the inactivity timeout:
----------	---

```
Switch# configure terminal
Switch(config)# line console 0
Switch(config-line)# usb-inactivity-timeout 60
```

If there is no input on the USB console for 60 minutes, the console changes to RJ-45, and a system message log appears showing the inactivity timeout.

Related Commands	Command	Description
	<b>no media-type rj45</b>	Resets the console port as the USB port if it has been manually set to the RJ-45 port.

# vlan (global configuration)

Use the **vlan** global configuration command to add a VLAN and to enter the config-vlan mode. Use the **no** form of this command to delete the VLAN. Configuration information for normal-range VLANs (VLAN IDs 1 to 1005) is always saved in the VLAN database. When VLAN Trunking Protocol (VTP) mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005), and the VTP mode, domain name, and the VLAN configuration are saved 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*

<b>Syntax Description</b>	<i>vlan-id</i>	ID of the VLAN to be added and configured. For <i>vlan-id</i> , 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.
---------------------------	----------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.2(53)EY	This command was introduced.

<b>Usage Guidelines</b>	<p>You must use the <b>vlan</b> <i>vlan-id</i> global configuration command to add extended-range VLANs (VLAN IDs 1006 to 4094). Before configuring VLANs in the extended range, you must use the <b>vtp transparent</b> global configuration or VLAN configuration command to put the switch in VTP transparent mode. Extended-range VLANs are not learned by VTP and are not added to the VLAN database, but when VTP mode is transparent, VTP mode and domain name and all VLAN configurations are saved in the running configuration, and you can save them in the switch startup configuration file.</p>
-------------------------	---

When you save the VLAN and VTP configurations in the startup configuration file and reboot the switch, the configuration is selected in these ways:

- If both the VLAN database and the configuration file show the VTP mode as transparent and the VTP domain names match, the VLAN database is ignored. The VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode is server, or if the startup VTP mode or domain names do not match the VLAN database, the VTP mode and the VLAN configuration for the first 1005 VLANs use the VLAN database information.

If you try to create an extended-range VLAN when the switch is not in VTP transparent mode, the VLAN is rejected, and you receive an error message.

If you enter an invalid VLAN ID, you receive an error message and do not enter config-vlan mode.

Entering the **vlan** command with a VLAN ID enables config-vlan 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 the config-vlan mode. Only the **shutdown** command (for VLANs 1 to 1005) takes effect immediately.

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

**Note**

Although all commands are visible, the only VLAN configuration commands that are supported on extended-range VLANs are **mtu** *mtu-size*, **private-vlan**, and **remote-span**. For extended-range VLANs, all other characteristics must remain at the default state.

- **are** *are-number*: defines the maximum number of all-routes explorer (ARE) hops for this VLAN. This keyword applies only to TrCRF VLANs. The range is 0 to 13. The default is 7. If no value is entered, 0 is assumed to be the maximum.
- **backupcrf**: specifies the backup CRF mode. This keyword applies only to TrCRF VLANs.
  - **enable** backup CRF mode for this VLAN.
  - **disable** backup CRF mode for this VLAN (the default).
- **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 (no source-routing bridge) for FDDI-NET, TrBRF, and Token Ring-NET VLANs. The **type** keyword applies only to TrCRF VLANs and is one of these:
  - **srb** (source-route bridging)
  - **srt** (source-route transparent) bridging VLAN
- **exit**: applies changes, increments the VLAN database revision number (VLANs 1 to 1005 only), and exits config-vlan mode.
- **media**: defines the VLAN media type. See [Table 2-16](#) for valid commands and syntax for different media types.

**Note**

The switch supports only Ethernet ports. You configure only FDDI and Token Ring media-specific characteristics for VLAN Trunking Protocol (VTP) global advertisements to other switches. These VLANs are locally suspended.

