# 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**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **shutdown** command causes a port to stop forwarding. The default state for a user network interface (UNI) is shut down. Before you can configure a UNI, you must enable it with the **no shutdown** command. Network node interfaces (NNIs) are enabled by default.

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

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

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

## Examples

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

```
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.

## Related Commands

| Command | Description |
|---|---|
| show interfaces | 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

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

## Defaults

No default is defined.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

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

## Examples

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

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

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

## Related Commands

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

# snmp-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**] | **config** | **copy-config** | **entity** | **envmon** [**fan** | **shutdown** | **status** | **supply** | **temperature**] | **flash** | **mac-notification** | **port-security** [**trap-rate** *value*] | **rtr** | **snmp** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] | **storm-control trap-rate** *value* | **stpx** [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**] | **syslog** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete**]

**no snmp-server enable traps** [**bridge** [**newroot**] [**topologychange**] | **config** | **copy-config** | **entity** | **envmon** [**fan** | **shutdown** | **status** | **supply** | **temperature**] | **flash** | **mac-notification** | **port-security** [**trap-rate** *value*] | **rtr** | **snmp** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] | **storm-control trap-rate** *value* | **stpx** [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**] | **syslog** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete**]

## Syntax Description

| | |
|---|---|
| **bridge** [**newroot**] [**topologychange**] | (Optional) Generate Spanning Tree Protocol (STP) bridge MIB traps. The keywords have these meanings:<br>• **newroot**—(Optional) Enable SNMP STP bridge MIB new root traps.<br>• **topologychange**—(Optional) Enable SNMP STP bridge MIB topology change traps. |
| **config** | (Optional) Enable SNMP configuration traps. |
| **copy-config** | (Optional) Enable SNMP copy-configuration traps. |
| **entity** | (Optional) Enable SNMP entity traps. |
| **envmon** [**fan** \| **shutdown** \| **status** \| **supply** \| **temperature**] | Optional) Enable SNMP environmental traps. The keywords have these meanings:<br>• **fan**—(Optional) Enable fan traps.<br>• **shutdown**—(Optional) Enable environmental monitor shutdown traps.<br>• **status**—(Optional) Enable SNMP environmental status-change traps.<br>• **supply**—(Optional) Enable environmental monitor power-supply traps.<br>• **temperature**—(Optional) Enable environmental monitor temperature traps. |
| **flash** | (Optional) Enable SNMP flash notifications. |
| **mac-notification** | (Optional) Enable MAC address notification traps. |
| **port-security** [**trap-rate** *value*] | (Optional) Enable port security traps. Use the **trap-rat**e keyword to set the maximum number of port-security traps sent per second. The range is from 0 to 1000; the default is 0 (no limit imposed; a trap is sent at every port-security occurrence). |
| **rtr** | (Optional) Enable SNMP Response Time Reporter traps. |

| | |
|---|---|
| **snmp** [**authentication** \| **coldstart** \| **linkdown** \| **linkup** \| **warmstart**] | (Optional) Enable SNMP traps. The keywords have these meanings:<br>• **authentication**—(Optional) Enable authentication trap.<br>• **coldstart**—(Optional) Enable cold-start trap.<br>• **linkdown**—(Optional) Enable linkdown trap.<br>• **linkup**—(Optional) Enable linkup trap.<br>• **warmstart**—(Optional) Enable warm-start trap. |
| **storm-control trap-rate** *value* | (Optional) Enable storm-control traps. Use the **trap-rat**e keyword to set the maximum number of storm-control traps sent per second. The range is from 0 to 1000; the default is 0 (no limit is imposed; a trap is sent at every storm-control occurrence). |
| **stpx** [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**] | (Optional) Enable SNMP STPX MIB traps. The keywords have these meanings:<br>• **inconsistency**—(Optional) Enable SNMP STPX MIB inconsistency update traps.<br>• **root-inconsistency**—(Optional) Enable SNMP STPX MIB root inconsistency update traps.<br>• **loop-inconsistency**—(Optional) Enable SNMP STPX MIB loop inconsistency update traps. |
| **syslog** | (Optional) Enable SNMP syslog traps. |
| **tty** | (Optional) Send TCP connection traps. This is enabled by default. |
| **vlan-membership** | (Optional) Enable SNMP VLAN membership traps. |
| **vlancreate** | (Optional) Enable SNMP VLAN-created traps. |
| **vlandelete** | (Optional) Enable SNMP VLAN-deleted traps. |

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

## Defaults

The sending of SNMP traps is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | 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 port security traps to the NMS:

```
Switch(config)# snmp-server enable traps port security
```

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

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the running configuration on the switch. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**. |
| **snmp-server host** | 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

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

| | |
|---|---|
| *notification-type* | (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:<br>• **bridge**—Send SNMP Spanning Tree Protocol (STP) bridge MIB traps.<br>• **config**—Send SNMP configuration traps.<br>• **copy-config**—Send SNMP copy configuration traps.<br>• **entity**— Send SNMP entity traps.<br>• **envmon**—Send environmental monitor traps.<br>• **flash**—Send SNMP FLASH notifications.<br>• **mac-notification—**Send SNMP MAC notification traps.<br>• **port-security—**Send SNMP port-security traps.<br>• **rtr—**Send SNMP Response Time Reporter traps.<br>• **snmp—**Send SNMP-type traps.<br>• **storm-control—**Send SNMP storm-control traps.<br>• **stpx—**Send SNMP STP extended MIB traps.<br>• **syslog—**Send SNMP syslog traps.<br>• **tty—**Send TCP connection traps.<br>• **vlan-membership—** Send SNMP VLAN membership traps.<br>• **vlancreate—**Send SNMP VLAN-created traps.<br>• **vlandelete—**Send SNMP VLAN-deleted traps. |

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

## Defaults

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

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

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

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

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | 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 |
|---|---|
| **show running-config** | Displays the running configuration on the switch. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**. |
| **snmp-server enable traps** | 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

| | |
|---|---|
| **added** | Enable the MAC notification trap whenever a MAC address is added on this interface. |
| **removed** | 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(25)EX | 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 |
|---|---|
| **clear mac address-table notification** | Clears the MAC address notification global counters. |
| **mac address-table notification** | Enables the MAC address notification feature. |
| **show mac address-table notification** | Displays the MAC address notification settings for all interfaces or on the specified interface when the **interface** keyword is appended. |
| **snmp-server enable traps** | Sends the SNMP MAC notification traps when the **mac-notification** keyword is appended. |

# spanning-tree bpdufilter

Use the **spanning-tree bpdufilter** interface configuration command on a network node interface (NNI) to prevent the 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 bpdufilter** {**disable** | **enable**}

**no spanning-tree bpdufilter**

## Syntax Description

| | |
|---|---|
| **disable** | Disable BPDU filtering on the specified NNI. |
| **enable** | Enable BPDU filtering on the specified NNI. |

## Defaults

BPDU filtering is disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure BPDU filtering only on NNIs. To set a port as an NNI, enter the **port-type nni** interface configuration command.

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 NNI 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 NNIs by using the **spanning-tree portfast bpdufilter default** global configuration command.

You can use the **spanning-tree bpdufilter** interface configuration command on an NNI to override the setting of the **spanning-tree portfast bpdufilter 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 bpdufilter enable
```

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

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the current operating configuration. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**. |
| **spanning-tree portfast (global configuration)** | Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled NNIs or enables the Port Fast feature on all nontrunking NNIs. |
| **spanning-tree portfast (interface configuration)** | Enables the Port Fast feature on an NNI and all its associated VLANs. |

# spanning-tree bpduguard

Use the **spanning-tree bpduguard** interface configuration command on a network node interface (NNI) to put the 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

| | |
|---|---|
| **disable** | Disable BPDU guard on the specified NNI. |
| **enable** | Enable BPDU guard on the specified NNI. |

## Defaults

BPDU guard is disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure BPDU guard only on NNIs. To set a port as an NNI, enter the **port-type nni** interface configuration command.

