snmp ifindex clear

To clear any previously configured **snmp ifindex** commands that were entered for a specific interface, use the **snmp ifindex clear** command.

snmp ifindex clear

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switches.

Usage Guidelines

Interface index persistence occurs when ifIndex values in the interface MIB (IF-MIB) persist across reboots and allow for consistent identification of specific interfaces using SNMP.

Use the **snmp ifindex clear** command on a specific interface when you want that interface to use the global configuration setting for ifIndex persistence. This command clears any ifIndex configuration commands previously entered for that specific interface.

Examples

This example shows how to enable ifIndex persistence for all interfaces:

```
Router(config)# snmp-server ifindex persist
```

This example shows how to disable IfIndex persistence for FastEthernet 1/1 only:

```
Router(config)# interface fastethernet 1/1
Router(config-if)# no snmp ifindex persist
Router(config-if)# exit
```

This example shows how to clear the ifIndex configuration from the FastEthernet 1/1 configuration:

```
Router(config)# interface fastethernet 1/1
Router(config-if)# snmp ifindex clear
Router(config-if)# exit
```

As a result of this sequence of commands, ifIndex persistence is enabled for all interfaces that are specified by the **snmp-server ifindex persist** global configuration command.

Related Commands

snmp ifindex persist
snmp-server ifindex persist

snmp ifindex persist

To enable ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) on a specific interface, use the **snmp ifindex persist** command. To disable ifIndex persistence only on a specific interface, use the **no** form of this command.

snmp ifindex persist

no snmp ifindex persist

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switches.

Usage Guidelines

Interface index persistence occurs when ifIndex values in the IF-MIB persist across reboots and allow for consistent identification of specific interfaces using SNMP.

The **snmp ifindex persist** interface configuration command enables and disables ifIndex persistence for individual entries (that correspond to individual interfaces) in the ifIndex table of the IF-MIB.

The **snmp-server ifindex persist** global configuration command enables and disables ifIndex persistence for all interfaces on the routing device. This action applies only to interfaces that have ifDescr and ifIndex entries in the ifIndex table of the IF-MIB.

Examples

This example shows how to enable ifIndex persistence for interface FastEthernet 1/1 only:

```
Router(config)# interface fastethernet 1/1
Router(config-if)# snmp ifindex persist
Router(config-if)# exit
```

This example shows how to enable ifIndex persistence for all interfaces, and then disable ifIndex persistence for interface FastEthernet 1/1 only:

```
Router(config)# snmp-server ifindex persist
Router(config)# interface fastethernet 1/1
Router(config-if)# no snmp ifindex persist
Router(config-if)# exit
```

Related Commands

snmp ifindex clear
snmp-server ifindex persist

snmp-server enable traps

To enable SNMP notifications (traps or informs), use the **snmp-server enable traps** command. To disable all SNMP notifications, use the **no** form of this command.

snmp-server enable traps [**flash** [**insertion** | **removal**] | **fru-ctrl** | **port-security** [**trap-rate** *trap-rate*] | **removal** | **stpx** | **vlancreate** | **vlandelete** | **vtp**] [**mac-notification** [**change** | **move** | **threshold**]

no snmp-server enable traps [**flash** [**insertion** | **removal**] | **fru-ctrl** | **port-security** [**trap-rate** *trap-rate*] | **removal** | **stpx** | **vlancreate** | **vlandelete** | **vtp**] [**mac-notification**]

Syntax Description

flash	(Optional) Controls the SNMP FLASH trap notifications.
insertion	(Optional) Controls the SNMP Flash insertion trap notifications.
removal	(Optional) Controls the SNMP Flash removal trap notifications.
fru-ctrl	(Optional) Controls the SNMP entity FRU control trap notifications.
port-security	(Optional) Controls the SNMP trap generation.
trap-rate *trap-rate*	(Optional) Sets the number of traps per second.
stpx	(Optional) Controls all the traps defined in CISCO-STP-EXTENSIONS-MIB notifications.
vlancreate	(Optional) Controls the SNMP VLAN created trap notifications.
vlandelete	(Optional) Controls the SNMP VLAN deleted trap notifications.
vtp	(Optional) Controls the SNMP VTP trap notifications.
mac-notification	(Optional) Controls the SNMP MAC trap notifications.
change	(Optional) Controls the SNMP MAC change trap notifications
move	(Optional) Controls the SNMP MAC move trap notifications
threshold	(Optional) Controls the SNMP MAC threshold trap notifications

Defaults

SNMP notifications are disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(31)SG	Support for MAC notification was added.

Usage Guidelines

If you enter this command without an option, all notification types controlled by this command are enabled.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. To specify whether the notifications should be sent as traps or informs, use the **snmp-server host** [**traps** | **informs**] command.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send notifications, you must configure at least one **snmp-server host** command.

This list of the MIBs is used for the traps:

- **flash—**Controls SNMP FLASH traps from the CISCO-FLASH-MIB.
  - **insertion**—Controls the SNMP Flash insertion trap notifications.
  - **removal**—Controls the SNMP Flash removal trap notifications.
- **fru-ctrl—**Controls the FRU control traps from the CISCO-ENTITY-FRU-CONTROL-MIB.
- **port-security—**Controls the port-security traps from the CISCO-PORT-SECURITY-MIB.
- **stpx—**Controls all the traps from the CISCO-STP-EXTENSIONS-MIB.
- **vlancreate—**Controls SNMP VLAN created trap notifications.
- **vlandelete—**Controls SNMP VLAN deleted trap notifications.
- **vtp—**Controls the VTP traps from the CISCO-VTP-MIB.

Examples

This example shows how to send all traps to the host is specified by the name myhost.cisco.com using the community string defined as public:

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

This example shows how to enable the MAC address change MIB notification:

```
Switch(config)# snmp-server enable traps mac-notification change
Switch(config)#
```

SNMP traps can be enabled with a rate-limit to detect port-security violations due to restrict mode. The following example shows how to enable traps for port-security with a rate of 5 traps per second:

```
Switch(config)# snmp-server enable traps port-security trap-rate 5
Switch(config)#
```

Related Commands

clear mac-address-table
mac-address-table notification
show mac-address-table notification
snmp-server enable traps
snmp trap mac-notification change

Refer to Cisco IOS documentation for additional **snmp-server enable traps** commands.

snmp-server ifindex persist

To globally enable ifIndex values that will remain constant across reboots for use by SNMP, use the **snmp-server ifindex persist** command. To globally disable inIndex persistence, use the **no** form of this command.

snmp-server ifindex persist

no snmp-server ifindex persist

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switches.

Usage Guidelines

Interface index persistence occurs when ifIndex values in the IF-MIB persist across reboots and allow for consistent identification of specific interfaces using SNMP.

The **snmp-server ifindex persist** global configuration command does not override the interface-specific configuration. To override the interface-specific configuration of ifIndex persistence, enter the **no snmp ifindex persist** and **snmp ifindex clear** interface configuration commands.

Entering the **no snmp-server ifindex persist** global configuration command enables and disables ifIndex persistence for all interfaces on the routing device using ifDescr and ifIndex entries in the ifIndex table of the IF-MIB.

Examples

This example shows how to enable ifIndex persistence for all interfaces:

```
Router(config)# snmp-server ifindex persist
```

Related Commands

snmp ifindex clear
snmp ifindex persist

snmp-server ifindex persist compress

To configure the format of the ifIndex table in a compressed format, use the **snmp-server ifindex persist compress** command. To place the table in a decompressed format, use the **no** form of this command.

snmp-server ifindex persist compress

no snmp-server ifindex persist compress

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration mode.

Command History

Release	Modification
12.2(40)SG	Support for this command was introduced on the Catalyst 4500 series switches.

Usage Guidelines

This command is hidden on Supervisor Engine V and later supervisor engines because the ifIndex table is always in a compressed format on those supervisor engines.

At bootup, if the nvram:ifIndex-table.gz file (the ifIndex table ina compressed format) is present on a Supervisor Engine II+, Supervisor Engine III, or Supervisor Engine IV, the **snmp-server ifindex persist compress** command is automatically run even if the startup-config file does not have this configuration.

Examples

This example shows how to enable compression of the ifIndex table:

```
Router(config)# snmp-server ifindex persist compress
```

This example shows how to disable compression of the ifIndex table:

```
Router(config)# no snmp-server ifindex persist compress
```

Related Commands

snmp ifindex clear
snmp ifindex persist
snmp-server ifindex persist

snmp trap mac-notification change

To enable SNMP MAC address notifications, use the **snmp trap mac-notification** command. To return to the default setting, use the **no** form of this command.

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

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

Syntax Description

added	Specifies enabling the MAC address notification trap whenever a MAC address is added to an interface.
removed	Specifies enabling the MAC address notification trap whenever a MAC address is removed from an interface.

Defaults

MAC address addition and removal are disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch

Usage Guidelines

Even though you enable the change notification trap for a specific interface by using the **snmp trap mac-notification change** command, the trap is generated only when you enable the **snmp-server enable traps mac-notification change** and the **mac address-table notification change** 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 gigabitethernet1/1
Switch(config-if)# snmp trap mac-notification change added
```

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

Related Commands

clear mac-address-table
mac-address-table notification
show mac-address-table notification
snmp-server enable traps

Refer to Cisco IOS documentation for additional **snmp-server enable traps** commands.

spanning-tree backbonefast

To enable BackboneFast on a spanning-tree VLAN, use the **spanning-tree backbonefast** command. To disable BackboneFast, use the **no** form of this command.

spanning-tree backbonefast

no spanning-tree backbonefast

Syntax Description

This command has no arguments or keywords.

Defaults

BackboneFast is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

BackboneFast should be enabled on all Catalyst 4506 series switches to allow the detection of indirect link failures. Enabling BackboneFast starts the spanning-tree reconfiguration more quickly.

Examples

This example shows how to enable BackboneFast on all VLANs:

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

Related Commands

spanning-tree cost
spanning-tree port-priority
spanning-tree portfast default
spanning-tree portfast (interface configuration mode)
spanning-tree uplinkfast
spanning-tree vlan
show spanning-tree

spanning-tree bpdufilter

To enable BPDU filtering on an interface, use the **spanning-tree bpdufilter** command. To return to the default settings, use the **no** form of this command.

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

no spanning-tree bpdufilter

Syntax Description

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

Defaults

Disabled

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Caution Use care when entering the **spanning-tree bpdufilter enable** command. Enabling BPDU filtering on an interface is approximately equivalent to disabling the spanning tree for this interface. It is possible to create bridging loops if this command is not correctly used.

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

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

- **spanning-tree bpdufilter enable**—This state unconditionally enables the BPDU filter feature on the interface.
- **spanning-tree bpdufilter disable**—This state unconditionally disables the BPDU filter feature on the interface.
- **no spanning-tree bpdufilter**—This state enables the BPDU filter feature on the interface if the interface is in operational PortFast state and if the **spanning-tree portfast bpdufilter default** command is configured.

Examples

This example shows how to enable the BPDU filter feature on this interface:

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

Related Commands

show spanning-tree
spanning-tree portfast bpdufilter default

spanning-tree bpduguard

To enable BPDU guard on an interface, use the **spanning-tree bpduguard** command. To return to the default settings, use the **no** form of this command.

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

no spanning-tree bpduguard

Syntax Description

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

Defaults

BPDU guard is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

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

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

Examples

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

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

Related Commands

show spanning-tree
spanning-tree portfast bpduguard default

spanning-tree cost

To calculate the path cost of STP on an interface, use the **spanning-tree cost** command. To revert to the default, use the **no** form of this command.

spanning-tree cost *cost*

no spanning-tree cost *cost*

Syntax Description

cost	Path cost; valid values are from 1 to 200,000,000.

Defaults

The default settings are as follows:

- FastEthernet—19
- GigabitEthernet—1

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

When you configure the cost, the higher values indicate higher costs. The range applies regardless of the protocol type that is specified. The path cost is calculated, based on the interface bandwidth.

Examples

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