- **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 if the VTP v2 mode is disabled, or TrCRF if the VTP Version 2 (v) mode is enabled.
- **tr-net** is Token Ring network entity title (NET) media type if the VTP v2 mode is disabled or TrBRF media type if the VTP v2 mode is enabled.
- **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. This parameter identifies the TrBRF to which a TrCRF belongs and is required when defining a TrCRF. The range is 0 to 1005. The default parent VLAN ID is 0 (no parent VLAN) for FDDI and Token Ring VLANs. For both Token Ring and TrCRF VLANs, the parent VLAN ID must already exist in the database and be associated with a Token Ring-NET or TrBRF VLAN.
- **remote-span**: configure the VLAN as a Remote SPAN (RSPAN) VLAN. When the RSPAN feature is added to an existing VLAN, the VLAN is first deleted and is then recreated with the RSPAN feature. Any access ports are deactivated until the RSPAN feature is removed. If VTP is enabled, the new RSPAN VLAN is propagated by VTP for VLAN-IDs that are lower than 1024. Learning is disabled on the VLAN. .
- **ring** *ring-number*: defines the logical ring for an FDDI, Token Ring, or TrCRF VLAN. The range is 1 to 4095. The default for Token Ring VLANs is 0. For FDDI VLANs, there is no default.
- **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 config-vlan 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. This keyword applies only to 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. For FDDI-NET VLANs, the default STP type is **ieee**. For Token Ring-NET VLANs, the default STP type is **ibm**. For FDDI and Token Ring VLANs, the default is no type specified.
  - **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.

**Table 2-16 Valid Commands and Syntax for Different Media Types**

Media Type	Valid Syntax
Ethernet	<b>name</b> <i>vlan-name</i> , <b>media</b> <b>ethernet</b> , <b>state</b> { <b>suspend</b>   <b>active</b> }, <b>said</b> <i>said-value</i> , <b>mtu</b> <i>mtu-size</i> , <b>remote-span</b> , <b>tb-vlan1</b> <i>tb-vlan1-id</i> , <b>tb-vlan2</b> <i>tb-vlan2-id</i>
FDDI	<b>name</b> <i>vlan-name</i> , <b>media</b> <b>fddi</b> , <b>state</b> { <b>suspend</b>   <b>active</b> }, <b>said</b> <i>said-value</i> , <b>mtu</b> <i>mtu-size</i> , <b>ring</b> <i>ring-number</i> , <b>parent</b> <i>parent-vlan-id</i> , <b>tb-vlan1</b> <i>tb-vlan1-id</i> , <b>tb-vlan2</b> <i>tb-vlan2-id</i>

**Table 2-16** Valid Commands and Syntax for Different Media Types (continued)

Media Type	Valid Syntax
FDDI-NET	<b>name</b> <i>vlan-name</i> , <b>media</b> <b>fd-net</b> , <b>state</b> { <b>suspend</b>   <b>active</b> }, <b>said</b> <i>said-value</i> , <b>mtu</b> <i>mtu-size</i> , <b>bridge</b> <i>bridge-number</i> , <b>stp type</b> { <b>ieee</b>   <b>ibm</b>   <b>auto</b> }, <b>tb-vlan1</b> <i>tb-vlan1-id</i> , <b>tb-vlan2</b> <i>tb-vlan2-id</i> If VTP v2 mode is disabled, do not set the <b>stp type</b> to <b>auto</b> .
Token Ring	VTP v1 mode is enabled. <b>name</b> <i>vlan-name</i> , <b>media</b> <b>tokenring</b> , <b>state</b> { <b>suspend</b>   <b>active</b> }, <b>said</b> <i>said-value</i> , <b>mtu</b> <i>mtu-size</i> , <b>ring</b> <i>ring-number</i> , <b>parent</b> <i>parent-vlan-id</i> , <b>tb-vlan1</b> <i>tb-vlan1-id</i> , <b>tb-vlan2</b> <i>tb-vlan2-id</i>
Token Ring concentrator relay function (TrCRF)	VTP v2 mode is enabled. <b>name</b> <i>vlan-name</i> , <b>media</b> <b>tokenring</b> , <b>state</b> { <b>suspend</b>   <b>active</b> }, <b>said</b> <i>said-value</i> , <b>mtu</b> <i>mtu-size</i> , <b>ring</b> <i>ring-number</i> , <b>parent</b> <i>parent-vlan-id</i> , <b>bridge type</b> { <b>srb</b>   <b>srt</b> }, <b>are</b> <i>are-number</i> , <b>ste</b> <i>ste-number</i> , <b>backupcrf</b> { <b>enable</b>   <b>disable</b> }, <b>tb-vlan1</b> <i>tb-vlan1-id</i> , <b>tb-vlan2</b> <i>tb-vlan2-id</i>
Token Ring-NET	VTP v1 mode is enabled. <b>name</b> <i>vlan-name</i> , <b>media</b> <b>tr-net</b> , <b>state</b> { <b>suspend</b>   <b>active</b> }, <b>said</b> <i>said-value</i> , <b>mtu</b> <i>mtu-size</i> , <b>bridge</b> <i>bridge-number</i> , <b>stp type</b> { <b>ieee</b>   <b>ibm</b> }, <b>tb-vlan1</b> <i>tb-vlan1-id</i> , <b>tb-vlan2</b> <i>tb-vlan2-id</i>
Token Ring bridge relay function (TrBRF)	VTP v2 mode is enabled. <b>name</b> <i>vlan-name</i> , <b>media</b> <b>tr-net</b> , <b>state</b> { <b>suspend</b>   <b>active</b> }, <b>said</b> <i>said-value</i> , <b>mtu</b> <i>mtu-size</i> , <b>bridge</b> <i>bridge-number</i> , <b>stp type</b> { <b>ieee</b>   <b>ibm</b>   <b>auto</b> }, <b>tb-vlan1</b> <i>tb-vlan1-id</i> , <b>tb-vlan2</b> <i>tb-vlan2-id</i>