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

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

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

You can use the **spanning-tree bpduguard** interface configuration command on an NNI 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 current operating configuration. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**. |
| **spanning-tree portfast (global configuration)** | Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled NNIs or enables the Port Fast feature on all nontrunking NNIs. |
| **spanning-tree portfast (interface configuration)** | Enables the Port Fast feature on an NNI and all its associated VLANs. |

# spanning-tree cost

Use the **spanning-tree cost** interface configuration command on a network node interface (NNI) 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

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

## Defaults

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

- 1000 Mbps—4
- 100 Mbps—19
- 10 Mbps—100

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure spanning-tree cost only on NNIs. To set a port as an NNI, enter the **port-type nni** interface configuration command.

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

If you configure an NNI 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 |
|---|---|
| **show spanning-tree interface** *interface-id* | Displays spanning-tree information for the specified interface. |
| **spanning-tree port-priority** | Configures an NNI priority. |
| **spanning-tree vlan priority** | 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(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). This command affects only network node interfaces (NNIs).

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

# spanning-tree extend system-id

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(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). This command affects only network node interfaces (NNIs).

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

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

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

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

## Related Commands

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

# spanning-tree guard

Use the **spanning-tree guard** interface configuration command on a network node interface (NNI) to enable root guard or loop guard on all the VLANs associated with the selected NNI. 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

| | |
|---|---|
| **loop** | Enable loop guard. |
| **none** | Disable root guard or loop guard. |
| **root** | 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(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure spanning-tree guard only on NNIs. To set a port as an NNI, enter the **port-type nni** interface configuration command.

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

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

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

Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send bridge protocol data units (BPDUs) on root or alternate

ports. When the switch is operating in MST mode, BPDUs are not sent on nonboundary interfaces if the interface is blocked by loop guard in all MST instances. On a boundary interface, loop guard blocks the interface in all MST instances.

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

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

## 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 |
|---|---|
| **show running-config** | Displays the current operating configuration. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**. |
| **spanning-tree cost** | Sets the path cost for spanning-tree calculations. |
| **spanning-tree loopguard default** | Prevents alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. |
| **spanning-tree mst cost** | Configures the path cost for MST calculations. |
| **spanning-tree mst port-priority** | Configures an NNI priority. |
| **spanning-tree mst root** | Configures the MST root switch priority and timers based on the network diameter. |
| **spanning-tree port-priority** | Configures an NNI priority. |
| **spanning-tree vlan priority** | Sets the switch priority for the specified spanning-tree instance. |

# spanning-tree link-type

Use the **spanning-tree link-type** interface configuration command on a network node interface (NNI) to override the default link-type setting, which is determined by the duplex mode of the NNI, 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

| | |
|---|---|
| **point-to-point** | Specify that the link type of an NNI is point-to-point. |
| **shared** | Specify that the link type of an NNI 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(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure spanning-tree link type only on NNIs. To set a port as an NNI, enter the **port-type nni** interface configuration command.

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

# spanning-tree loopguard default

Use the **spanning-tree loopguard default** global configuration command to enable loopguard by default on all network node interfaces (NNIs). Enabling loopguard prevents 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

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is supported only on NNIs. This command has no effect on user network interfaces (UNIs).

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 NNIs 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 |
|---|---|
| **show running-config** | Displays the current operating configuration. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**. |
| **spanning-tree guard loop** | Enables the loop guard feature on all the VLANs associated with the specified NNI. |

# 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**

## Syntax Description

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

## Defaults

The default mode is rapid PVST+.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is supported on the switch only on network node interfaces (NNIs). It is not supported on user network interfaces (UNIs).

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 PVST+ on the switch:

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

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

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the current operating configuration. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**. |

# 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(25)EX | This command was introduced. |

## Usage Guidelines

On the Cisco ME switch, spanning-tree MST configuration is supported only on network node interfaces (NNIs). User network interfaces (UNIs) do not participate in Spanning Tree Protocol (STP).

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 15. 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 16 MST instances. The number of VLANs that can be mapped to a particular MST instance is unlimited.

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

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

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

## Examples

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

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

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

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

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

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

## Related Commands

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

# spanning-tree mst cost

Use the **spanning-tree mst cost** interface configuration command on a network node interface (NNI) 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

| | |
|---|---|
| *instance-id* | Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 15. |
| *cost* | 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 Mbps—20000
- 100 Mbps—200000
- 10 Mbps—2000000

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure path cost only on NNIs. To set a port as an NNI, enter the **port-type nni** interface configuration command.

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

# spanning-tree mst forward-time

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**

## Syntax Description

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

## Defaults

The default is 15 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

On the Cisco ME switch, spanning-tree MST configuration is supported only on network node interfaces (NNIs). User network interfaces (UNIs) do not participate in Spanning Tree Protocol (STP).

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

## Examples

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

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

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

## Related Commands

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

# spanning-tree mst hello-time

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**

## Syntax Description

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

## Defaults

The default is 2 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

On the Cisco ME switch, spanning-tree MST configuration is supported only on network node interfaces (NNIs). User network interfaces (UNIs) do not participate in Spanning Tree Protocol (STP).

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

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

## Examples

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

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

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

## Related Commands

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

# spanning-tree mst max-age

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**

## Syntax Description

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

## Defaults

The default is 20 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25(EX) | This command was introduced. |

## Usage Guidelines

On the Cisco ME switch, spanning-tree MST configuration is supported only on network node interfaces (NNIs). User network interfaces (UNIs) do not participate in Spanning Tree Protocol (STP).

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

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

## Examples

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

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

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

## Related Commands

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

# spanning-tree mst max-hops

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**

## Syntax Description

| | |
|---|---|
| *hop-count* | Number of hops in a region before the BPDU is discarded. The range is 1 to 40 hops. |

## Defaults

The default is 20 hops.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

On the Cisco ME switch, spanning-tree MST configuration is supported only on network node interfaces (NNIs). User network interfaces (UNIs) do not participate in Spanning Tree Protocol (STP).

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

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

## Examples

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

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

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

## Related Commands

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

# spanning-tree mst port-priority

Use the **spanning-tree mst port-priority** interface configuration command on a network node interface (NNI) 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

| | |
|---|---|
| *instance-id* | Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 15. |
| *priority* | The range is 0 to 240 in increments of 16. Valid priority values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority. |

## Defaults

The default is 128.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure spanning-tree MST port priority only on NNIs. To set a port as an NNI, enter the **port-type nni** interface configuration command.

You can assign higher priority values (lower numerical values) to NNIs that you want selected first and lower priority values (higher numerical values) that you want selected last. If all NNIs 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 |
|---|---|
| **show spanning-tree mst interface** *interface-id* | Displays MST information for the specified interface. |
| **spanning-tree mst cost** | Sets the path cost for MST calculations. |
| **spanning-tree mst priority** | Sets the switch priority for the specified spanning-tree instance. |

# spanning-tree mst 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

| | |
|---|---|
| *instance-id* | Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 15. |
| **priority** | 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.<br>The range is 0 to 61440 in increments of 4096. Valid priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected. |

## Defaults

The default is 32768.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs); it is only supported on network node interfaces (NNIs).

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

# spanning-tree mst root

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

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

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

## Syntax Description

| | |
|---|---|
| *instance-id* | Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 15. |
| **root primary** | Force this switch to be the root switch. |
| **root secondary** | Set this switch to be the root switch should the primary root switch fail. |
| **diameter** *net-diameter* | (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. |
| **hello-time** *seconds* | (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(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs); it is only supported on network node interfaces (NNIs).

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

# spanning-tree port-priority

Use the **spanning-tree port-priority** interface configuration command on a network node interface (NNI) 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

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

## Defaults

The default is 128.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure spanning-tree port priority only on NNIs. To set a port as an NNI, enter the **port-type nni** interface configuration command.