```
Switch(config)# interface fastethernet 2/1
Switch(config-if)# spanning-tree cost 250
Switch(config-if)#
```

Related Commands

spanning-tree port-priority
spanning-tree portfast default
spanning-tree portfast (interface configuration mode)
spanning-tree uplinkfast
spanning-tree vlan
show spanning-tree

spanning-tree etherchannel guard misconfig

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

spanning-tree etherchannel guard misconfig

no spanning-tree etherchannel guard misconfig

Syntax Description

This command has no arguments or keywords.

Defaults

Spanning-tree EtherChannel guard is enabled.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

When an EtherChannel guard misconfiguration is detected, this message is displayed:

```
%SPANTREE-2-CHNL_MISCFG:Detected loop due to etherchannel misconfig of interface
Port-Channel1
```

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

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

Examples

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

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

Related Commands

show etherchannel
show interfaces status
shutdown (refer to Cisco IOS documentation)

spanning-tree extend system-id

To enable the extended system ID feature on a chassis that supports 1024 MAC addresses, use the **spanning-tree extend system-id** command. To disable the feature, use the **no** form of this command.

spanning-tree extend system-id

no spanning-tree extend system-id

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled on systems that do not provide 1024 MAC addresses.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Releases 12.1(13)E and later support chassis with 64 or 1024 MAC addresses. For chassis with 64 MAC addresses, STP uses the extended system ID plus a MAC address to make the bridge ID unique for each VLAN.

You cannot disable the extended system ID on chassis that support 64 MAC addresses.

Enabling or disabling the extended system ID updates the bridge IDs of all active STP instances, which might change the spanning-tree topology.

Examples

This example shows how to enable the extended system ID:

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

Related Commands

show spanning-tree

spanning-tree guard

To enable root guard, use the **spanning-tree guard** command. To disable root guard, use the **no** form of this command.

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

no spanning-tree guard

Syntax Description

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

Defaults

Root guard is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Loop guard support was added.

Examples

This example shows how to enable root guard:

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

Related Commands

show spanning-tree

spanning-tree link-type

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

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

no spanning-tree link-type

Syntax Description

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

Defaults

Link type is derived from the duplex mode.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

RSTP+ fast transition works only on point-to-point links between two bridges.

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

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

Examples

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

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

Related Commands

show spanning-tree interface

spanning-tree loopguard default

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

spanning-tree loopguard default

no spanning-tree loopguard default

Syntax Description

This command has no keywords or arguments.

Defaults

Loop guard is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Loop guard provides an additional security in the bridge network. Loop guard prevents alternate or root ports from becoming the designated port because of a failure leading to a unidirectional link.

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

Individual loop-guard port configuration overrides this global default.

Examples

This example shows how to enable loop guard:

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

Related Commands

show spanning-tree
spanning-tree guard

spanning-tree mode

To switch between PVST+ and MST modes, use the **spanning-tree mode** command. To return to the default settings, use the **no** form of this command.

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

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

Syntax Description

pvst	Specifies PVST+ mode.
mst	Specifies MST mode.
rapid-pvst	Specifies Rapid PVST mode.

Defaults

PVST+ mode

Command Modes

Configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(19)EW	Support for the **rapid-pvst** keyword.

Usage Guidelines

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

Examples

This example shows how to switch to MST mode:

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

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

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

Related Commands

show spanning-tree mst

spanning-tree mst

To set the path cost and port-priority parameters for any MST instance (including the CIST with instance ID 0), use the **spanning-tree mst** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst *instance-id* [**cost** *cost*] | [**port-priority** *prio*]

no spanning-tree mst *instance-id* {**cost** | **port-priority**}

Syntax Description

instance-id	Instance ID number; valid values are from 0 to 15.
cost *cost*	(Optional) Specifies the path cost for an instance; valid values are from 1 to 200000000.
port-priority *prio*	(Optional) Specifies the port priority for an instance; valid values are from 0 to 240 in increments of 16.

Defaults

Port priority is **128**.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The higher **cost** *cost* values indicate higher costs. When entering the *cost* value, do not include a comma in the entry; for example, enter **1000**, not **1,000**.

The higher **port-priority** *prio* values indicate smaller priorities.

By default, the cost depends on the port speed; faster interface speeds indicate smaller costs. MST always uses long path costs.

Examples

This example shows how to set the interface path cost:

```
Switch(config-if)# spanning-tree mst 0 cost 17031970
Switch(config-if)#
```

This example shows how to set the interface priority:

```
Switch(config-if)# spanning-tree mst 0 port-priority 64
Switch(config-if)#
```

Related Commands

show spanning-tree mst
spanning-tree port-priority

spanning-tree mst configuration

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

spanning-tree mst configuration

no spanning-tree mst configuration

Syntax Description

This command has no arguments or keywords.

Defaults

The default settings are as follows:

- No VLANs are mapped to any MST instance.
- All VLANs are mapped to the CIST instance.
- The region name is an empty string.
- The revision number is 0.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The MST configuration consists of three main parameters:

- Instance VLAN mapping (see the **instance** command)
- Region name (see the **name** command)
- Configuration revision number (see the **revision** command)

By default, the value for the MST configuration is the default value for all its parameters.

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

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

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

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

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

In the unlikely event that two users enter a new configuration at exactly at the same time, this message is displayed:

```
Switch(config-mst)# exit
% MST CFG:Configuration change lost because of concurrent access
Switch(config-mst)#
```

Examples

This example shows how to enter the MST configuration submode:

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

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

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

Related Commands

instance
name
revision
show spanning-tree mst

spanning-tree mst forward-time

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

spanning-tree mst forward-time *seconds*

no spanning-tree mst forward-time

Syntax Description

seconds	Number of seconds to set the forward delay timer for all the instances on the Catalyst 4500 series switch; valid values are from 4 to 30 seconds.

Defaults

The forward delay timer is set for 15 seconds.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

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

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

Related Commands

show spanning-tree mst

spanning-tree mst hello-time

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

spanning-tree mst hello-time *seconds*

no spanning-tree mst hello-time

Syntax Description

seconds	Number of seconds to set the hello-time delay timer for all the instances on the Catalyst 4500 series switch; valid values are from 1 to 10 seconds.

Defaults

The hello-time delay timer is set for 2 seconds.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

If you do not specify the *hello-time* value, the value is calculated from the network diameter.

Examples

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

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

Related Commands

show spanning-tree mst

spanning-tree mst max-age

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

spanning-tree mst max-age *seconds*

no spanning-tree mst max-age

Syntax Description

seconds	Number of seconds to set the max-age timer for all the instances on the Catalyst 4500 series switch; valid values are from 6 to 40 seconds.

Defaults

The max-age timer is set for 20 seconds.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

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

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

Related Commands

show spanning-tree mst

spanning-tree mst max-hops

To specify the number of possible hops in the region before a BPDU is discarded, use the **spanning-tree mst max-hops** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst max-hops *hopnumber*

no spanning-tree mst max-hops

Syntax Description

hopnumber	Number of possible hops in the region before a BPDU is discarded; valid values are from 1 to 40 hops.

Defaults

Number of hops is 20.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to set the number of possible hops in the region before a BPDU is discarded to 25:

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

Related Commands

show spanning-tree mst

spanning-tree mst root

To designate the primary root, secondary root, bridge priority, and timer value for an instance, use the **spanning-tree mst root** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst *instance-id* **root** {**primary** | **secondary**} | {**priority** *prio*} [**diameter** *dia* [**hello-time** *hello*]]

no spanning-tree mst root

Syntax Description

instance-id	Instance identification number; valid values are from 1 to 15.
root	Configures switch as the root switch.
primary	Sets a high enough priority (low value) to make the bridge root of the spanning-tree instance.
secondary	Designates this switch as a secondary root if the primary root fails.
priority *prio*	Sets the bridge priority; see the "Usage Guidelines" section for valid values and additional information.
diameter *dia*	(Optional) Sets the timer values for the bridge based on the network diameter; valid values are from 2 to 7.
hello-time *hello*	(Optional) Specifies the duration between the generation of configuration messages by the root switch.

Defaults

Bridge priority is 32768.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

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

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

The **spanning-tree root secondary** bridge priority value is 16384.

The **diameter** *dia* and **hello-time** *hello* options are available for instance 0 only.

If you do not specify the *hello_time* value, the value is calculated from the network diameter.

Examples

This example shows how to set the priority and timer values for the bridge:

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

Related Commands

show spanning-tree mst

spanning-tree pathcost method

To set the path cost calculation method, use the **spanning-tree pathcost method** command. To revert to the default setting, use the **no** form of this command.

spanning-tree pathcost method {**long** | **short**}

no spanning-tree pathcost method

Syntax Description

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

Defaults

Port path cost has 16-bit-based values.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command applies to all the spanning-tree instances on the switch.

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

The **short** path cost calculation method (16 bits) yields values in the range of 1 through 65,535.

Examples

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

```
Switch(config) spanning-tree pathcost method long
Switch(config)
```

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