Table 2-17 describes the rules for configuring VLANs.

**Table 2-17** VLAN Configuration Rules

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrCRF VLAN media type.	Specify a parent VLAN ID of a TrBRF that already exists in the database. Specify a ring number. Do not leave this field blank. Specify unique ring numbers when TrCRF VLANs have the same parent VLAN ID. Only one backup concentrator relay function (CRF) can be enabled.
VTP v2 mode is enabled, and you are configuring VLANs other than TrCRF media type.	Do not specify a backup CRF.
VTP v2 mode is enabled, and you are configuring a TrBRF VLAN media type.	Specify a bridge number. Do not leave this field blank.



**Table 2-17**      **VLAN Configuration Rules (continued)**

Configuration	Rule
VTP v1 mode is enabled.	No VLAN can have an STP type set to auto.  This rule applies to Ethernet, FDDI, FDDI-NET, Token Ring, and Token Ring-NET VLANs.
Add a VLAN that requires translational bridging (values are not set to zero).	The translational bridging VLAN IDs that are used must already exist in the database.  The translational bridging VLAN IDs that a configuration points to must also contain a pointer to the original VLAN in one of the translational bridging parameters (for example, Ethernet points to FDDI, and FDDI points to Ethernet).  The translational bridging VLAN IDs that a configuration points to must be different media types than the original VLAN (for example, Ethernet can point to Token Ring).  If both translational bridging VLAN IDs are configured, these VLANs must be different media types (for example, Ethernet can point to FDDI and Token Ring).

### Examples

This example shows how to add an Ethernet VLAN with default media characteristics. The default includes a *vlan-name* of *VLANxxx*, where *xxx* 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** config-vlan configuration command, the VLAN is added if it did not already exist; otherwise, this command does nothing.

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
Switch(config)#
```

This example shows how to create a new extended-range VLAN with all the default characteristics, to enter config-vlan mode, and to save the new VLAN in the switch startup configuration file:

```
Switch(config)# vtp mode transparent
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

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

### Related Commands

Command	Description
<a href="#">show vlan</a>	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.

## vtp (global configuration)

Use the **vtp** global configuration command to set or modify the VLAN Trunking Protocol (VTP) configuration characteristics. Use the **no** form of this command to remove the settings or to return to the default settings.