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 NNI to the VLAN.

If you configure an NNI 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 |
|---|---|
| **show spanning-tree interface** *interface-id* | Displays spanning-tree information for the specified interface. |
| **spanning-tree cost** | Sets the path cost for spanning-tree calculations. |
| **spanning-tree vlan priority** | Sets the switch priority for the specified spanning-tree instance. |

# spanning-tree portfast (global configuration)

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

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

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

## Syntax Description

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

## Defaults

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

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs) on the switch. Spanning-tree configuration affects only NNIs. To set a port as an NNI, enter the **port-type nni** interface configuration command.

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

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

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

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

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

Use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking NNIs. Configure Port Fast only on NNIs 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 NNI moves directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-delay time.

You can override the **spanning-tree portfast default** global configuration command by using the **spanning-tree portfast** interface configuration command on an NNI. You can use the **no spanning-tree portfast default** global configuration command to disable Port Fast on all NNIs 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 bpdufilter default
```

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

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

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

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

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

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the current operating configuration. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**. |
| **spanning-tree bpdufilter** | Prevents an interface from sending or receiving BPDUs. |
| **spanning-tree bpduguard** | Puts an NNI in the error-disabled state when it receives a BPDU. |
| **spanning-tree portfast (interface configuration)** | Enables the Port Fast feature on an NNI in all its associated VLANs. |

# spanning-tree portfast (interface configuration)

Use the **spanning-tree portfast** interface configuration command on a network node interface (NNI) to enable the Port Fast feature on an NNI in all its associated VLANs. When the Port Fast feature is enabled, the NNI 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

| | |
|---|---|
| **disable** | (Optional) Disable the Port Fast feature on the specified interface. |
| **trunk** | (Optional) Enable the Port Fast feature on a trunking interface. |

## Defaults

The Port Fast feature is disabled on all NNIs.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can enable the spanning-tree Port Fast feature only on NNIs. To set a port as an NNI, enter the **port-type nni** interface configuration command.

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

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

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

This feature affects all VLANs on the NNI.

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

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

If you configure the **spanning-tree portfast default** global configuration command, you can disable Port Fast on an NNI that is not a trunk interface by using the **spanning-tree portfast disable** 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 |
|---|---|
| **show running-config** | Displays the current operating configuration. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**. |
| **spanning-tree bpdufilter** | Prevents an interface from sending or receiving bridge protocol data units (BPDUs). |
| **spanning-tree bpduguard** | Puts an interface in the error-disabled state when it receives a BPDU. |
| **spanning-tree portfast (global configuration)** | Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled NNIs or enables the Port Fast feature on all nontrunking NNIs. |

# 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

| | |
|---|---|
| *vlan-id* | VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. |
| **forward-time** *seconds* | (Optional) 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. |
| **hello-time** *seconds* | (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. |
| **max-age** *seconds* | (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. |
| **priority** *priority* | (Optional) Set the switch priority for the specified spanning-tree instance. This setting affects the likelihood that this switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch.<br>The range is 0 to 61440 in increments of 4096. Valid priority values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected. |
| **root primary** | (Optional) Force this switch to be the root switch. |
| **root secondary** | (Optional) Set this switch to be the root switch should the primary root switch fail. |
| **diameter** *net-diameter* | (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 |
|---|---|
| 12.25(EX) | This command was introduced. |

**Usage Guidelines** The switch does not support Spanning Tree Protocol (STP) on user network interfaces (UNIs). Only the switch network node interfaces (NNIs) in a VLAN participate in STP.

Disabling the STP causes the VLAN to stop participating in the spanning-tree topology. NNIs 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 NNIs 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 |
|---|---|
| **show spanning-tree vlan** | Displays spanning-tree information. |
| **spanning-tree cost** | Sets the path cost for spanning-tree calculations. |
| **spanning-tree guard** | Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface. |
| **spanning-tree port-priority** | Sets an interface priority. |
| **spanning-tree portfast (global configuration)** | Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled NNIs or enables the Port Fast feature on all nontrunking NNIs. |
| **spanning-tree portfast (interface configuration)** | Enables the Port Fast feature on an NNI in all its associated VLANs. |

# speed

Use the **speed** interface configuration command to specify the speed of a 10/100 Mbps or 10/100/1000 Mbps 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**

**Note** For speed configurations restrictions on small form-factor pluggable (SFP) module ports, see the "Usage Guidelines" section.

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

## Syntax Description

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

## Defaults

The default is **auto**.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You can configure the Fast Ethernet port speed as either 10 or 100 Mbps.

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

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

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

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

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

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

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

## Examples

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

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

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

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

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

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

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

## Related Commands

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

# storm-control

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

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

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

## Syntax Description

| | |
|---|---|
| **broadcast** | Enable broadcast storm control on the interface. |
| **multicast** | Enable multicast storm control on the interface. |
| **unicast** | Enable unicast storm control on the interface. |
| **level** *level* [*level-low*] | Specify the rising and falling suppression levels as a percentage of total bandwidth of the port.<br>• *level*—Rising suppression level, up to two decimal places. The range is 0.00 to 100.00. Block the flooding of storm packets when the value specified for *level* is reached.<br>• *level-low*—(Optional) Falling suppression level, up to two decimal places. The range is 0.00 to 100.00. This value must be less than or equal to the rising suppression value. If you do not configure a falling suppression level, it is set to the rising suppression level. |
| **level bps** *bps* [*bps-low*] | Specify the rising and falling suppression levels as a rate in bits per second at which traffic is received on the port.<br>• *bps*—Rising suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. Block the flooding of storm packets when the value specified for *bps* is reached.<br>• *bps-low*—(Optional) Falling suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. This value must be equal to or less than the rising suppression value.<br>You can use metric suffixes such as k, m, and g for large number thresholds. |

| | |
|---|---|
| **level pps** *pps* [*pps-low*] | Specify the rising and falling suppression levels as a rate in packets per second at which traffic is received on the port.<br>• *pps*—Rising suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. Block the flooding of storm packets when the value specified for *pps* is reached.<br>• *pps-low*—(Optional) Falling suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. This value must be equal to or less than the rising suppression value.<br>You can use metric suffixes such as k, m, and g for large number thresholds. |
| **action** {**shutdown** \| **trap**} | Action taken when a storm occurs on a port. The default action is to filter traffic and to not send an Simple Network Management Protocol (SNMP) trap.<br>The keywords have these meanings:<br>• **shutdown**—Disables the port during a storm.<br>• **trap**—Sends an SNMP trap when a storm occurs. |

## Defaults

Broadcast, multicast, and unicast storm control are disabled.

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

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Storm control is supported only on physical interfaces. It is not supported on EtherChannel port channels, even though it is available in the command-line interface (CLI). If the port is a user network interface (UNI), you must use the **no shutdown** interface configuration command to enable it before using the **storm-control** command. UNIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

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

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

**Note** When the storm control threshold for multicast traffic is reached, all multicast traffic except control traffic, such as bridge protocol data unit (BDPU) and Cisco Discovery Protocol (CDP) frames, are blocked.

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

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

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

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

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

## Examples

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

```
Switch(config-if)# storm-control broadcast level 75.5
```

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

```
Switch(config-if)# storm-control unicast level 87 65
```

This example shows how to enable multicast storm control on a port with a 2000-packets-per-second rising suppression level and a 1000-packets-per-second falling suppression level:

```
Switch(config-if)# storm-control multicast level pps 2k 1k
```

This example shows how to enable the **shutdown** action on a port:

```
Switch(config-if)# storm-control action shutdown
```

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

## Related Commands

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

# switchport

Use the **switchport** interface configuration command with no keywords to put an interface that was processing traffic through the CPU into normal switching mode. Use the **no** form of this command to put an interface in Layer 3 mode.

**switchport**

**no switchport**

## Syntax Description

This command has no arguments or keywords.

## Defaults

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

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Use the **no switchport** command (without parameters) to set the interface so that traffic on the interface is processed by the CPU. You must enter the **no switchport** command and then assign an IP address to the port.

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

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

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

## Examples

This example shows how to cause an interface to stop operating as a switching port and process traffic on the port through the CPU.

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

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

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

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

## Related Commands

| Command | Description |
|---|---|
| **show interfaces switchport** | Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings. |
| **show running-config** | Displays the current operating configuration. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**. |

# switchport access vlan

Use the **switchport access vlan** interface configuration command to configure a port as a static-access or dynamic-access port. If the switchport mode is set to **access** (by using the **switchport mode** interface configuration command), use this command to set the port to operate as a member of the specified VLAN or to specify that the port uses VLAN Membership Policy Server (VMPS) protocol where VLAN assignment based on the incoming packets it receives. Use the **no** form of this command to reset the access VLAN mode to the default VLAN for the switch.

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

**no switchport access vlan**

## Syntax Description

| | |
|---|---|
| *vlan-id* | Configure the interface as a static access port with the VLAN ID of the access mode VLAN; the range is 1 to 4094. |
| **dynamic** | Specify that the access mode VLAN is dependent on the VMPS protocol. The port is assigned to a VLAN based on the source MAC address of a host (or hosts) connected to the port. The switch sends every new MAC address received to the VMPS server to obtain the VLAN name to which the dynamic-access port should be assigned. If the port already has a VLAN assigned and the source has already been approved by the VMPS, the switch forwards the packet to the VLAN.<br>**Note** This keyword is visible only on user network interfaces (UNIs). |

## Defaults

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

A dynamic-access port is initially a member of no VLAN and receives its assignment based on the packet it receives.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

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

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

An access port can be assigned to only one VLAN.

The VMPS server (such as a Catalyst 6500 series switch) must be configured before a port is configured as dynamic.

If the specified VLAN is configured as a UNI community VLAN, the interface is configured as UNI community port. Otherwise the port is configured as a UNI isolated port.

This command is supported on IEEE802.1Q tunnel ports.

These restrictions apply to dynamic-access ports:

- The **dynamic** keyword is not visible on network node interfaces (NNIs).
- The software implements the VLAN Query Protocol (VQP) client, which can query a VMPS such as a Catalyst 6500 series switch. The switch cannot be a VMPS servers. The VMPS server must be configured before a port is configured as dynamic.
- Use dynamic-access ports only to connect end stations. Connecting them to switches or routers (that use bridging protocols) can cause a loss of connectivity.
- Dynamic-access ports can only be in one VLAN and do not use VLAN tagging.
- Dynamic-access ports cannot be configured as:
  - Members of an EtherChannel port group (dynamic-access ports cannot be grouped with any other port, including other dynamic ports).
  - Source or destination ports in a static address entry.
  - Monitor ports.

## Examples

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

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

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 |
|---|---|
| **show interfaces switchport** | Displays the administrative and operational status of a switching port, including port blocking and port protection settings. |
| **switchport mode** | Configures the VLAN membership mode of a port. |

# switchport block

Use the **switchport block** interface configuration command to prevent unknown multicast or unicast packets from being forwarded. Use the **no** form of this command to allow forwarding unknown multicast or unicast packets.

**switchport block** {**multicast | unicast**}

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

## Syntax Description

| | |
|---|---|
| **multicast** | Specify that unknown multicast traffic should be blocked. |
| **unicast** | Specify that unknown unicast traffic should be blocked. |

## Defaults

Unknown multicast and unicast traffic is not blocked.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

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

If the port is a user network interface (UNI), you must use the **no shutdown** interface configuration command to enable it before using the **switchport block** command. UNIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

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

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

## Examples

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

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

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

**Related Commands**

| Command | Description |
|---|---|
| **show interfaces switchport** | Displays the administrative and operational status of a switching port, including port blocking and port protection settings. |

# switchport host

Use the **switchport host** interface configuration command to optimize a 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(25)EX | 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 |
|---|---|
| **show interfaces switchport** | Displays the administrative and operational status of a switching 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 default.

**switchport mode** {**access** | **private-vlan** | **trunk**}

**no switchport mode**

## Syntax Description

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

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

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

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

When you enter **trunk** mode, the interface changes to permanent trunking mode and negotiates to convert the link into a trunk link even if the interface connecting to it does not agree to the change. If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.

Access ports and trunk ports are mutually exclusive.

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

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

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

**Note** Only user network interfaces (UNIs) can be dynamic-access ports.

## Examples

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

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

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

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

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 |
|---|---|
| **show interfaces switchport** | Displays the administrative and operational status of a switching port, including port blocking and port protection settings. |
| **switchport access vlan** | Configures a port as a static-access or dynamic-access port. |
| **switchport trunk** | Configures the trunk characteristics when an interface is in trunking mode. |

# switchport mode private-vlan

Use the **switchport mode private-vlan** interface configuration command to configure a port as a promiscuous or host private VLAN port. Use the **no switchport mode** command to reset the mode to the default access mode.

**switchport mode private-vlan** {**host** | **promiscuous**}

**no switchport mode private-vlan**

**Note** The **promiscuous** keyword is visible only on network node interfaces (NNIs).

## Syntax Description

| | |
|---|---|
| **host** | Configure the interface as a private-VLAN host port. Host ports belong to private-VLAN secondary VLANs and are either community ports or isolated ports, depending on the VLAN that they belong to. |
| **promiscuous** | Configure the interface as a private-VLAN promiscuous port. Promiscuous ports are members of private-VLAN primary VLANs. This keyword is only on available NNIs. User network interfaces (UNIs) cannot be configured as private VLAN promiscuous ports. |

## Defaults

The default private-VLAN mode is neither host nor promiscuous.

The default switchport mode is **access**.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

A private-VLAN promiscuous port must be an NNI. To configure a UNI as an NNI, enter the **port-type nni** interface configuration command. There can be no more than four NNIs on a switch.

A private-VLAN host or promiscuous port cannot be a Switched Port Analyzer (SPAN) destination port. If you configure a SPAN destination port as a private-VLAN host or promiscuous port, the port becomes inactive.

Do not configure private VLAN on ports with these other features:

- dynamic-access port VLAN membership
- Port Aggregation Protocol (PAgP) for only NNIs
- Link Aggregation Control Protocol (LACP) only for NNIs
- Multicast VLAN Registration (MVR)

A private-VLAN port cannot be a SPAN destination port.

While a port is part of the private-VLAN configuration, any EtherChannel configuration for it is inactive.

A private-VLAN port cannot be a secure port and should not be configured as a protected port.

**Note** For more information about private-VLAN interaction with other features, see the software configuration guide for this release.

If the port is an NNI, we strongly recommend that you enable spanning tree Port Fast and bridge-protocol-data-unit (BPDU) guard on isolated and community host ports to prevent STP loops due to misconfigurations and to speed up STP convergence.

If you configure a port as a private-VLAN host port and you do not configure a valid private-VLAN association by using the **switchport private-vlan host-association** interface configuration command, the interface becomes inactive.

If you configure an NNI as a private-VLAN promiscuous port and you do not configure a valid private VLAN mapping by using the **switchport private-vlan mapping** interface configuration command, the interface becomes inactive.

## Examples

This example shows how to configure an interface as a private-VLAN host port and associate it to primary VLAN 20. The interface is a member of secondary isolated VLAN 501 and primary VLAN 20.

**Note** When you configure an NNI as a private VLAN host port, you should also enable BPDU guard and Port Fast by using the **spanning-tree portfast bpduguard default** global configuration command and the **spanning-tree portfast** interface configuration command.

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 501
Switch(config-if)# end
```