```
Switch(config) spanning-tree pathcost method short
Switch(config)
```

Related Commands

show spanning-tree

spanning-tree portfast (interface configuration mode)

To enable PortFast mode, where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire, use the **spanning-tree portfast** command. To return to the default setting, use the **no** form of this command.

spanning-tree portfast {**disable** | **trunk**}

no spanning-tree portfast

Syntax Description

disable	Disables PortFast on the interface.
trunk	Enables PortFast on the interface even while in the trunk mode.

Defaults

PortFast mode is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	The **disable** and **trunk** options were added.

Usage Guidelines

You should use this feature only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt the Catalyst 4500 series switch and network operation.

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

Be careful when using the **no spanning-tree portfast** command. This command does not disable PortFast if the **spanning-tree portfast default** command is enabled.

This command has four states:

- **spanning-tree portfast**—This command enables PortFast unconditionally on the given port.
- **spanning-tree portfast disable**—This command explicitly disables PortFast for the given port. The configuration line shows up in the running-configuration as it is not the default.
- **spanning-tree portfast trunk**—This command allows you to configure PortFast on trunk ports.

Note If you enter the **spanning-tree portfast trunk** command, the port is configured for PortFast even when in the access mode.

- **no spanning-tree portfast**—This command implicitly enables PortFast if the **spanning-tree portfast default** command is defined in global configuration and if the port is not a trunk port. If you do not configure PortFast globally, the **no spanning-tree portfast** command is equivalent to the **spanning-tree portfast disable** command.

Examples

This example shows how to enable PortFast mode:

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

Related Commands

spanning-tree cost
spanning-tree port-priority
spanning-tree portfast default
spanning-tree uplinkfast
spanning-tree vlan
show spanning-tree

spanning-tree portfast bpdufilter default

To enable the BPDU filtering by default on all PortFast ports, use the **spanning-tree portfast bpdufilter default** command. To return to the default settings, use the **no** form of this command.

spanning-tree portfast bpdufilter default

no spanning-tree portfast bpdufilter default

Syntax Description

This command has no keywords or arguments.

Defaults

BPDU filtering is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The **spanning-tree portfast bpdufilter default** command enables BPDU filtering globally on the Catalyst 4500 series switch. BPDU filtering prevents a port from sending or receiving any BPDUs.

You can override the effects of the **spanning-tree portfast bpdufilter default** command by configuring BPDU filtering at the interface level.

Note Be careful when enabling BPDU filtering. Functionality is different when enabling on a per-port basis or globally. When enabled globally, BPDU filtering is applied only on ports that are in an operational PortFast state. Ports still send a few BPDUs at linkup before they effectively filter outbound BPDUs. If a BPDU is received on an edge port, it immediately loses its operational PortFast status and BPDU filtering is disabled.

When enabled locally on a port, BPDU filtering prevents the Catalyst 4500 series switch from receiving or sending BPDUs on this port.

Caution Be careful when using this command. This command can cause bridging loops if not used correctly.

Examples

This example shows how to enable BPDU filtering by default:

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

Related Commands

show spanning-tree mst
spanning-tree bpdufilter

spanning-tree portfast bpduguard default

To enable BPDU guard by default on all the PortFast ports, use the **spanning-tree portfast bpduguard default** command. To return to the default settings, use the **no** form of this command.

spanning-tree portfast bpduguard default

no spanning-tree portfast bpduguard default

Syntax Description

This command has no keywords or arguments.

Defaults

BPDU guard is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Caution Be careful when using this command. You should use this command only with the interfaces that connect to the end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt the Catalyst 4500 series switch and network operation.

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

Examples

This example shows how to enable BPDU guard by default:

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

Related Commands

show spanning-tree mst
spanning-tree bpduguard

spanning-tree portfast default

To globally enable PortFast by default on all access ports, use the **spanning-tree portfast default** command. To disable PortFast as default on all access ports, use the **no** form of this command.

spanning-tree portfast default

no spanning-tree portfast default

Syntax Description

This command has no arguments or keywords.

Defaults

PortFast is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Caution Be careful when using this command. You should use this command only with the interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt the Catalyst 4500 series switch and network operation.

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

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

Examples

This example shows how to globally enable PortFast by default on all access ports:

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

Related Commands

show spanning-tree
spanning-tree portfast (interface configuration mode)

spanning-tree port-priority

To prioritize an interface when two bridges compete for position as the root bridge, use the **spanning-tree port-priority** command. The priority you set breaks the tie. To revert to the default setting, use the **no** form of this command.

spanning-tree port-priority *port_priority*

no spanning-tree port-priority

Syntax Description

port_priority	Port priority; valid values are from 0 to 240 in increments of 16.

Defaults

Port priority value is set to 128.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to increase the possibility that the spanning-tree instance 20 will be chosen as the root-bridge on interface FastEthernet 2/1:

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

Related Commands

spanning-tree cost
spanning-tree portfast default
spanning-tree portfast (interface configuration mode)
spanning-tree uplinkfast
spanning-tree vlan
show spanning-tree

spanning-tree uplinkfast

To enable the UplinkFast feature, use the **spanning-tree uplinkfast** command. To disable UplinkFast, use the **no** form of this command.

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

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

Syntax Description

max-update-rate *packets_per_second*	(Optional) Specifies the maximum rate (in packets per second) at which update packets are sent; valid values are from 0 to 65535.

Defaults

The default settings are as follows:

- Disabled.
- Maximum update rate is 150.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command should be used only on access switches.

When UplinkFast is configured, the bridge priority is changed to 49,152 so that this switch will not be selected as root. All interface path costs of all spanning-tree interfaces belonging to the specified spanning-tree instances are also increased by 3000.

When spanning tree detects that the root interface has failed, the UplinkFast feature causes an immediate switchover to an alternate root interface, transitioning the new root interface directly to the forwarding state. During this time, a topology change notification is sent. To minimize the disruption caused by the topology change, a multicast packet is sent to 01-00-0C-CD-CD-CD for each station address in the forwarding bridge except for those associated with the old root interface.

Use the **spanning-tree uplinkfast max-update-rate** command to enable UplinkFast (if not already enabled) and change the rate at which the update packets are sent. Use the **no** form of this command to return the default rate of 150 packets per second.

Examples

This example shows how to enable UplinkFast and set the maximum rate to 200 packets per second:

```
Switch(config)# spanning-tree uplinkfast
Switch(config)# spanning-tree uplinkfast max-update-rate 200
```

Related Commands

spanning-tree cost
spanning-tree port-priority
spanning-tree portfast default
spanning-tree portfast (interface configuration mode)
spanning-tree vlan

spanning-tree vlan

To configure STP on a per-VLAN basis, use the **spanning-tree vlan** command. To return to the default value, use the **no** form of this command.

spanning-tree vlan *vlan_id* [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds* | **priority** *priority* | **protocol** *protocol* | **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 identification number; valid values are from 1 to 4094.
forward-time *seconds*	(Optional) Sets the STP forward delay time; valid values are from 4 to 30 seconds.
hello-time *seconds*	(Optional) Specifies, in seconds, the time between configuration messages generated by the root switch; valid values are from 1 to 10 seconds.
max-age *seconds*	(Optional) Sets the maximum time, in seconds, that the information in a BPDU is valid; valid values are from 6 to 40 seconds.
priority *priority*	(Optional) Sets the STP bridge priority; valid values are from 0 to 65535.
protocol *protocol*	(Optional) Specifies the protocol.
root primary	(Optional) Forces this switch to be the root bridge.
root secondary	(Optional) Specifies this switch act as the root switch should the primary root fail.
diameter *net-diameter*	(Optional) Specifies the maximum number of bridges between two end stations; valid values are from 2 to 7.

Defaults

The default settings are as follows:

- Forward-time—15 seconds
- Hello-time—2 seconds
- Max-age—20 seconds
- Priority—32768 with STP enabled; 128 with MST enabled
- Root—No STP root

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for extended addressing was added.

Usage Guidelines

When you are setting the **max-age** *seconds* value, if a bridge does not hear BPDUs from the root bridge within the specified interval, it assumes that the network has changed and recomputes the spanning-tree topology.

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

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

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

Examples

This example shows how to enable spanning tree on VLAN 200:

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

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
Switch(config)#
```

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
Switch(config)#
```

Related Commands

spanning-tree cost
spanning-tree port-priority
spanning-tree portfast default
spanning-tree portfast (interface configuration mode)
spanning-tree uplinkfast
show spanning-tree

speed

To configure the interface speed, use the **speed** command. To disable a speed setting, use the **no** form of this command.

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

no speed

Syntax Description

10	(Optional) Configures the interface to transmit at 10 Mbps.
100	(Optional) Configures the interface to transmit at 100 Mbps.
1000	(Optional) Configures the interface to transmit at 1000 Mbps.
auto [**10** | **100** | **1000**]	(Optional) Enables the interface to autonegotiate the speed and specify the exact values to advertise when autonegotiating.
nonegotiate	(Optional) Enables the interface to not negotiate the speed.

Defaults

The default values are shown in the following table:

Interface Type	Supported Syntax	Default Setting
10/100-Mbps module	**speed** [**10** | **100** | **auto** [**10** | **100**]]	Auto
100-Mbps fiber modules	Not applicable	Not applicable
Gigabit Ethernet Interface	**speed nonegotiate**	Nonegotiate
10/100/1000	**speed** [**10** | **100** | **1000** | **auto** [**10** | **100** | **1000**]]	Auto
1000	Not applicable	Not applicable

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(20)EWA	Support for auto negotiating specific speeds added.

Usage Guidelines

Table 2-28 lists the supported command options by interface.

Table 2-28 Supported speed Command Options

Interface Type	Supported Syntax	Default Setting	Guidelines
10/100-Mbps module	**speed** [**10** | **100** | **auto**]	**auto**	If the speed is set to 10 or 100 and you do not configure the duplex setting, the duplex is set to half.
100-Mbps fiber modules	Not applicable.	Not applicable.	Not applicable.
Gigabit Ethernet Interface	**speed nonegotiate**	**nonegotiate** is enabled.	This is only applicable to Gigabit Ethernet ports.
10/100/1000	**speed** [**10** | **100** | **1000** | **auto**]	**auto**	If the speed is set to 10 or 100 and you do not configure the duplex setting, the duplex is set to half. If the speed is set to 1000 or auto with any subset containing 1000 (e.g. **speed auto 10 1000** or **speed auto** on a 10/100/1000 port), you will not able to set half duplex.
1000	Not applicable.	Not applicable.	The speed is always 1000. The duplex is half.

If you configure the interface speed and duplex commands manually and enter a value other than **speed auto** (for example, 10 or 100 Mbps), make sure that you configure the connecting interface speed command to a matching speed but do not use the auto parameter.

When manually configuring the interface speed to either 10 or 100 Mbps, the switch prompts you to also configure duplex mode on the interface.

Note Catalyst 45006 switches cannot automatically negotiate the interface speed and the duplex mode if either connecting interface is configured to a value other than **auto**.

Caution Changing the interface speed and the duplex mode configuration might shut down and reenable the interface during the reconfiguration.

Table 2-29 describes the system's performance for different combinations of the duplex and speed modes. The specified **duplex** command that is configured with the specified **speed** command produces the resulting system action.

Table 2-29 System Action Using duplex and speed Commands

duplex Command	speed Command	Resulting System Action
duplex auto	**speed auto**	Autonegotiates both speed and duplex modes
duplex half	**speed 10**	Forces 10 Mbps and half duplex
duplex full	**speed 10**	Forces 10 Mbps and full duplex
duplex half	**speed 100**	Forces 100 Mbps and half duplex
duplex full	**speed 100**	Forces 100 Mbps and full duplex
duplex full	**speed 1000**	Forces 1000 Mbps and full duplex

Examples

This example shows how to set the interface speed to 100 Mbps on the Fast Ethernet interface 5/4:

```
Switch(config)# interface fastethernet 5/4
Switch(config-if)# speed 100
```

This example shows how to allow Fast Ethernet interface 5/4 to autonegotiate the speed and duplex mode:

```
Switch(config)# interface fastethernet 5/4
Switch(config-if)# speed auto
```

Note The **speed auto 10 100** command is similar to the **speed auto** command on a Fast Ethernet interface.

This example shows how to limit the interface speed to 10 and 100 Mbps on the Gigabit Ethernet interface 1/1 in auto-negotiation mode:

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

This example shows how to limit the speed negotiation to 100 Mbps on the Gigabit Ethernet interface 1/1:

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

Related Commands

duplex
interface (refer to Cisco IOS documentation)
show controllers (refer to Cisco IOS documentation)
show interfaces (refer to Cisco IOS documentation)

storm-control

To enable broadcast storm control on a port and to specify what to do when a storm occurs on a port, use the **storm-control** interface configuration command. To disable storm control for the broadcast traffic and to disable a specified storm-control action, use the **no** form of this command.

storm-control {**broadcast level** *high level* [*lower level*]} | **action** {**shutdown** | **trap**}}

no storm-control {**broadcast level** *level* [*lower level*]} | **action** {**shutdown** | **trap**}}

Syntax Description

broadcast	Enables the broadcast storm control on the port.
level *high-level lower-level*	Defines the rising and falling suppression levels: • *high-level*—Rising suppression level as a percent of total bandwidth, up to two decimal places; valid values are from 0 to 100 percent. Blocks the flooding of storm packets when the value specified for *level* is reached. • *lower-level*—(Optional) Falling suppression level as a percent of total bandwidth, up to two decimal places; valid values are from 0 to 100. This value must be less than the rising suppression value.
action	Directs the switch to take action when a storm occurs on a port.
shutdown	Disables the port during a storm.
trap	Sends an SNMP trap when a storm occurs. This keyword is available but not supported in 12.1(19)EW.

Defaults

Broadcast storm control is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(40)SG	Support for the Supervisor Engine 6-E and Catalyst 4900M chassis is introduced.

Usage Guidelines

Enter the **storm-control broadcast level** command to enable traffic storm control on the interface, configure the traffic storm control level, and apply the traffic storm control level to the broadcast traffic on the interface.

The Catalyst 4500 series switch supports broadcast traffic storm control on all LAN ports.

The period is required when you enter the fractional suppression level.

The suppression level is entered as a percentage of the total bandwidth. A threshold value of 100 percent indicates that no limit is placed on traffic. A value of 0.0 means that all specified traffic on that port is blocked.

Enter the **show interfaces counters** **storm-control** command to display the discard count.

Enter the **show running-config** command to display the enabled suppression mode and level setting.

To turn off suppression for the specified traffic type, you can do one of the following:

- Set the *high-level* value to 100 percent for the specified traffic type.
- Use the **no** form of this command.

The lower level is ignored for the interfaces that perform storm control in the hardware.

Note The **lower level** keyword does not apply to the Supervisor Engine 6-E and Catalyst 4900M chassis implementations.

Examples

This example shows how to enable broadcast storm control on a port with a 75.67 percent rising suppression level:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/1
Switch(config-if)# storm-control broadcast level 75.67
Switch(config-if)# end
```

This example shows how to disable the port during a storm:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/1
Switch(config-if)# storm-control action shutdown
Switch(config-if)# end
```

This example shows how to disable storm control on a port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/1
Switch(config-if)# no storm-control broadcast level
Switch(config-if)# end
```

This example shows how to disable storm control by setting the high level to 100 percent:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/1
Switch(config-if)# storm-control broadcast level 100
Switch(config-if)# end
```

Related Commands

show interfaces counters
show running-config

storm-control broadcast include multicast

To enable multicast storm control on a port, use the **storm-control broadcast include multicast** command. To disable multicast storm control, use the **no** form of this command.

storm-control broadcast include multicast

no storm-control broadcast include multicast

Syntax Description

This command has no arguments or keywords.

Defaults

Multicast storm control is disabled.

Command Modes

Global configuration mode
Interface configuration mode on a Supervisor Engine 6-E and Catalyst 4900M chassis

Command History

Release	Modification
12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(40)SG	Support for the Supervisor Engine 6-E and Catalyst 4900M chassis is introduced.

Usage Guidelines

This command prompts the hardware to filter multicast packets if it is already filtering broadcast packets.

The Supervisor Engine 6-E and Catalyst 4900M chassis supports per-interface multicast suppression. When you enable multicast suppression on an interface you subject incoming multicast and broadcast traffic on that interface to suppression.

Examples

This example shows how to enable multicast storm control globally:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# storm-control broadcast include multicast
Switch(config)# end
```

This example shows how to enable per-port Multicast storm control on a Supervisor Engine 6-E:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet2/4
Switch(config-if)# storm-control broadcast include multicast
Switch(config)# end
```

Related Commands

storm-control

switchport

To modify the switching characteristics of a Layer 2 switch interface, use the **switchport** command. To return the interface to the routed-interface status and cause all further Layer 2 configuration to be erased, use the **no** form of this command without parameters.

switchport [**access vlan** *vlan_num*] | [**nonegotiate**] | [**voice vlan** {*vlan_id* | **dot1p** | **none** | **untagged**}]

no switchport [**access** | **nonegotiate** | **voice vlan**]

Syntax Description

access vlan *vlan_num*	(Optional) Sets the VLAN when the interface is in access mode; valid values are from 1 to 1005.
nonegotiate	(Optional) Specifies that the DISL/DTP negotiation packets will not be sent on the interface.
voice vlan *vlan_id*	(Optional) Specifies the number of the VLAN; valid values are from 1 to 1005.
dot1p	(Optional) Specifies that the PVID packets are tagged as priority.
none	(Optional) Specifies that the telephone and voice VLAN do not communicate.
untagged	(Optional) Specifies the untagged PVID packets.

Defaults

The default settings are as follows:

- Switchport trunking mode is enabled.
- Dynamic negotiation parameter is set to auto.
- Access VLANs and trunk interface native VLANs are a default VLAN corresponding to the platform or interface hardware.
- All VLAN lists include all VLANs.
- No voice VLAN is enabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(11)EW	Support for voice VLAN was added.

Usage Guidelines

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

The **no** form of the **switchport access** command resets the access mode VLAN to the appropriate default VLAN for the device. The **no** form of the **switchport nonegotiate** command removes the **nonegotiate** status.

When you are using the **nonegotiate** keyword, DISL/DTP negotiation packets will not be sent on the interface. The device will trunk or not trunk according to the **mode** parameter given: **access** or **trunk**. This command will return an error if you attempt to execute it in **dynamic** (**auto** or **desirable**) mode.

The voice VLAN is automatically set to VLAN 1 unless you use one of the optional keywords.

If you use the **switch port voice vlan** command for an interface, the interface cannot join a port channel.

When you use the **switchport voice vlan** command, the output for the **show running-config** command changes to show the voice VLAN set.

Examples

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

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

This example shows how to cause a port interface in access mode, which is configured as a switched interface, to operate in VLAN 2:

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

This example shows how to cause a port interface, which is configured as a switched interface, to refrain from negotiating in trunking mode and act as a trunk or access port (depending on the **mode** set):

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

This example shows how to set the voice VLAN for the interface to VLAN 2:

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

Related Commands

show interfaces switchport

switchport access vlan

To set the VLAN when an interface is in access mode, use the **switchport access vlan** command. To reset the access mode VLAN to the appropriate default VLAN for the device, use the **no** form of this command.

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

no switchport access vlan

Syntax Description

vlan-id	(Optional) Number of the VLAN on the interface in access mode; valid values are from 1 to 4094.
dynamic	(Optional) Enables VMPS control of the VLAN.

Defaults

The default settings are as follows:

- The access VLAN and trunk interface native VLAN are default VLANs that correspond to the platform or the interface hardware.
- All VLAN lists include all VLANs.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(13)EW	Support for VPMS was added.

Usage Guidelines

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter the **switchport access vlan** command. This action is required only if you have not already entered the **switchport** command for the interface.

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

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

If your system is configured with a Supervisor Engine I, valid values for *vlan-id* are from 1 to 1005. If your system is configured with a Supervisor Engine II, valid values for *vlan-id* are from 1 to 4094. Extended-range VLANs are not supported on systems configured with a Supervisor Engine I.

Examples

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

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

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

This example shows how to cause a port interface that has already been configured as a switched interface to operate in VLAN 2 instead of the platform's default VLAN when in access mode:

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

Related Commands

show interfaces switchport

switchport autostate exclude

To exclude a port from the VLAN interface link-up calculation, use the **switchport autostate exclude** command. To return to the default settings, use the **no** form of this command.

switchport autostate exclude

no switchport autostate exclude

Syntax Description

This command has no keywords or arguments.

Defaults

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

Command Modes

Interface configuration mode

Command History

Release	Modification
12.2(37)SG	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter the **switchport autostate exclude** command. This action is required only if you have not entered the **switchport** command for the interface.

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

The **switchport autostate exclude** command marks the port to be excluded from the interface VLAN up calculation when there are multiple ports in the VLAN.

The **show interface** *interface* **switchport** command displays the autostate mode if the mode has been set. If the mode has not been set, the autostate mode is not displayed.

Examples

This example shows how to exclude a port from the VLAN interface link-up calculation:

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

This example shows how to include a port in the VLAN interface link-up calculation:

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

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

Related Commands

show interfaces switchport

switchport block

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

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

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

Syntax Description

multicast	Specifies that the unknown multicast traffic should be blocked.
unicast	Specifies that the unknown unicast traffic should be blocked.

Defaults

Unknown multicast and unicast traffic are not blocked.

All traffic with unknown MAC addresses is sent to all ports.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

You can block the unknown multicast or unicast traffic on the switch ports.

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

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

Examples

This example shows how to block the 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

show interfaces switchport

switchport mode

To set the interface type, use the **switchport mode** command. To reset the mode to the appropriate default mode for the device, use the **no** form of this command.

switchport mode {**access** | **dot1q-tunnel** | **trunk** | **dynamic** {**auto** | **desirable**}}

switchport mode private-vlan {**host** | **promiscuous** | **trunk promiscuous** | **trunk** [**secondary**]}

no switchport mode dot1q-tunnel

no switchport mode private-vlan

Syntax Description

access	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
dot1q-tunnel	Specifies an 802.1Q tunnel port.
trunk	Specifies a trunking VLAN Layer 2 interface.
dynamic auto	Specifies that the interface convert the link to a trunk link.
dynamic desirable	Specifies that the interface actively attempt to convert the link to a trunk link.
private-vlan host	Specifies that the ports with a valid PVLAN trunk association become active host private VLAN trunk ports.
private-vlan promiscuous	Specifies that the ports with a valid PVLAN mapping become active promiscuous ports.
private-vlan trunk promiscuous	Specifies that the ports with valid PVLAN trunk mapping become active promiscuous trunk ports.
private-vlan trunk secondary	Specifies that the ports with a valid PVLAN trunk association become active host private VLAN trunk ports.

Defaults

Link converts to a trunk link.

dot1q tunnel ports are disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(18)EW	Support was added for configuring dot1q tunnel ports.
12.2(31)SG	Support was added for trunk promiscuous ports.

Usage Guidelines

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

If you enter **trunk** mode, the interface goes into permanent trunking mode and negotiates to convert the link into a trunk link even if the neighboring interface does not approve the change.

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

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

If you specify the **dot1q-tunnel keyword**, the port is set unconditionally as an 802.1Q tunnel port.

The port becomes inactive if you configure it as a private VLAN trunk port and one of the following applies:

- The port does not have a valid PVLAN association.
- The port does not have valid allowed normal VLANs.

If a private port PVLAN association or mapping is deleted, or if a private port is configured as a SPAN destination, it becomes inactive.

Examples

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

```
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)#
```

This example shows how to set a port to PVLAN host mode:

```
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)#
```

This example shows how to set a port to private VLAN trunk:

```
Switch(config-if)# switchport mode private-vlan trunk
Switch(config-if)#
```

This example shows how to configure a port for an 802.1Q tunnel port:

```
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)#
```

This example shows how to configure a promiscuous trunk port:

```
Switch(config-if)# switchport mode private-vlan trunk promiscuous
Switch(config-if)#
```

This example shows how to configure an isolated trunk port:

```
Switch(config-if)# switchport mode private-vlan trunk
OR
Switch(config-if)# switchport mode private-vlan trunk secondary
Switch(config-if)#
```

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

This example shows how to configure interface FastEthernet 5/2 as a PVLAN promiscuous port, map it to a PVLAN, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 200 2
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name:Fa5/2
Switchport:Enabled
Administrative Mode:private-vlan promiscuous
Operational Mode:private-vlan promiscuous
Administrative Trunking Encapsulation:negotiate
Operational Trunking Encapsulation:native
Negotiation of Trunking:Off
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Voice VLAN:none
Administrative Private VLAN Host Association:none
Administrative Private VLAN Promiscuous Mapping:200 (VLAN0200) 2 (VLAN0002)
Private VLAN Trunk Native VLAN:none
Administrative Private VLAN Trunk Encapsulation:dot1q
Administrative Private VLAN Trunk Normal VLANs:none
Administrative Private VLAN Trunk Private VLANs:none
Operational Private VLANs:
  200 (VLAN0200) 2 (VLAN0002)
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled:2-1001
Capture Mode Disabled
Capture VLANs Allowed:ALL
```

This example shows how to configure interface FastEthernet 5/1 as a PVLAN host port and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 202 440
Switch(config-if)# end
```

```
Switch# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Appliance trust: none
Administrative Private Vlan
  Host Association: 202 (VLAN0202) 440 (VLAN0440)
  Promiscuous Mapping: none
  Trunk encapsulation : dot1q
  Trunk vlans:
Operational private-vlan(s):
  202 (VLAN0202) 440 (VLAN0440)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

This example shows how to configure interface FastEthernet 5/2 as a secondary trunk port, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk secondary
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10. 3-4
Switch(config-if)# switchport private-vlan association trunk 3 301
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
    Switchport: Enabled
    Administrative Mode: private-vlan trunk secondary
    Operational Mode: private-vlan trunk secondary
    Administrative Trunking Encapsulation: negotiate
    Operational Trunking Encapsulation: dot1q
    Negotiation of Trunking: On
    Access Mode VLAN: 1 (default)
    Trunking Native Mode VLAN: 1 (default)
    Administrative Native VLAN tagging: enabled
    Voice VLAN: none
    Administrative private-vlan host-association: none A
    dministrative private-vlan mapping: none
    Administrative private-vlan trunk native VLAN: 10
    Administrative private-vlan trunk Native VLAN tagging: enabled
    Administrative private-vlan trunk encapsulation: dot1q
    Administrative private-vlan trunk normal VLANs: none
    Administrative private-vlan trunk associations:
        3 (VLAN0003) 301 (VLAN0301)
    Administrative private-vlan trunk mappings: none
    Operational private-vlan: none
    Operational Normal VLANs: none
    Trunking VLANs Enabled: ALL
    Pruning VLANs Enabled: 2-1001
    Capture Mode Disabled Capture VLANs Allowed: ALL

    Unknown unicast blocked: disabled
    Unknown multicast blocked: disabled
    Appliance trust: none
Switch(config-if)#
```

This example shows how to configure interface FastEthernet 5/2 as a promiscuous trunk port and to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk promiscuous
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10, 3-4
Switch(config-if)# switchport private-vlan mapping trunk 3 301, 302
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan trunk promiscuous
Operational Mode: private-vlan trunk promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

```
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 10
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: 3-4,10
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
    3 (VLAN0003) 301 (VLAN0301)  302 (VLAN0302)
Operational private-vlan:
  3 (VLAN0003) 301 (VLAN0301) 302 (VLAN0302)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Switch(config-if)#
```

Related Commands

show interfaces switchport
switchport
switchport private-vlan host-association
switchport private-vlan mapping

switchport port-security

To enable port security on an interface, use the **switchport port-security** command. To disable port security and set parameters to their default states, use the **no** form of this command.

switchport port-security [**aging** {**static** | **time** *time* | **type** {**absolute** | **inactivity**}} | **limit rate invalid-source-mac** [**N** | **none**] | **mac-address** *mac-address* [**vlan** {**access** | **voice**} | **mac-address sticky** [*mac-address*] [**vlan access** | **voice**] | **maximum** *value* [**vlan** {**access** | **voice**} | **violation** {**restrict** | **shutdown**}]

no switchport port-security [**aging** {**static** | **time** *time* | **type** {**absolute** | **inactivity**}} | **limit rate invalid-source-mac** [**N** | **none**] | **mac-address** *mac-address* [**vlan** {**access** | **voice**} | **mac-address sticky** [*mac-address*] [**vlan access** | **voice**] | **maximum** *value* [**vlan** {**access** | **voice**} | **violation** {**restrict** | **shutdown**}]

Syntax Description

aging	(Optional) Specifies aging for port security.
static	(Optional) Enables aging for statically configured secure addresses on this port.
time *time*	(Optional) Specifies the aging time for this port. The valid values are from 0 to 1440 minutes. If the time is 0, aging is disabled for this port.
type absolute	(Optional) Sets the aging type as absolute aging. All the secure addresses on this port age out exactly after the time (minutes) specified and are removed from the secure address list.
type inactivity	(Optional) Sets the aging type as inactivity aging. 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.
limit rate invalid-source-mac	(Optional) Sets the rate limit for bad packets. This rate limit also applies to the port where DHCP snooping security mode is enabled as filtering the IP and MAC address.
N none	(Optional) Supplies a rate limit (**N**) or indicates none (**none**).
mac-address *mac-address*	(Optional) Specifies a secure MAC address for the interface; a 48-bit MAC address. You can add additional secure MAC addresses up to the maximum value that is configured.
sticky	(Optional) Configures the dynamic addresses as sticky on the interface.
vlan access	(Optional) Deletes the secure MAC addresses from access VLANs.
vlan voice	(Optional) Deletes the secure MAC addresses from voice VLANs.
maximum *value*	(Optional) Sets the maximum number of secure MAC addresses for the interface. Valid values are from 1 to 3072. The default setting is 1.
violation	(Optional) Sets the security violation mode and action to be taken if port security is violated.
restrict	(Optional) Sets the security violation restrict mode. In this mode, a port security violation restricts data and causes the security violation counter to increment.
shutdown	(Optional) Sets the security violation shutdown mode. In this mode, a port security violation causes the interface to immediately become error disabled.

Defaults

The default settings are as follows:

- Port security is disabled.
- When port security is enabled and no keywords are entered, the default maximum number of secure MAC addresses is 1.
- Aging is disabled.
- Aging time is 0 minutes.
- All secure addresses on this port age out immediately after they are removed from the secure address list.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(19)EW	Extended to include DHCP snooping security enhancement.
12.2(18)EW	Add support for sticky interfaces.
12.2(31)SG	Add support for sticky port security.

Usage Guidelines

After you set the maximum number of secure MAC addresses that are allowed on a port, you can add secure addresses to the address table by manually configuring them, by allowing the port to dynamically configure them, or by configuring some MAC addresses and allowing the rest to be dynamically configured.

The packets are dropped into the hardware when the maximum number of secure MAC addresses are in the address table and a station that does not have a MAC address in the address table 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 set the maximum allowed secure addresses on the port to more than 1.

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

A secure port has the following limitations:

- A secure port cannot be a dynamic access port or a trunk port.
- A secure port cannot be a routed 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 belong to a Fast EtherChannel or Gigabit EtherChannel port group.
- A secure port cannot be an 802.1X port.
- If you try to enable 802.1X on a secure port, an error message appears, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to a secure port, an error message appears, and the security settings are not changed.

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

To enable secure address aging for a particular port, set the aging time to a value other than 0 for that port.

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 action removes the secure address when it becomes 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.

If the sticky command is executed without a MAC address specified, all MAC addresses that are learned on that port will be made sticky. You can also specify a specific MAC address to be a sticky address by entering the **sticky** keyword next to it.

You can configure the sticky feature even when port security is not enabled on the interface. The feature becomes operational when you enable port security on the interface.

You can use the **no** form of the **sticky** command only if the sticky feature is already enabled on the interface.

Examples

This example shows how to set the aging time to 2 hours (120 minutes) for the secure addresses on the Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 0/12
Switch(config-if)# switchport port-security aging time 120
Switch(config-if)#
```

This example shows how to set the aging timer type to Inactivity for the secure addresses on the Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 0/12
Switch(config-if)# switch port-security aging type inactivity
Switch(config-if)#
```

The following example shows how to configure rate limit for invalid source packets on Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 0/12
Switch(config-if)# switchport port-security limit rate invalid-source-mac 100
Switch(config-if)#
```

The following example shows how to configure rate limit for invalid source packets on Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 0/12
Switch(config-if)# switchport port-security limit rate invalid-source-mac none
Switch(config-if)#
```

You can verify the settings for all secure ports or the specified port by using the **show port-security** privileged EXEC command.

This example shows how to remove all sticky and static addresses that are configured on the interface:

```
Switch(config)# interface fastethernet 2/12
Switch(config-if)# no switchport port-security mac-address
Switch(config-if)
```

This example shows how to configure a secure MAC address on Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 0/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 1000.2000.3000
Switch(config-if)
```

This example shows how to make all MAC addresses learned on Fast Ethernet port 12 sticky:

```
Switch(config)# interface fastethernet 2/12
SSwitch(config-if)# switchport port-security mac-address sticky
Switch(config-if)
```

This example shows how to make MAC address 1000.2000.3000 sticky on Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 2/12
Switch(config-if)# switchport port-security mac-address sticky 1000.2000.3000
Switch(config-if)
```

This example shows how to disable the sticky feature on Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 2/12
Switch(config-if)# no switchport port-security mac-address sticky
Switch(config-if)
```

Note This command makes all sticky addresses on this interface normal learned entries. It does not delete the entries from the secure MAC address table.

Note The following examples show how to configure sticky secure MAC addresses in access and voice VLANs on interfaces with voice VLAN configured. If you do not have voice VLAN configured the **vlan** [**access** | **voice**] keywords are not supported.

This example shows how to configure sticky MAC addresses for voice and data VLANs on Fast Ethernet interface 5/1 and to verify the configuration:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fa5/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.obob vlan voice
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0005 vlan access
Switch(config-if)# end
```

This example shows how to designate a maximum of one MAC address for a voice VLAN (for a Cisco IP Phone, let's say) and one MAC address for the data VLAN (for a PC, let's say) on Fast Ethernet interface 5/1 and to verify the configuration:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fa5/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security maximum 1 vlan voice
Switch(config-if)# switchport port-security maximum 1 vlan access
Switch(config-if)# end
```

Note Sending traffic to the ports causes the system to configure the port with sticky secure addresses.

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

Related Commands

show interfaces switchport
show port-security
switchport block

switchport private-vlan association trunk

To configure the association between a secondary VLAN and a VLAN on a private VLAN trunk port, use the **switchport private-vlan association trunk** command. To remove the private VLAN mapping from the port, use the **no** form of this command.

switchport private-vlan association trunk {*primary-vlan-id*} {*secondary-vlan-id*}

no switchport private-vlan association trunk {*primary-vlan-id*}

Syntax Description

primary-vlan-id	Number of the primary VLAN of the private VLAN relationship.
secondary-vlan-id	Number of the secondary VLAN of the private VLAN relationship.

Defaults

Private VLAN mapping is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(20)EW	Support for community VLAN was added.

Usage Guidelines

Multiple private VLAN pairs can be specified so that a private VLAN trunk port can carry multiple secondary VLANs. If an association is specified for the existing primary VLAN, the existing association is replaced.

Only isolated secondary VLANs can be carried over a private VLAN trunk.

Note Community secondary VLANs on a private VLAN trunk are not supported in this release.

If there is no trunk association, any packets received on the secondary VLANs are dropped.