**vtp** { **domain** *domain-name* | **file** *filename* | **interface** *name* [**only**] | **mode** { **client** | **server** | **transparent** } | **password** *password* | **pruning** | **version** *number* }

**no vtp** { **file** | **interface** | **mode** | **password** | **pruning** | **version** }

Syntax Description	
<b>domain</b> <i>domain-name</i>	Specify the VTP domain name, an ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the switch. The domain name is case sensitive.
<b>file</b> <i>filename</i>	Specify the Cisco IOS file system file where the VTP VLAN configuration is stored.
<b>interface</b> <i>name</i>	Specify the name of the interface providing the VTP ID updated for this device.
<b>only</b>	(Optional) Use only the IP address of this interface as the VTP IP updater.
<b>mode</b>	Specify the VTP device mode as client, server, or transparent.
<b>client</b>	Place the switch in VTP client mode. A switch in VTP client mode is enabled for VTP, and can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on the switch. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.
<b>server</b>	Place the switch in VTP server mode. A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on the switch. The switch can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot.
<b>transparent</b>	Place the switch in VTP transparent mode. A switch in VTP transparent mode is disabled for VTP, does not send advertisements or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.  When VTP mode is transparent, the mode and domain name are saved in the switch running configuration file, and you can save them in the switch startup configuration file by entering the <b>copy running-config startup config</b> privileged EXEC command.
<b>password</b> <i>password</i>	Set the administrative domain password for the generation of the 16-byte secret value used in MD5 digest calculation to be sent in VTP advertisements and to validate received VTP advertisements. The password can be an ASCII string from 1 to 32 characters. The password is case sensitive.
<b>pruning</b>	Enable VTP pruning on the switch.
<b>version</b> <i>number</i>	Set VTP version to Version 1 or Version 2.

**Defaults**

The default filename is *flash:vlan.dat*.

The default mode is server mode.

No domain name or password is defined.

No password is configured.

Pruning is disabled.

The default version is Version 1.

**Command Modes**

Global configuration

**Command History**

Release	Modification
12.2(53)EY	This command was introduced.

**Usage Guidelines**

When you save VTP mode, domain name, and VLAN configurations in the switch startup configuration file and reboot the switch, the VTP and VLAN configurations are selected by these conditions:

- If both the VLAN database and the configuration file show the VTP mode as transparent and the VTP domain names match, the VLAN database is ignored. The VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the startup VTP mode is server mode, or the startup VTP mode or domain names do not match the VLAN database, VTP mode and VLAN configuration for the first 1005 VLANs are selected by VLAN database information, and VLANs greater than 1005 are configured from the switch configuration file.

The **vtp file filename** cannot be used to load a new database; it renames only the file in which the existing database is stored.

Follow these guidelines when configuring a VTP domain name:

- The switch is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the switch does not send any VTP advertisements even if changes occur to the local VLAN configuration. The switch leaves the no-management-domain state after it receives the first VTP summary packet on any port that is trunking or after you configure a domain name by using the **vtp domain** command. If the switch receives its domain from a summary packet, it resets its configuration revision number to 0. After the switch leaves the no-management-domain state, it can no be configured to re-enter it until you clear the NVRAM and reload the software.
- Domain names are case-sensitive.
- After you configure a domain name, it cannot be removed. You can only reassign it to a different domain.

Follow these guidelines when setting VTP mode:

- The **no vtp mode** command returns the switch to VTP server mode.
- The **vtp mode server** command is the same as **no vtp mode** except that it does not return an error if the switch is not in client or transparent mode.
- If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. If you have switches in client mode, be sure to make all VTP or VLAN configuration changes on a switch in server mode. If the receiving switch is in server mode or transparent mode, the switch configuration is not changed.
- Switches in transparent mode do not participate in VTP. If you make VTP or VLAN configuration changes on a switch in transparent mode, the changes are not propagated to other switches in the network.
- If you change the VTP or VLAN configuration on a switch that is in server mode, that change is propagated to all the switches in the same VTP domain.
- The **vtp mode transparent** command disables VTP from the domain but does not remove the domain from the switch.
- The VTP mode must be transparent for you to add extended-range VLANs or for VTP and VLAN information to be saved in the running configuration file.
- If extended-range VLANs are configured on the switch and you attempt to set the VTP mode to server or client, you receive an error message, and the configuration is not allowed.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.

Follow these guidelines when setting a VTP password:

- Passwords are case sensitive. Passwords should match on all switches in the same domain.
- When you use the **no vtp password** form of the command, the switch returns to the no-password state.