This example shows how to configure an NNI as a private VLAN promiscuous port and map it to a private VLAN. The interface is a member of primary VLAN 20 and secondary VLANs 501 to 503 are mapped to it.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 501-503
Switch(config-if)# end
```

You can verify private VLAN switchport mode by using the **show interfaces** *interface-id* **switchport** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **private-vlan** | Configures a VLAN as a community, isolated, or primary VLAN or associates a primary VLAN with secondary VLANs. |
| **show interfaces switchport** | Displays the administrative and operational status of a switching port, including private VLAN configuration. |
| **switchport private-vlan** | Configures private VLAN associations and mappings between primary and secondary VLANs on an interface. |

# switchport port-security

Use the **switchport port-security** interface configuration command without keywords to enable port security on the interface. Use the keywords to configure secure MAC addresses, sticky MAC address learning, a maximum number of secure MAC addresses, or the violation mode. Use the **no** form of this command to disable port security or to set the parameters to their default states.

**switchport port-security** [**mac-address** *mac-address* [**vlan access**] | **mac-address sticky** [*mac-address* | **vlan access**]] [**maximum** *value* [**vlan access**]]

**no switchport port-security** [**mac-address** *mac-address* [**vlan access**] | **mac-address sticky** [*mac-address* | **vlan access**]] [**maximum** *value* [**vlan access**]]

**switchport port-security** [**aging**] [**violation** {**protect | restrict | shutdown**}]

**no switchport port-security** [**aging**] [**violation** {**protect | restrict | shutdown**}]

## Syntax Description

| | |
|---|---|
| **aging** | (Optional) See the **switchport port-security aging** command. |
| **mac-address** *mac-address* | (Optional) Specify a secure MAC address for the interface by entering a 48-bit MAC address. You can add additional secure MAC addresses up to the maximum value configured. |
| **vlan** *vlan-id* | (Optional) On a trunk port only, specify the VLAN ID and the MAC address. If no VLAN ID is specified, the native VLAN is used. |
| **vlan access** | (Optional) On an access port only, specify the VLAN as an access VLAN. |
| **mac-address sticky** [*mac-address*] | (Optional) Enable the interface for *sticky learning* by entering only the **mac-address sticky** keywords. When sticky learning is enabled, the interface adds all secure MAC addresses that are dynamically learned to the running configuration and converts these addresses to sticky secure MAC addresses.<br>(Optional) Enter a *mac-address* to specify a sticky secure MAC address. |
| **maximum** *value* | (Optional) Set the maximum number of secure MAC addresses for the interface.The maximum number of secure MAC addresses that you can configure on a switch is set by the maximum number of available MAC addresses allowed in the system, approximately 2000. This number represents the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces.<br>The default setting is 1. |
| **vlan** [*vlan-list*] | (Optional) For trunk ports, you can set the maximum number of secure MAC addresses on a VLAN. If the **vlan** keyword is not entered, the default value is used.<br>• **vlan**—set a per-VLAN maximum value.<br>• **vlan** *vlan-list*—set a per-VLAN maximum value on a range of VLANs separated by a hyphen or a series of VLANs separated by commas. For nonspecified VLANs, the per-VLAN maximum value is used. |

| | |
|---|---|
| **violation** | (Optional) Set the security violation mode or the action to be taken if port security is violated. The default is **shutdown**. |
| **protect** | Set the security violation protect mode. In this mode, when the number of port secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.<br>**Note** We do not recommend configuring the protect mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit. |
| **restrict** | Set the security violation restrict mode. In this mode, when the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. |
| **shutdown** | Set the security violation shutdown mode. In this mode, the interface is error-disabled when a violation occurs and the port LED turns off. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands. |

## Defaults

The default is to disable port security.

When port security is enabled and no keywords are entered, the default maximum number of secure MAC addresses is 1.

The default violation mode is **shutdown**.

Sticky learning is disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If the port is a user network interface (UNI), you must use the **no shutdown** interface configuration command to enable it before using the **switchport port-security** command. UNIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

A secure port has the following limitations:

- A secure port can be an access port or a trunk port; it cannot be a dynamic access port.

- A secure port cannot be a protected port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot be a private-VLAN port.
- A secure port cannot belong to a Fast EtherChannel or Gigabit EtherChannel port group.
- When you enter a maximum secure address value for an interface, if the new value is greater than the previous value, the new value overrides the previously configured value. If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.
- The switch does not support port security aging of sticky secure MAC addresses.

A security violation occurs when the maximum number of secure MAC addresses are in the address table and a station whose MAC address is not in the address table attempts to access the interface or when a station whose MAC address is configured as a secure MAC address on another secure port attempts to access the interface.

If you enable port security on a voice VLAN port and if there is a PC connected to the IP phone, you should set the maximum allowed secure addresses on the port to more than 1.

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

Setting a maximum number of addresses to one and configuring the MAC address of an attached device ensures that the device has the full bandwidth of the port.

When you enter a maximum secure address value for an interface, this occurs:

- If the new value is greater than the previous value, the new value overrides the previously configured value.
- If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.

Sticky secure MAC addresses have these characteristics:

- When you enable sticky learning on an interface by using the **switchport port-security mac-address sticky** interface configuration command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses and adds all sticky secure MAC addresses to the running configuration.
- If you disable sticky learning by using the **no switchport port-security mac-address sticky** interface configuration command or the running configuration is removed, the sticky secure MAC addresses remain part of the running configuration but are removed from the address table. The addresses that were removed can be dynamically reconfigured and added to the address table as dynamic addresses.
- When you configure sticky secure MAC addresses by using the **switchport port-security mac-address sticky** *mac-address* interface configuration command, these addresses are added to the address table and the running configuration. If port security is disabled, the sticky secure MAC addresses remain in the running configuration.
- If you save the sticky secure MAC addresses in the configuration file, when the switch restarts or the interface shuts down, the interface does not need to relearn these addresses. If you do not save the sticky secure addresses, they are lost. If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.

- If you disable sticky learning and enter the **switchport port-security mac-address sticky** *mac-address* interface configuration command, an error message appears, and the sticky secure MAC address is not added to the running configuration.

## Examples

This example shows how to enable port security on a port and to set the maximum number of secure addresses to 5. The violation mode is the default, and no secure MAC addresses are configured.

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
```

This example shows how to configure a secure MAC address and a VLAN ID on a port.

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 3
```

This example shows how to enable sticky learning and to enter two sticky secure MAC addresses on a port:

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.000f
```

You can verify your settings by using the **show port-security** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **clear port-security** | Deletes from the MAC address table a specific type of secure address or all the secure addresses on the switch or an interface. |
| **show port-security address** | Displays all the secure addresses configured on the switch. |
| **show port-security interface** *interface-id* | Displays port security configuration for the switch or for the specified interface. |

# switchport port-security aging

Use the **switchport port-security aging** interface configuration command to set the aging time and type for secure address entries or to change the aging behavior for secure addresses on a particular port. Use the **no** form of this command to disable port security aging or to set the parameters to their default states.

**switchport port-security aging** {**static** | **time** *time* | **type** {**absolute** | **inactivity**}}

**no switchport port-security aging** {**static** | **time** | **type**}

## Syntax Description

| | |
|---|---|
| **static** | Enable aging for statically configured secure addresses on this port. |
| **time** *time* | Specify the aging time for this port. The range is 0 to 1440 minutes. If the time is 0, aging is disabled for this port. |
| **type** | Set the aging type. |
| **absolute** | Set absolute aging type. All the secure addresses on this port age out exactly after the time *(*minutes) specified and are removed from the secure address list. |
| **inactivity** | Set the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period. |

## Defaults

The port security aging feature is disabled. The default time is 0 minutes.

The default aging type is absolute.