Examples

This example shows how to configure a port with a primary VLAN (VLAN 18) and secondary VLAN (VLAN 20):

```
Switch(config-if)# switchport private-vlan association trunk 18 20
Switch(config-if)#
```

This example shows how to remove the private VLAN association from the port:

```
Switch(config-if)# no switchport private-vlan association trunk 18
Switch(config-if)#
```

This example shows how to configure interface FastEthernet 5/2 as a secondary trunk port, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk secondary
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10. 3-4
Switch(config-if)# switchport private-vlan association trunk 3 301
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
    Switchport: Enabled
    Administrative Mode: private-vlan trunk secondary
    Operational Mode: private-vlan trunk secondary
    Administrative Trunking Encapsulation: negotiate
    Operational Trunking Encapsulation: dot1q
    Negotiation of Trunking: On
    Access Mode VLAN: 1 (default)
    Trunking Native Mode VLAN: 1 (default)
    Administrative Native VLAN tagging: enabled
    Voice VLAN: none
    Administrative private-vlan host-association: none A
    dministrative private-vlan mapping: none
    Administrative private-vlan trunk native VLAN: 10
    Administrative private-vlan trunk Native VLAN tagging: enabled
    Administrative private-vlan trunk encapsulation: dot1q
    Administrative private-vlan trunk normal VLANs: none
    Administrative private-vlan trunk associations:
        3 (VLAN0003) 301 (VLAN0301)
    Administrative private-vlan trunk mappings: none
    Operational private-vlan: none
    Operational Normal VLANs: none
    Trunking VLANs Enabled: ALL
    Pruning VLANs Enabled: 2-1001
    Capture Mode Disabled Capture VLANs Allowed: ALL

    Unknown unicast blocked: disabled
    Unknown multicast blocked: disabled
    Appliance trust: none
Switch(config-if)#
```

Related Commands

show interfaces switchport
switchport mode

switchport private-vlan host-association

To define a PVLAN association for an isolated or community port, use the **switchport private-vlan host-association** command. To remove the PVLAN mapping from the port, use the **no** form of this command.

switchport private-vlan host-association {*primary-vlan-id*} {*secondary-vlan-id*}

no switchport private-vlan host-association

Syntax Description

primary-vlan-id	Number of the primary VLAN of the PVLAN relationship; valid values are from 1 to 4094.
secondary-vlan-list	Number of the secondary VLAN of the private VLAN relationship; valid values are from 1 to 4094.

Defaults

Private VLAN mapping is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for extended addressing was added.

Usage Guidelines

There is no runtime effect on the port unless it is in PVLAN host mode. If the port is in PVLAN host mode but all VLANs do not exist, the command is allowed, but the port is made inactive.

The secondary VLAN may be an isolated or community VLAN.

Examples

This example shows how to configure a port with a primary VLAN (VLAN 18) and secondary VLAN (VLAN 20):

```
Switch(config-if)# switchport private-vlan host-association 18 20
Switch(config-if)#
```

This example shows how to remove the PVLAN association from the port:

```
Switch(config-if)# no switchport private-vlan host-association
Switch(config-if)#
```

This example shows how to configure interface FastEthernet 5/1 as a PVLAN host port and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 202 440
Switch(config-if)# end
Switch# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Appliance trust: none
Administrative Private Vlan
  Host Association: 202 (VLAN0202) 440 (VLAN0440)
  Promiscuous Mapping: none
  Trunk encapsulation : dot1q
  Trunk vlans:
Operational private-vlan(s):
  202 (VLAN0202) 440 (VLAN0440)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

Related Commands

show interfaces switchport
switchport mode

switchport private-vlan mapping

To define private VLAN mapping for a promiscuous port, use the **switchport private-vlan mapping** command. To clear all mapping from the primary VLAN, use the **no** form of this command.

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

switchport private-vlan mapping trunk {*primary-vlan-id*} [**add** | **remove**] *secondary-vlan-list*

no switchport private-vlan mapping [**trunk**]

Syntax Description

primary-vlan-id	Number of the primary VLAN of the private VLAN relationship; valid values are from 2 to 4094 (excluding 1002 to 1005).
secondary-vlan-list	Number of the secondary VLANs to map to the primary VLAN; valid values are from 2 to 4094.
add	Maps the secondary VLANs to the primary VLAN.
remove	Clears mapping between the secondary VLANs and the primary VLAN.
trunk	Maps the trunks secondary VLANs to the primary VLAN.

Defaults

Private VLAN mapping is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for extended addressing was added.
12.2(20)EW	Support for community VLAN was added.
12.2(31)SG	Support for trunk VLAN was added.

Usage Guidelines

There is no run-time effect on the port unless it is in private VLAN promiscuous mode. If the port is in private VLAN promiscuous mode but the VLANs do not exist, the command is allowed, but the port is made inactive.

The secondary VLAN may be an isolated or community VLAN.

Note The maximum number of unique private VLAN pairs supported by the **switchport private-vlan mapping trunk** command above is 500. For example, one thousand secondary VLANs could map to one primary VLAN, or one thousand secondary VLANs could map one to one to one thousand primary VLANs.

Examples

This example shows how to configure the mapping of primary VLAN 18 to the secondary isolated VLAN 20 on a port:

```
Switch(config-if)# switchport private-vlan mapping 18 20
Switch(config-if)#
```

This example shows how to add a VLAN to the mapping:

```
Switch(config-if)# switchport private-vlan mapping 18 add 21
Switch(config-if)#
```

This example shows how to add a range of secondary VLANs to the mapping:

```
Switch(config-if)# switchport private-vlan mapping 18 add 22-24
Switch(config-if)#
```

This example shows how to add a range of secondary VLANs to the trunk mapping:

```
Switch(config-if)# switchport private-vlan mapping trunk 18 add 22-24
Switch(config-if)#
```

This example shows how to configure interface FastEthernet 5/2 as a PVLAN promiscuous port, map it to a PVLAN, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 200 2
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name:Fa5/2
Switchport:Enabled
Administrative Mode:private-vlan promiscuous
Operational Mode:private-vlan promiscuous
Administrative Trunking Encapsulation:negotiate
Operational Trunking Encapsulation:native
Negotiation of Trunking:Off
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Voice VLAN:none
Administrative Private VLAN Host Association:none
Administrative Private VLAN Promiscuous Mapping:200 (VLAN0200) 2 (VLAN0002)
Private VLAN Trunk Native VLAN:none
Administrative Private VLAN Trunk Encapsulation:dot1q
Administrative Private VLAN Trunk Normal VLANs:none
Administrative Private VLAN Trunk Private VLANs:none
Operational Private VLANs:
  200 (VLAN0200) 2 (VLAN0002)
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled:2-1001
Capture Mode Disabled
Capture VLANs Allowed:ALL
```

This example shows how to configure interface FastEthernet 5/2 as a promiscuous trunk port and to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk promiscuous
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10, 3-4
Switch(config-if)# switchport private-vlan mapping trunk 3 301, 302
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan trunk promiscuous
Operational Mode: private-vlan trunk promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 10
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: 3-4,10
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
    3 (VLAN0003) 301 (VLAN0301)  302 (VLAN0302)
Operational private-vlan:
  3 (VLAN0003) 301 (VLAN0301) 302 (VLAN0302)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Switch(config-if)#
```

Related Commands

show interfaces private-vlan mapping

switchport private-vlan trunk allowed vlan

To configure a list of the allowed normal VLANs on a private VLAN trunk port, use the **switchport private-vlan trunk allowed vlan** command. To remove all the allowed normal VLANs from a private VLAN trunk port, use the **no** form of this command.

switchport private-vlan trunk allowed vlan {*vlan-list*} **all** | **none** | [**add** | **remove** | **except**] *vlan_atom* [,*vlan_atom...*]

no switchport private-vlan trunk allowed vlan

Syntax Description

vlan_list	Sets the list of allowed VLANs; see the "Usage Guidelines" section for formatting guidelines for *vlan_list*.
all	Specifies all VLANs from 1 to 4094. This keyword is not supported on commands that do not permit all VLANs in the list to be set at the same time.
none	Indicates an empty list. This keyword is not supported on commands that require certain VLANs to be set or at least one VLAN to be set.
add	(Optional) Adds the defined list of VLANs to those currently set instead of replacing the list.
remove	(Optional) Removes the defined list of VLANs from those currently set instead of replacing the list.
except	(Optional) Lists the VLANs that should be calculated by inverting the defined list of VLANs.
vlan_atom	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

All allowed normal VLANs are removed from a private VLAN trunk port.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

By default, no normal VLANs are allowed unless you explicitly configure the VLANs to be allowed.

Use this command only for normal VLANs on a private VLAN trunk port.

Use the **switchport private-vlan association trunk** command to configure a port that can carry private VLANs on a private VLAN trunk port.

Examples

This example shows how to configure the private VLAN trunk port that carries normal VLANs 1 to10:

```
Switch(config-if)# switchport private-vlan trunk allowed vlan 1-10
Switch(config-if)#
```

This example shows how to remove all the allowed normal VLANs from a private VLAN trunk port:

```
Switch(config-if)# no switchport private-vlan trunk allowed vlan
Switch(config-if)#
```

This example shows how to configure interface FastEthernet 5/2 as a secondary trunk port, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk secondary
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10. 3-4
Switch(config-if)# switchport private-vlan association trunk 3 301
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
    Switchport: Enabled
    Administrative Mode: private-vlan trunk secondary
    Operational Mode: private-vlan trunk secondary
    Administrative Trunking Encapsulation: negotiate
    Operational Trunking Encapsulation: dot1q
    Negotiation of Trunking: On
    Access Mode VLAN: 1 (default)
    Trunking Native Mode VLAN: 1 (default)
    Administrative Native VLAN tagging: enabled
    Voice VLAN: none
    Administrative private-vlan host-association: none A
    dministrative private-vlan mapping: none
    Administrative private-vlan trunk native VLAN: 10
    Administrative private-vlan trunk Native VLAN tagging: enabled
    Administrative private-vlan trunk encapsulation: dot1q
    Administrative private-vlan trunk normal VLANs: none
    Administrative private-vlan trunk associations:
        3 (VLAN0003) 301 (VLAN0301)
    Administrative private-vlan trunk mappings: none
    Operational private-vlan: none
    Operational Normal VLANs: none
    Trunking VLANs Enabled: ALL
    Pruning VLANs Enabled: 2-1001
    Capture Mode Disabled Capture VLANs Allowed: ALL

    Unknown unicast blocked: disabled
    Unknown multicast blocked: disabled
    Appliance trust: none
Switch(config-if)#
```

This example shows how to configure interface FastEthernet 5/2 as a promiscuous trunk port and to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk promiscuous
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10, 3-4
Switch(config-if)# switchport private-vlan mapping trunk 3 301, 302
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan trunk promiscuous
Operational Mode: private-vlan trunk promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 10
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: 3-4,10
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
    3 (VLAN0003) 301 (VLAN0301)  302 (VLAN0302)
Operational private-vlan:
  3 (VLAN0003) 301 (VLAN0301) 302 (VLAN0302)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Switch(config-if)#
```

Related Commands

show interfaces switchport
switchport mode

switchport private-vlan trunk native vlan tag

To control the tagging of the native VLAN traffic on 802.1Q private VLAN trunks, use the **switchport private-vlan trunk native vlan tag** command. To remove the control of tagging (and default to the global setting), use the **no** form of this command.

switchport private-vlan trunk native vlan tag

no switchport private-vlan trunk native vlan tag

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is global; the settings on the port are determined by the global setting.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(18)EW	Removed **vlan-id** keyword.

Usage Guidelines

The configuration created with this command only applies to ports that are configured as private VLAN trunks.

Examples

This example shows how to enable 802.1Q native VLAN tagging on a PVLAN trunk:

```
Switch(config-if)# switchport private-vlan trunk native vlan tag
Switch(config-if)#
```

Related Commands

show interfaces switchport
switchport mode

switchport trunk

To set the trunk characteristics when an interface is in trunking mode, use the **switchport trunk** command. To reset all of the trunking characteristics back to the original defaults, use the **no** form of this command.

switchport trunk encapsulation {**isl** | **dot1q** | **negotiate**}

no switchport trunk encapsulation

switchport trunk native vlan {**tag** | *vlan_id*}

no switchport trunk native vlan {**tag** | *vlan_id*}

switchport trunk allowed vlan *vlan_list*

no switchport trunk allowed vlan *vlan_list*

switchport trunk pruning vlan *vlan_list*

no switchport trunk pruning vlan *vlan_list*

Syntax Description

encapsulation isl	Sets the trunk encapsulation format to ISL.
encapsulation dot1q	Sets the trunk encapsulation format to 802.1Q.
encapsulation negotiate	Specifies that if DISL and DTP negotiation do not resolve the encapsulation format, ISL will be the selected format.
native vlan *tag*	Specifies the tagging of native VLAN traffic on 802.1Q trunks.
native vlan *vlan_id*	Sets the native VLAN for the trunk in 802.1Q trunking mode.
allowed vlan *vlan_list*	Sets the list of allowed VLANs that transmit this interface in tagged format when in trunking mode. See the “Usage Guidelines” section for formatting guidelines for *vlan_list*.
pruning vlan *vlan_list*	Sets the list of VLANs that are enabled for VTP pruning when the switch is in trunking mode. See the “Usage Guidelines” section for formatting guidelines for *vlan_list*.

Defaults

The default settings are as follows:

- The encapsulation type is dependent on the platform or interface hardware.
- The access VLANs and trunk interface native VLANs are a default VLAN that corresponds to the platform or the interface hardware.
- All VLAN lists include all VLANs.
- Native VLAN tagging is enabled on the port if enabled globally.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for extended addressing was added.
12.2(18)EW	Support for native VLAN tagging was added.

Usage Guidelines

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 supported on commands that do not permit all VLANs in the list to be set at the same time.
- **none** indicates an empty list. This keyword is not supported 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.
- **remove** removes the defined list of VLANs from those currently set, instead of replacing the list.
- **except** lists the VLANs that should be calculated by inverting the defined list of VLANs.
- *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).

The **switchport trunk encapsulation** command is supported only for platforms and interface hardware that can support both ISL and 802.1Q formats.

If you enter the **negotiate** keywords, and DISL and DTP negotiation do not resolve the encapsulation format, ISL is the selected format. The **no** form of this command resets the trunk encapsulation format back to the default.

The **no** form of the **native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.

The **no** form of the **allowed vlan** command resets the list to the default list, which allows all VLANs.

The **no** form of the **pruning vlan** command resets the list to the default list, which enables all VLANs for VTP pruning.

These configuration guidelines and restrictions apply when using 802.1Q trunks and impose some limitations on the trunking strategy for a network:

- When connecting Cisco switches through an 802.1Q trunk, make sure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.
- Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can cause spanning-tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk. If this is not possible, disable spanning tree on every VLAN in the network. Make sure that your network is free of physical loops before disabling spanning tree.
- When you connect two Cisco switches through 802.1Q trunks, the switches exchange spanning-tree BPDUs on each VLAN that is allowed on the trunks. The BPDUs on the native VLAN of the trunk are sent untagged to the reserved 802.1d spanning-tree multicast MAC address (01-80-C2-00-00-00). The BPDUs on all other VLANs on the trunk are sent tagged to the reserved SSTP multicast MAC address (01-00-0c-cc-cc-cd).

- Non-Cisco 802.1Q switches maintain only a single instance of spanning tree (MST) that defines the spanning-tree topology for all VLANs. When you connect a Cisco switch to a non-Cisco switch through an 802.1Q trunk, the MST of the non-Cisco switch and the native VLAN spanning tree of the Cisco switch combine to form a single spanning-tree topology known as the CST.
- Because Cisco switches transmit BPDUs to the SSTP multicast MAC address on the VLANs other than the native VLAN of the trunk, non-Cisco switches do not recognize these frames as BPDUs and flood them on all ports in the corresponding VLAN. Cisco switches connected to the non-Cisco 802.1Q network receive these flooded BPDUs. Because Cisco switches receive the flooded BPDUs, the switches can maintain a per-VLAN spanning-tree topology across a network of non-Cisco 802.1Q switches. The non-Cisco 802.1Q network separating the Cisco switches is treated as a single broadcast segment between all switches that are connected to the non-Cisco 802.1Q network through the 802.1Q trunks.
- Ensure that the native VLAN is the same on *all* of the 802.1Q trunks connecting the Cisco switches to the non-Cisco 802.1Q network.
- If you are connecting multiple Cisco switches to a non-Cisco 802.1Q network, all of the connections must be through the 802.1Q trunks. You cannot connect Cisco switches to a non-Cisco 802.1Q network through the ISL trunks or through the access ports. This action causes the switch to place the ISL trunk port or access port into the spanning-tree “port inconsistent” state and no traffic will pass through the port.

Follow these guidelines for native VLAN tagging:

- The **no switchport trunk native vlan tag** command disables the native VLAN tagging operation on a port. This overrides the global tagging configuration.
- The **switchport trunk native vlan tag** command can be used to reenable tagging on a disabled port.
- The **no** option is saved to NVRAM so that the user does not have to manually select the ports to disable the tagging operation each time that the switch reboots.
- When the **switchport trunk native vlan tag** command is enabled and active, all packets on the native VLAN are tagged, and incoming untagged data packets are dropped. Untagged control packets are accepted.

Examples

This example shows how to cause a port interface that is configured as a switched interface to encapsulate in 802.1Q trunking format regardless of its default trunking format in trunking mode:

```
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)#
```

This example shows how to enable 802.1Q tagging on a port:

```
Switch(config-if)# switchport trunk native vlan tag
Switch(config-if)#
```

This example shows how to configure a secure MAC-address and a maximum limit of secure MAC addresses on Gigabit Ethernet port 1 for all VLANs:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 3
```

This example shows how to configure a secure MAC-address on Gigabit Ethernet port 1 in a specific VLAN or range of VLANs:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# vlan-range 2-6
Switch(config-if-vlan-range)# port-security maximum 3
```

This example shows how to configure a secure MAC-address in a VLAN on Gigabit Ethernet port 1:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# vlan-range 2-6
Switch(config-if-vlan-range)# port-security mac-address 1.1.1
Switch(config-if-vlan-range)# port-security mac-address sticky 1.1.2
Switch(config-if-vlan-range)# port-security mac-address sticky 1.1.3
```

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

Related Commands

show interfaces switchport

system mtu

To set the maximum Layer 2 or Layer 3 payload size, use the **system mtu** command. To revert to the default MTU setting, use the **no** form of this command.

system mtu *datagram-size*

no system mtu

Syntax Description

datagram-size	Layer 2 payload size; valid values from 1500 to 1552 bytes.

Defaults

The default MTU setting is 1500 bytes.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The *datagram-size* parameter specifies the Ethernet payload size, not the total Ethernet frame size, and the Layer 3 MTU is changed as a result of changing the **system mtu** command.

For ports from 3 to18 on model WS-X4418-GB and ports from 1 to 12 on model WS-X4412-2GB-TX, only the standard IEEE Ethernet payload size of 1500 bytes is supported.

For other modules, an Ethernet payload size of up to 1552 bytes is supported with a total Ethernet frame size of up to 1600 bytes.

Examples

This example shows how to set the MTU size to 1550 bytes:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# system mtu 1550
Switch(config)# end
Switch#
```

This example shows how to revert to the default MTU setting:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no system mtu
Switch(config)# end
Switch#
```

Related Commands

show interfaces
show system mtu

test cable-diagnostics tdr

To test the condition of copper cables on 48-port 10/100/1000 BASE-T modules, use the **test cable-diagnostics tdr** command.

test cable-diagnostics tdr {**interface** {*interface interface-number*}

Note This command will be deprecated in future Cisco IOS releases. Please use the **diagnostic start** command.

Syntax Description

interface *interface*	Interface type; valid values are **fastethernet** and **gigabitethernet**.
interface-number	Module and port number.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(25)SG	Support for this command on the Catalyst 4500 series switch.

Usage Guidelines

The TDR test is supported on Catalyst 4500 series switches running Cisco IOS Release 12.2(25)SG for the following line cards only:

- WS-X4548-GB-RJ45
- WS-X4548-GB-RJ45V
- WS-X4524-GB-RJ45V
- WS-X4013+TS
- WS-C4948
- WS-C4948-10GE

The valid values for **interface** *interface* are **fastethernet** and **gigabitethernet**.

Do not start the test at the same time on both ends of the cable. Starting the test at both ends of the cable at the same time can lead to false test results.

Do not change the port configuration during any cable diagnostics test. This action may result in incorrect test results.

The interface must be operating before starting the TDR test. If the port is down, the results of the test will be invalid. Issue the **no shutdown** command on the port.

Examples

This example shows how to start the TDR test on port 1 on module 2:

```
Switch# test cable-diagnostics tdr int gi2/1
Switch#
```

This example shows the message that displays when the TDR test is not supported on a module:

```
Switch# test cable-diagnostics tdr int gi2/1
00:03:15:%C4K_IOSDIAGMAN-4-TESTNOTSUPPORTEDONMODULE: Online cable
diag tdr test is not supported on this module
Switch#
```

Note The **show cable-diagnostic tdr** command is used to display the results of a TDR test. The test results will not be available until approximately 1 minute after the test starts. If you enter the **show cable-diagnostic tdr** command within 1 minute of the test starting, you may see a “TDR test is in progress on interface...” message.

Related Commands

show cable-diagnostics tdr

traceroute mac

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

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

Syntax Description

interface *interface-id*	(Optional) Specifies the source or destination switch interface.
source-mac-address	MAC address of the source switch in hexadecimal format.
destination-mac-address	MAC address of the destination switch in hexadecimal format.
vlan *vlan-id*	(Optional) Specifies the VLAN on which to trace the Layer 2 path that the packets take from the source switch to the destination switch; valid VLAN IDs are from 1 to 4094. Do not enter leading zeros.
detail	(Optional) Displays detail information.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(15)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Do not use leading zeros when entering a VLAN ID.

The Layer 2 traceroute feature is available on these switches:

- Catalyst 2950 switches running Release 12.1(12c)EA1 or later
- Catalyst 3550 switches running Release 12.1(12c)EA1 or later
- Catalyst 4500 series switches running Catalyst operating system Release 6.2 or later for the supervisor engine
- Catalyst 4500 series switches running Release 12.1(15)EW or later
- Catalyst 5000 family switches running Catalyst operating system Release 6.1 or later for the supervisor engine
- Catalyst 6500 series switches running Catalyst operating system Release 6.1 or later for the supervisor engine

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

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

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

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

Layer 2 traceroute 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 a message appears.

This feature is not supported in Token Ring VLANs.