Follow these guidelines when setting VTP pruning:

- VTP pruning removes information about each pruning-eligible VLAN from VTP updates if there are no stations belonging to that VLAN.
- If you enable pruning on the VTP server, it is enabled for the entire management domain for VLAN IDs 1 to 1005.
- Only VLANs in the pruning-eligible list can be pruned.
- Pruning is supported with VTP Version 1 and Version 2.

Follow these guidelines when setting the VTP version:

- Toggling the Version 2 (v2) mode state modifies parameters of certain default VLANs.
- Each VTP switch automatically detects the capabilities of all the other VTP devices. To use Version 2, all VTP switches in the network must support Version 2; otherwise, you must configure them to operate in VTP Version 1 mode.
- If all switches in a domain are VTP Version 2-capable, you need only to configure Version 2 on one switch; the version number is then propagated to the other Version-2 capable switches in the VTP domain.
- If you are using VTP in a Token Ring environment, VTP Version 2 must be enabled.

- If you are configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, you must use Version 2.
- If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use Version 1.

You cannot save password, pruning, and version configurations in the switch configuration file.

## Examples

This example shows how to rename the filename for VTP configuration storage to *vtpfilename*:

```
Switch(config)# vtp file vtpfilename
```

This example shows how to clear the device storage filename:

```
Switch(config)# no vtp file vtpconfig
Clearing device storage filename.
```

This example shows how to specify the name of the interface providing the VTP updater ID for this device:

```
Switch(config)# vtp interface gigabitethernet
```

This example shows how to set the administrative domain for the switch:

```
Switch(config)# vtp domain OurDomainName
```

This example shows how to place the switch in VTP transparent mode:

```
Switch(config)# vtp mode transparent
```

This example shows how to configure the VTP domain password:

```
Switch(config)# vtp password ThisIsOurDomain'sPassword
```

This example shows how to enable pruning in the VLAN database:

```
Switch(config)# vtp pruning
Pruning switched ON
```

This example shows how to enable Version 2 mode in the VLAN database:

```
Switch(config)# vtp version 2
```

You can verify your settings by entering the **show vtp status** privileged EXEC command.

## Related Commands

Command	Description
<b>show vtp status</b>	Displays the VTP statistics for the switch and general information about the VTP management domain status.
<b>vtp (VLAN configuration)</b>	Configures VTP domain-name, password, pruning, version, and mode.

# vtp (VLAN configuration)

Use the **vtp** VLAN configuration command to configure VLAN Trunking Protocol (VTP) characteristics. You access VLAN configuration mode by entering the `vlan database` privileged EXEC command. Use the **no** form of this command to return to the default settings, disable the characteristic, or remove the password.

**vtp** { **domain** *domain-name* | **password** *password* | **pruning** | **v2-mode** | { **server** | **client** | **transparent** } }

**no vtp** { **client** | **password** | **pruning** | **transparent** | **v2-mode** }

## Syntax Description

<b>domain</b> <i>domain-name</i>	Set the VTP domain name by entering an ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the switch. The domain name is case sensitive.
<b>password</b> <i>password</i>	Set the administrative domain password for the generation of the 16-byte secret value used in MD5 digest calculation to be sent in VTP advertisements and to validate received VTP advertisements. The password can be an ASCII string from 1 to 32 characters. The password is case sensitive.
<b>pruning</b>	Enable pruning in the VTP administrative domain. VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN.
<b>v2-mode</b>	Enable VLAN Trunking Protocol (VTP) Version 2 in the administrative domains.
<b>client</b>	Place the switch in VTP client mode. A switch in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.
<b>server</b>	Place the switch in VTP server mode. A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot.
<b>transparent</b>	Place the switch in VTP transparent mode. A switch in VTP transparent mode is disabled for VTP, does not send advertisements or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.

## Defaults

- The default mode is server mode.
- No domain name is defined.
- No password is configured.
- Pruning is disabled.
- VTP Version 2 (v2 mode) is disabled.

**Command Modes** VLAN configuration**Command History**

Release	Modification
12.2(53)EY	This command was introduced.