The default static aging behavior is disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

To enable secure address aging for a particular port, set the aging time to a value other than 0 for that port. If the port is a user network interface (UNI), you must use the **no shutdown** interface configuration command to enable it before using the **switchport port-security aging** command. UNIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

To allow limited time access to particular secure addresses, set the aging type as **absolute**. When the aging time lapses, the secure addresses are deleted.

To allow continuous access to a limited number of secure addresses, set the aging type as **inactivity**. This removes the secure address when it become inactive, and other addresses can become secure.

To allow unlimited access to a secure address, configure it as a secure address, and disable aging for the statically configured secure address by using the **no switchport port-security aging static** interface configuration command.

## Examples

This example sets the aging time as 2 hours for absolute aging for all the secure addresses on the port.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport port-security aging time 120
```

This example sets the aging time as 2 minutes for inactivity aging type with aging enabled for configured secure addresses on the port.

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

This example shows how to disable aging for configured secure addresses.

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no switchport port-security aging static
```

## Related Commands

| Command | Description |
|---|---|
| **show port-security** | Displays the port security settings defined for the port. |
| **switchport port-security** | Enables port security on a port, restricts the use of the port to a user-defined group of stations, and configures secure MAC addresses. |

# switchport private-vlan

Use the **switchport private-vlan** interface configuration command on the switch to define a private-VLAN association for an isolated or community port or a mapping for a promiscuous port. Use the **no** form of this command to remove the private-VLAN association or mapping from the port.

**switchport private-vlan** {**association** {**host** *primary-vlan-id secondary-vlan-id* | **mapping** *primary-vlan-id* {**add** | **remove**} *secondary-vlan-list*} | **host-association** *primary-vlan-id secondary-vlan-id* | **mapping** *primary-vlan-id* {**add** | **remove**} *secondary-vlan-list*}

**no switchport private-vlan** {**association** {**host** | **mapping**} | **host-association** | **mapping**

**Note** The mapping commands are supported only on network node interfaces (NNIs).

## Syntax Description

| | |
|---|---|
| **association** | Define a private-VLAN association for a port. |
| **host** | Define a private-VLAN association for a community or isolated host port. |
| *primary-vlan-id* | The VLAN ID of the private-VLAN primary VLAN. The range is from 2 to 1001 and 1006 to 4094. |
| *secondary-vlan-id* | The VLAN ID of the private-VLAN secondary (isolated or community) VLAN. The range is from 2 to 1001 and 1006 to 4094. |
| **mapping** | Define private-VLAN mapping for a promiscuous port. Only NNIs can be configured as promiscuous ports. This keyword is not supported on user network interfaces (UNIs). |
| **add** | Associate secondary VLANs to the primary VLAN. |
| **remove** | Clear the association between secondary VLANs and the primary VLAN. |
| *secondary-vlan-list* | One or more secondary (isolated or community) VLANs to be mapped to the primary VLAN. |
| **host-association** | Define a private-VLAN association for a community or isolated host port. |

## Defaults

The default is to have no private-VLAN association or mapping configured.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Private-VLAN association or mapping has no effect on the port unless the port has been configured as a private-VLAN host or promiscuous port by using the **switchport mode private-vlan** {**host** | **promiscuous**} interface configuration command.

A promiscuous port must be an NNI; UNIs cannot be configured as promiscuous ports. To configure a port as a UNI, enter the **port-type uni** interface configuration command. A switch can have a maximum of four NNIs.

If the port is in private-VLAN host or promiscuous mode but the VLANs do not exist, the command is allowed, but the port is made inactive.

The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs. The list can contain one isolated VLAN and multiple community VLANs.

You can map a promiscuous port to only one primary VLAN. If you enter the **switchport private-vlan mapping** command on a promiscuous port that is already mapped to a primary and secondary VLAN, the primary VLAN mapping is overwritten.

You can add or remove secondary VLANs from promiscuous port private-VLAN mappings by using the **add** and **remove** keywords.

Entering the **switchport private-vlan association host** command has the same effect as entering the **switchport private-vlan host-association** interface configuration command.

Entering the **switchport private-vlan association mapping** command has the same effect as entering the **switchport private-vlan mapping** interface configuration command.

## Examples

This example shows how to configure an interface as a private VLAN host port and associate it with primary VLAN 20 and secondary VLAN 501:

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 501
Switch(config-if)# end
```

This example shows how to configure an NNI as a private-VLAN promiscuous port and map it to a private VLAN. The interface is a member of primary VLAN 20 and secondary VLANs 501 to 503 are mapped to it.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 add 501-503
Switch(config-if)# end
```

You can verify private-VLAN mapping by using the **show interfaces private-vlan mapping** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show interfaces private-vlan mapping** | Displays private VLAN mapping information for **VLAN SVIs**.? |
| **show vlan private-vlan** | Displays all private VLAN relationships or types configured on the switch. |

# switchport protected

Use the **switchport protected** interface configuration command to isolate unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch. Use the **no** form of this command to disable protection on the port.

**switchport protected**

**no switchport protected**

**Note** Protected ports are supported only on network node interfaces (NNIs).

## Syntax Description

This command has no arguments or keywords.

## Defaults

No protected port is defined. All ports are nonprotected.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The switchport protection feature is local to the switch; communication between protected ports on the same switch is possible only through a Layer 3 device. To prevent communication between protected ports on different switches, you must configure the protected ports for unique VLANs on each switch and configure a trunk link between the switches. A protected port is different from a secure port.

A protected port does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port. Data traffic cannot be forwarded between protected ports at Layer 2; only control traffic, such as PIM packets, is forwarded because these packets are processed by the CPU and forwarded in software. All data traffic passing between protected ports must be forwarded through a Layer 3 device.

Port monitoring does not work if both the monitor and monitored ports are protected ports.

## Examples

This example shows how to enable a protected port on an interface:

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

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

## Related Commands

| Command | Description |
|---|---|
| **show interfaces switchport** | Displays the administrative and operational status of a switching port, including port blocking and port protection settings. |
| **switchport block** | Prevents unknown multicast or unicast traffic on the interface. |

# 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*}

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

## Syntax Description

| | |
|---|---|
| **allowed vlan** *vlan-list* | 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 *vlan-list* format. The **none** keyword is not valid. The default is **all**. |
| **native vlan** *vlan-id* | Set the native VLAN for sending and receiving untagged traffic when the interface is in 802.1Q trunking mode. The range is 1 to 4094. |

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

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

  Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- **remove** removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 1 to 4094; extended-range VLAN IDs are valid.

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

## Defaults

VLAN 1 is the default native VLAN ID on the port.

The default for all VLAN lists is to include all VLANs.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | 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.

## 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
```

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

## Related Commands

| Command | Description |
|---|---|
| **show interfaces switchport** | Displays the administrative and operational status of a switching port, including port blocking and port protection settings. |
| **switchport mode** | 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 which 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*

## Syntax Description

| | |
|---|---|
| *value* | Specify the difference between the yellow and red threshold values (in Celsius). The range is 10 to 25. The default value is 10. |

## Defaults

The default value is 10.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You cannot configure the green and red thresholds but can configure the yellow threshold. Use the **system env temperature threshold yellow** *value* 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 **system env temperature threshold yellow 15** command.

**Note** The internal temperature sensor in the switch measures the internal system temperature and might vary ±5 degrees C.

## Examples

This example sets 15 as the difference between the yellow and red thresholds:

```
Switch(config)# system env temperature threshold yellow 15
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show env temperature status** | 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 ports or for Fast Ethernet (10/100) 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**

## Syntax Description

| | |
|---|---|
| *bytes* | Set the system MTU for ports that are set to 10 or 100 Mbps. The range is 1500 to 1546 bytes. |
| **jumbo** *bytes* | Set the system jumbo frame size (MTU) for Gigabit Ethernet ports. The range is 1500 to 9000 bytes. |

## Defaults

The default MTU size for all ports is 1500 bytes.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

When you use this command to change the MTU size, you must reset the switch before the new configuration takes effect.