**Usage Guidelines**

If the VTP mode is transparent, the mode and domain name are saved in the switch running configuration file, and you can save the configuration in the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

Follow these guidelines when setting the VTP mode:

- The **no vtp client** and **no vtp transparent** forms of the command return the switch to VTP server mode.
- The **vtp server** command is the same as **no vtp client** or **no vtp transparent** except that it does not return an error if the switch is not in client or transparent mode.
- If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. If you have switches in client mode, make sure to make all VTP or VLAN configuration changes on a switch in server mode. If the receiving switch is in server mode or transparent mode, the switch configuration is not changed.
- Switches in transparent mode do not participate in VTP. If you make VTP or VLAN configuration changes on a switch in transparent mode, the changes are not propagated to other switches in the network.
- If you make a change to the VTP or VLAN configuration on a switch in server mode, that change is propagated to all the switches in the same VTP domain.
- The **vtp transparent** command disables VTP from the domain but does not remove the domain from the switch.
- The VTP mode must be transparent for you to add extended-range VLANs or for the VTP and the VLAN configurations to be saved in the running configuration file.
- If extended-range VLANs are configured on the switch and you attempt to set the VTP mode to server or client, you receive an error message and the configuration is not allowed.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.

**Note**

VTP configuration in VLAN configuration mode is saved in the VLAN database when applied.

Follow these guidelines when configuring a VTP domain name:

- The switch is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the switch does not send any VTP advertisements even if changes occur to the local VLAN configuration. The switch leaves the no-management-domain state after receiving the first VTP summary packet on any port that is currently trunking or after configuring a domain name with the **vtp domain** command. If the switch receives its domain from a summary packet, it resets its configuration revision number to zero. After the switch leaves the no-management-domain state, it can never be configured to reenter it until you clear the NVRAM and reload the software.
- Domain names are case sensitive.
- After you configure a domain name, it cannot be removed. You can reassign it only to a different domain.

Follow these guidelines when configuring a VTP password:

- Passwords are case sensitive. Passwords should match on all switches in the same domain.
- When the **no vtp password** form of the command is used, the switch returns to the no-password state.

Follow these guidelines when enabling VTP pruning:

- If you enable pruning on the VTP server, it is enabled for the entire management domain.
- Only VLANs included in the pruning-eligible list can be pruned.
- Pruning is supported with VTP Version 1 and Version 2.

Follow these guidelines when enabling VTP Version 2 (v2-mode):

- Toggling the version (v2-mode) state modifies certain parameters of certain default VLANs.
- Each VTP switch automatically detects the capabilities of all the other VTP devices. To use VTP Version 2, all VTP switches in the network must support Version 2; otherwise, you must configure them to operate in VTP Version 1 (**no vtp v2-mode**).
- If all switches in a domain are VTP Version 2-capable, you need only to enable VTP Version 2 on one switch; the version number is then propagated to the other Version-2 capable switches in the VTP domain.
- If you are using VTP in a Token Ring environment or configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, VTP Version 2 (**v2-mode**) must be enabled.
- If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use VTP Version 1.



## Examples

This example shows how to place the switch in VTP transparent mode:

```
Switch(vlan)# vtp transparent  
Setting device to VTP TRANSPARENT mode.
```

This example shows how to set the administrative domain for the switch:

```
Switch(vlan)# vtp domain OurDomainName  
Changing VTP domain name from cisco to OurDomainName
```

This example shows how to configure the VTP domain password:

```
Switch(vlan)# vtp password private  
Setting device VLAN database password to private.
```

This example shows how to enable pruning in the proposed new VLAN database:

```
Switch(vlan)# vtp pruning  
Pruning switched ON
```

This example shows how to enable v2 mode in the proposed new VLAN database:

```
Switch(vlan)# vtp v2-mode  
V2 mode enabled.
```

You can verify your settings by entering the **show vtp status** privileged EXEC command.

## Related Commands

Command	Description
<b>show vtp status</b>	Displays the VTP statistics for the switch and general information about the VTP management domain status.
<b>switchport trunk pruning</b>	Configures the VLAN pruning-eligible list for ports in trunking mode.
<b>vtp (global configuration)</b>	Configures the VTP filename, interface, domain name, and mode.