Gigabit Ethernet ports are not affected by the **system mtu** command, and Fast Ethernet ports are not affected by the **system mtu jumbo** command.

If you enter a value that is outside the range for the specific type of switch, the value is not accepted.

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

The size of frames that can be received by the switch CPU is limited to 1546 bytes, no matter what value was entered with the **system mtu** command. Although frames that are forwarded or routed typically are not received by the CPU, in some cases packets are sent to the CPU, such as traffic sent to control traffic, SNMP, Telnet, or routing protocols.

## Examples

This example shows how to set the maximum packet size for Gigabit Ethernet ports to 1800 bytes:

```
Switch(config)# system mtu jumbo 1800
Switch(config)# exit
Switch# reload
```

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

## Related Commands

| Command | Description |
|---|---|
| show system mtu | Displays the packet size set for Fast Ethernet and Gigabit Ethernet ports. |

# table-map

Use the **table-map** global configuration command to create a quality of service (QoS) mapping and to enter table-map configuration mode. Table maps can be specified in policy-map class **set** commands or as mark down mappings for policers and are used to create and configure a mapping table for converting one packet-marking value to another. Use the **no** form of this command to delete the mapping table.

**table-map** *table-map-name*

**no table-map** *table-map-name*

## Syntax Description

| | |
|---|---|
| *class-map-name* | Name of the table map. |

## Defaults

No table maps are defined.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Use this command to specify the name of the table map that you want to create or to modify and to enter table-map configuration mode.

You use the **table-map** command to create a mapping table, which is a type of conversion chart used for establishing a *to-from* relationship between packet-marking types or categories. For example, you can use a mapping table to establish a to-from relationship among these categories:

- class of service (CoS)
- precedence
- Differentiated Services Code Point (DSCP)

The switch supports a maximum of 256 unique table maps.

The maximum number of map statements within a table map is 64.

After you are in table-map configuration mode, these configuration commands are available:

- **default**: the default behavior for setting a value not found in the table map. The default can be specified as one of these:
  - *default value*—uses the table map default value. The range is from 0 to 63.
  - **copy**—sets the default behavior for a value not found in the table map to copy.
  - **ignore**—sets the default behavior for a value not found in the table map to ignore.
- **exit**: exits from QoS table-map configuration mode.
- **map**: the table map **from** *from_value and* **to** *to_value*. Both value ranges are from 0 to 63.
- **no**: deletes the table map or sets the default values.

You can specify table maps in **set** commands and use them as mark-down mapping for the policers in input policy maps.

You cannot use table maps in output policy maps.

## Examples

This example shows how to create a table map to map DSCP to CoS values, setting those DSCP values that are not mapped to a CoS value of 4:

```
Switch(config)# table-map dscp-to-cos
Switch(config-tablemap)# map from 1 to 1
Switch(config-tablemap)# map from 2 to 1
Switch(config-tablemap)# map from 3 to 1
Switch(config-tablemap)# map from 4 to 2
Switch(config-tablemap)# map from 5 to 2
Switch(config-tablemap)# map from 6 to 3
Switch(config-tablemap)# default 4
Switch(config-tablemap)# exit
```

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

## Related Commands

| Command | Description |
|---|---|
| **class** | Defines a traffic classification match criteria for the specified class-map name. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |
| **set cos** | Classifies IP traffic by setting a CoS, DSCP, IP-precedence, or QoS group value in the packet. |
| **show table-map** | Displays QoS table maps. |

# test cable-diagnostics tdr

Use the **test cable-diagnostics tdr** privileged EXEC command to run the Time Domain Reflector (TDR) feature on an interface.

**test cable-diagnostics tdr interface** *interface-id*

**Note** TDR is supported only on the copper Ethernet 10/100 ports on the Cisco ME switch.

## Syntax Description

| | |
|---|---|
| *interface-id* | Specify the interface on which to run TDR. |

## Defaults

There is no default.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

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

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

## Examples

This example shows how to run TDR on an interface:

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

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

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

## Related Commands

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

# traceroute mac

Use the **traceroute 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.

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

**Note** Layer 2 traceroute is available only on network node interfaces (NNIs).

## 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(25)EX | 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.

**Note** CDP and Layer 2 traceroute are available only on NNIs.

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

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

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

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

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

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

This feature is not supported in Token Ring VLANs.

## Examples

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## Related Commands

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

# traceroute mac ip

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**]

**Note** Layer 2 traceroute is available only on network node interfaces (NNIs).

## Syntax Description

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

## Defaults

There is no default.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | 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.

**Note** CDP and Layer 2 traceroute are available only on network node interfaces (NNIs).

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

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

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

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

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

This feature is not supported in Token Ring VLANs.

## Examples

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

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

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

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

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

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

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

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

## Related Commands

| Command | Description |
|---|---|
| traceroute mac | 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

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

## Defaults

UDLD is disabled on all interfaces.

The message timer is set at 60 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | 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 |
|---|---|
| **show udld** | Displays UDLD administrative and operational status for all ports or the specified port. |
| **udld port** | Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command. |
| **udld reset** | Resets all interfaces shut down by UDLD and permits traffic to again pass through. |

# udld port

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**]

## Syntax Description

| | |
|---|---|
| **aggressive** | Enable UDLD in aggressive mode on the specified interface. |

## Defaults

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

On nonfiber-optic interfaces, UDLD is disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

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

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

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

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

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

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

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

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

## 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 |
|---|---|
| **show running-config** | Displays the running configuration on the switch. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**. |
| **show udld** | Displays UDLD administrative and operational status for all ports or the specified port. |
| **udld** | Enables aggressive or normal mode in UDLD or sets the configurable message timer time. |
| **udld reset** | Resets all interfaces shut down by UDLD and permits traffic to again pass through. |

# udld reset

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 and Port Aggregation Protocol (PAgP) still have their normal effects, if enabled).

**udld reset**

**Note** PAgP is available only on network node interfaces (NNIs).

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

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

## Examples

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.

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the running configuration on the switch. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**. |
| **show udld** | Displays UDLD administrative and operational status for all ports or the specified port. |
| **udld** | Enables aggressive or normal mode in UDLD or sets the configurable message timer time. |
| **udld port** | Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command. |

# uni-vlan

Use the **uni-vlan** VLAN configuration command to configure the VLAN as a user node interface (UNI) community or isolated VLAN. UNIs on a switch that are assigned to a community VLAN can exchange packets with one another; UNIs in an isolated VLAN cannot exchange packets. Use the **no** form of this command to return the VLAN to the default UNI isolated VLAN.

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

**no uni-vlan**

## Syntax Description

| | |
|---|---|
| **community** | Designate the UNI VLAN as a community VLAN. |
| **isolated** | Designate the UNI VLAN as an isolated VLAN. |

## Defaults

The default VLAN configuration is UNI isolated VLAN.

## Command Modes

VLAN configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

In a UNI isolated VLAN, packets are not exchanged between UNIs within the VLAN. Packets can be exchanged between UNIs and network node interfaces (NNIs) in the same UNI isolated VLAN.

In a UNI community VLAN, packets can be exchanged between UNIs or between UNIs and NNIs in the same community VLAN. However, there can be no more than eight UNIs in a UNI community VLAN.

VLAN 1 is always a UNI isolated VLAN; you cannot configure VLAN 1 as a UNI community VLAN. The reserved VLANs, 1002 to 1005, are not Ethernet VLANs.

As with any other VLAN, you can statically assign ports to UNI VLANs by using the **switchport access vlan** *vlan-id* interface configuration command. Ports are also dynamically assigned to UNI VLANs.

The **uni-vlan** command does not take effect until you exit from VLAN configuration mode.

A UNI VLAN cannot be a Remote Switched Port Analyzer (RSPAN) VLAN.

A UNI VLAN cannot be a private VLAN.

To change a UNI isolated VLAN to an RSPAN VLAN or a private VLAN, enter the **rspan-vlan** or **private-vlan** VLAN configuration command. This overwrites the default isolated VLAN configuration. To change a UNI community VLAN to an RSPAN VLAN or a private VLAN, you must first enter the **no uni-vlan** VLAN configuration command to return to the default UNI isolated VLAN configuration before entering the **rspan-vlan** or **private-vlan** VLAN configuration command.

**Note** For more information about UNI-VLANs and interaction with other features, see the software configuration guide for this release.

## Examples

This example show s how to change VLAN 20 from the default UNI isolated VLAN to a UNI community VLAN:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# uni-vlan community
Switch(config-vlan)# exit
```

You can verify your setting by entering the **show vlan uni-vlan** or **show vlan** *vlan-id* **uni-vlan [type]** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show interfaces status** | Displays the status of interfaces, including the VLANs to which they belong. |
| **show vlan uni-vlan** | Displays the UNI VLANs on the switch. |

# vlan

Use the **vlan** global configuration command with a VLAN ID to add a VLAN and to enter VLAN configuration 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 as well as in the switch running configuration file. Configuration information for extended-range VLANs (VLAN IDs greater than 1005), are saved only in the switch running configuration file. You can save configurations in the switch startup configuration file by entering the **copy running-config startup-config** privileged EXEC command.

**vlan** *vlan-id*

**no vlan** *vlan-id*

## Syntax Description

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

## Defaults

This command has no default settings.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

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

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

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

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

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

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

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

- **ste** *ste-number*: defines the maximum number of spanning-tree explorer (STE) hops for TrCRF VLANs. The range is 0 to 13. The default is 7.
- **stp type**: defines the spanning-tree type for FDDI-NET, Token Ring-NET, or TrBRF VLANs.
  - **ieee** for IEEE Ethernet STP running source-route transparent (SRT) bridging.
  - **ibm** for IBM STP running source-route bridging (SRB).
  - **auto** for STP running a combination of source-route transparent bridging (IEEE) and source-route bridging (IBM).
- **tb-vlan1** *tb-vlan1-id* and **tb-vlan2** *tb-vlan2-id*: specifies the first and second VLAN to which this VLAN is translationally bridged. Translational VLANs translate FDDI or Token Ring to Ethernet, for example. The range is 0 to 1005. If no value is specified, 0 (no transitional bridging) is assumed.
- **uni-vlan** {**community** | **isolated**}: configures the VLAN as a user node interface (UNI) community or UNI isolated VLAN. UNIs on a switch that are assigned to a community VLAN can communicate with each other. If the UNI VLAN is isolated (the default), ports in the VLAN cannot communicate. See the **uni-vlan** command for more information.

## Examples

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

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

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

This example shows how to create a new extended-range VLAN, to enter VLAN configuration mode and configure the VLAN as a UNI community VLAN, and to save the new VLAN in the switch startup configuration file:

```
Switch(config)# vlan 2000
Switch(config-vlan)# uni-vlan community
Switch(config-vlan)# exit
Switch(config)# exit
Switch# copy running-config startup config
```

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

## Related Commands

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

# vlan access-map

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

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

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

## Syntax Description

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

## Defaults

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

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

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

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

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

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

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

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

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

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

## Examples

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

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

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

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

## Related Commands

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

# vlan filter

Use the **vlan filter** global configuration command to apply a VLAN map to one or more VLANs. Use the **no** form of this command to remove the map.

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

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

## Syntax Description

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

## Defaults

There are no VLAN filters.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

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

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

## Examples

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

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

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

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

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

## Related Commands

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

# vmps reconfirm (privileged EXEC)

Use the **vmps reconfirm** privileged EXEC command to immediately send VLAN Query Protocol (VQP) queries to reconfirm all dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS).

**vmps reconfirm**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default is defined.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Examples

This example shows how to immediately send VQP queries to the VMPS:

```
Switch# vmps reconfirm
```

You can verify your setting by entering the **show vmps** privileged EXEC command and examining the VMPS Action row of the Reconfirmation Status section. The **show vmps** command shows the result of the last time the assignments were reconfirmed either because the reconfirmation timer expired or because the **vmps reconfirm** command was entered.

## Related Commands

| Command | Description |
|---|---|
| **show vmps** | Displays VQP and VMPS information. |
| **vmps reconfirm (global configuration)** | Changes the reconfirmation interval for the VQP client. |

# vmps reconfirm (global configuration)

Use the **vmps reconfirm** global configuration command to change the reconfirmation interval for the VLAN Query Protocol (VQP) client. Use the **no** form of this command to return to the default setting.

**vmps reconfirm** *interval*

**no vmps reconfirm**

## Syntax Description

| | |
|---|---|
| *interval* | Reconfirmation interval for VQP client queries to the VLAN Membership Policy Server (VMPS) to reconfirm dynamic VLAN assignments. The range is 1 to 120 minutes. |

## Defaults

The default reconfirmation interval is 60 minutes.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Examples

This example shows how to set the VQP client to reconfirm dynamic VLAN entries every 20 minutes:

```
Switch(config)# vmps reconfirm 20
```

You can verify your setting by entering the **show vmps** privileged EXEC command and examining information in the Reconfirm Interval row.

## Related Commands

| Command | Description |
|---|---|
| **show vmps** | Displays VQP and VMPS information. |
| **vmps reconfirm (privileged EXEC)** | Sends VQP queries to reconfirm all dynamic VLAN assignments with the VMPS. |

# vmps retry

Use the **vmps retry** global configuration command to configure the per-server retry count for the VLAN Query Protocol (VQP) client. Use the **no** form of this command to return to the default setting.

**vmps retry** *count*

**no vmps retry**

## Syntax Description

| | |
|---|---|
| *count* | Number of attempts to contact the VLAN Membership Policy Server (VMPS) by the client before querying the next server in the list. The range is 1 to 10. |

## Defaults

The default retry count is 3.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Examples

This example shows how to set the retry count to 7:

```
Switch(config)# vmps retry 7
```

You can verify your setting by entering the **show vmps** privileged EXEC command and examining information in the Server Retry Count row.

## Related Commands

| Command | Description |
|---|---|
| **show vmps** | Displays VQP and VMPS information. |

# vmps server

Use the **vmps server** global configuration command to configure the primary VLAN Membership Policy Server (VMPS) and up to three secondary servers. Use the **no** form of this command to remove a VMPS server.

**vmps server** *ipaddress* [**primary**]

**no vmps server** [*ipaddress*]

## Syntax Description

| | |
|---|---|
| *ipaddress* | IP address or hostname of the primary or secondary VMPS servers. If you specify a hostname, the Domain Name System (DNS) server must be configured. |
| **primary** | (Optional) Decides whether primary or secondary VMPS servers are being configured. |

## Defaults

No primary or secondary VMPS servers are defined.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The first server entered is automatically selected as the primary server whether or not **primary** is entered. The first server address can be overridden by using **primary** in a subsequent command.

When using the **no** form without specifying the *ipaddress*, all configured servers are deleted. If you delete all servers when dynamic-access ports are present, the switch cannot forward packets from new sources on these ports because it cannot query the VMPS.

## Examples

This example shows how to configure the server that has IP address 191.10.49.20 as the primary VMPS server. The servers with IP addresses 191.10.49.21 and 191.10.49.22 are configured as secondary servers:

```
Switch(config)# vmps server 191.10.49.20 primary
Switch(config)# vmps server 191.10.49.21
Switch(config)# vmps server 191.10.49.22
```

This example shows how to delete the server with IP address 191.10.49.21:

```
Switch(config)# no vmps server 191.10.49.21
```

You can verify your setting by entering the **show vmps** privileged EXEC command and examining information in the VMPS Domain Server row.

**Related Commands**

| Command | Description |
|---|---|
| **show vmps** | Displays VQP and VMPS information. |