Examples

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

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 (2.2.6.6) :Fa0/1 =>Fa0/3
con5                 (2.2.5.5        )  :    Fa0/3 =>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[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
Switch#
```

This example shows how to display the detailed Layer 2 path:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C2950G-24-EI / 2.2.6.6 :
        Fa0/1 [auto, auto] =>Fa0/3 [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.
Switch#
```

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

```
Switch# traceroute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source .....
Source 0000.0201.0501 found on con5[WS-C2950G-24-EI] (2.2.5.5)
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/1 [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.
Switch#
```

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.
Switch#
```

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.
Switch#
```

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
Switch#
```

This example shows the Layer 2 path when the 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.
Switch#
```

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

```
Switch# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 (2.2.6.6) :Fa0/1 =>Fa0/3
con5                 (2.2.5.5        )  :    Fa0/3 =>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[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
Switch#
```

Related Commands

traceroute mac ip

traceroute mac ip

To display the Layer 2 path that is taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname, use the **traceroute mac** command.

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

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The Layer 2 traceroute feature is available on these switches:

- Catalyst 2950 switches running Release 12.1(12c)EA1 or later
- Catalyst 3550 switches running Release 12.1(12c)EA1 or later
- Catalyst 4500 series switches running Catalyst operating system Release 6.2 or later for the supervisor engine
- Catalyst 4500 series switches running Release 12.1(15)EW or later
- Catalyst 5000 family switches running Catalyst operating system Release 6.1 or later for the supervisor engine
- Catalyst 6500 series switches running Catalyst operating system Release 6.1 or later for the supervisor engine

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

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

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

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 a message appears.

Layer 2 traceroute 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 / WS-C2950G-24-EI / 2.2.6.6 :
        Fa0/1 [auto, auto] =>Fa0/3 [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.
Switch#
```

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) :Fa0/1 =>Fa0/3
con5                (2.2.5.5        )  :    Fa0/3 =>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
Switch#
```

This example shows the Layer 2 path when Address Resolution Protocol (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.
Switch#
```

Related Commands

traceroute mac

trust

To define a trust state for traffic classified through the **class** policy-map configuration command, use the **trust** policy-map class configuration command. To return to the default setting, use the **no** form of this command.

trust [**cos** | **dscp**]

no trust [**cos** | **dscp**]

Syntax Description

cos	(Optional) Classify an ingress packet by using the packet class of service (CoS) value. For an untagged packet, the port default CoS value is used.
dscp	(Optional) Classify an ingress packet by using the packet Differentiated Services Code Point (DSCP) values (most significant 6 bits of 8-bit service-type field). For a non-IP packet, the packet CoS value is used if the packet is tagged. If the packet is untagged, the default port CoS value is used to map CoS to DSCP.

Defaults

The action is not trusted.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

Use this command to distinguish the quality of service (QoS) trust behavior for certain traffic from other traffic. For example, inbound traffic with certain DSCP values can be trusted. You can configure a class map to match and trust the DSCP values in the inbound traffic.

Trust values set with this command supersede trust values set with the **qos trust** interface configuration command.

If you specify **trust cos**, QoS uses the received or default port CoS value and the CoS-to-DSCP map to generate a DSCP value for the packet.

If you specify **trust dscp**, QoS uses the DSCP value from the ingress packet. For non-IP packets that are tagged, QoS uses the received CoS value; for non-IP packets that are untagged, QoS uses the default port CoS value. In either case, the DSCP value for the packet is derived from the CoS-to-DSCP map.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Examples

This example shows how to define a port trust state to trust inbound DSCP values for traffic classified with “class1”:

```
Switch# configure terminal
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch#
```

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

Related Commands

class
police
policy-map
set
show policy-map

tx-queue

To configure the transmit queue parameters for an interface, use the **tx-queue** command. To return to the default value, use the **no** form of this command.

tx-queue [*queue-id*] {**bandwidth** *bandwidth-rate* | **priority high** | **shape** *shape-rate*}

no tx-queue

Syntax Description

queue-id	(Optional) Number of the queue; valid values are from 1 to 4.
bandwidth *bandwidth-rate*	Specifies traffic bandwidth; valid values are from 16000 to 1000000000 bits per second.
priority high	Specifies high priority.
shape *shape-rate*	Specifies the maximum rate that packets are passed through a transmit queue; valid values are from 16000 to 1000000000 bits per second.

Defaults

The default settings are as follows:

- Encapsulation type is dependent on the platform or interface hardware.
- QoS enabled bandwidth rate is 4:255.
- QoS disabled bandwidth rate is 255:1.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

The bandwidth and shape rates cannot exceed the maximum speed of the interface.

The bandwidth can be configured only on the following:

- Uplink ports on Supervisor Engine III (WS-X4014)
- Ports on the WS-X4306-GB module
- The two 1000BASE-X ports on the WS-X4232-GB-RJ module
- The first two ports on the WS-X4418-GB module
- The two 1000BASE-X ports on the WS-X4412-2GB-TX module

Only transmit queue 3 can be configured to be a high-priority transmit queue.

Examples

This example shows how to allocate bandwidth on queue 1 to 100 Mbps:

```
Switch(config-if)# tx-queue 1
Switch(config-if-tx-queue)# bandwidth 1000000000
Switch(config-if-tx-queue)#
```

This example shows how to configure transmit queue 3 to the high priority:

```
Switch(config-if)# tx-queue 3
Switch(config-if-tx-queue)# priority high
Switch(config-if-tx-queue)#
```

This example shows how to configure the traffic shaping rate of 64 kbps to transmit queue 1:

```
Switch(config-if)# tx-queue 1
Switch(config-if-tx-queue)# shape 64000
Switch(config-if-tx-queue)#
```

Related Commands

show qos interface

udld (global configuration mode)

To enable aggressive or normal mode in the UDLD protocol and to set the configurable message timer time, use the **udld** command. Use the **no** form of this command to do the following:

- Disable normal mode UDLD on all the fiber ports by default
- Disable aggressive mode UDLD on all the fiber ports by default
- Disable the message timer

udld enable | aggressive

no udld enable | aggressive

udld message time *message-timer-time*

no udld message time

Syntax Description

enable	Enables UDLD in normal mode by default on all the fiber interfaces.
aggressive	Enables UDLD in aggressive mode by default on all the fiber interfaces.
message time *message-timer-time*	Sets the period of time between the UDLD probe messages on the ports that are in advertisement mode and are currently determined to be bidirectional; valid values are from 1to 90 seconds.

Defaults

All fiber interfaces are disabled and the message timer time equals 15 seconds.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

If you enable aggressive mode, once all the neighbors of a port have aged out either in the advertisement or in the detection phase, UDLD restarts the linkup sequence to try to resynchronize with any potentially out-of-sync neighbor and shuts down the port if the message train from the link is still undetermined.

This command affects the fiber interfaces only. Use the **udld (interface configuration mode)** command to enable UDLD on the other interface types.

Examples

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

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

Related Commands

show udld
udld (interface configuration mode)

udld (interface configuration mode)

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

udld {**enable** | **aggressive** | **disable**}

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

Syntax Description

enable	Enables UDLD on this interface.
aggressive	Enables UDLD in aggressive mode on this interface.
disable	Disables UDLD on this interface.

Defaults

The fiber interfaces are enabled per the state of the global **udld** (**enable** or **aggressive**) command, and the nonfiber interfaces are enabled with UDLD disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

If you enable aggressive mode, once all the neighbors of a port have aged out either in the advertisement or in the detection phase, UDLD restarts the linkup sequence to try to resynchronize with any potentially out-of-sync neighbor and shuts down the port if the message train from the link is still undetermined.

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

Use the **udld aggressive** command on the fiber ports to override the setting of the global **udld** (**enable** or **aggressive**) command. Use the **no** form on the fiber ports to remove this setting, return control of UDLD enabling back to the global **udld** command or to disable UDLD on the nonfiber ports.

The **disable** keyword is supported on the fiber ports only. Use the **no** form of this command to remove this setting and return control of UDLD to the **udld (global configuration mode)** command.

If the port changes from fiber to nonfiber or vice versa, all configurations will be maintained because of a change of module or a GBIC change detected by the platform software.

Examples

This example shows how to cause any port interface to enable UDLD, despite the current global **udld (global configuration mode)** setting:

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

This example shows how to cause any port interface to enable UDLD in aggressive mode, despite the current global **udld** (**enable** or **aggressive**) setting:

```
Switch (config-if)# udld aggressive
Switch (config-if)#
```

This example shows how to cause a fiber port interface to disable UDLD, despite the current global **udld (global configuration mode)** setting:

```
Switch (config-if)# udld disable
Switch (config-if)#
```

Related Commands

show udld
udld (global configuration mode)

udld reset

To reset all the UDLD ports in the shutdown state, use the **udld reset** command.

udld reset

Syntax Description

This command has no keywords or variables.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

If the interface configuration is still enabled for UDLD, these ports will begin to run UDLD again and may shut down if the reason for the shutdown has not been corrected.

The **udld reset** command permits the traffic to flow on the ports again; other features, such as spanning tree, PAgP, and DTP, operate normally if enabled.

Examples

This example shows how to reset all the ports that are shut down by UDLD:

```
Switch# udld reset
Switch#
```

Related Commands

show udld

unidirectional

To configure the nonblocking Gigabit Ethernet ports to unidirectionally send or receive traffic on an interface, use the **unidirectional** command. To disable unidirectional communication, use the **no** form of this command.

unidirectional {**receive-only** | **send-only**}

no unidirectional {**receive-only** | **send-only**}

Syntax Description

receive-only	Specifies the unidirectional reception.
send-only	Specifies the unidirectional transmission.

Defaults

Disabled

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Enabling port unidirectional mode automatically disables port UDLD. You must manually ensure that the unidirectional link does not create a spanning-tree loop in the network.

Examples

This example shows how to set Gigabit Ethernet interface 1/1 to receive traffic unidirectionally:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# unidirectional receive-only
Switch(config-if)# end
Switch#
```

Related Commands

show interfaces switchport

username

To establish a username-based authentication system, use the **username** command.

username *name* **secret** {**0** | **5**} *password*

Syntax Description

name	User ID of the user.
secret 0 | **5**	Specifies the authentication system for the user; valid values are **0** (text immediately following is not encrypted) and **5** (text immediately following is encrypted using an MD5-type encryption method).
password	Password of the user.

Defaults

No username-based authentication system is established.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Use this command to enable enhanced password security for the specified username. This command enables MD5 encryption on the password. MD5 encryption is a strong encryption method that is not retrievable. You cannot use MD5 encryption with protocols that require clear-text passwords, such as CHAP.

You can use this command for defining usernames that get special treatment. For example, you can define an “info” username that does not require a password but that connects the user to a general-purpose information service.

The **username** command provides both username and **secret** authentication for login purposes only.

The *name* argument can be only one word. White spaces and quotation marks are not allowed.

You can use multiple **username** commands to specify options for a single user.

For information about additional **username** commands, refer to the *Cisco IOS Command Reference*.

Examples

This example shows how to specify an MD5 encryption on a password (warrior) for a username (xena):

```
Switch(config)# username xena secret 5 warrior
Switch(config)#
```

Related Commands

enable password (refer to Cisco IOS documentation)
enable secret (refer to Cisco IOS documentation)
username (refer to Cisco IOS documentation)

verify

To verify the checksum of a file on a Flash memory file system, use the **verify** command.

verify [**/md5**] [*flash-filesystem***:**] [*filename*] [*expected-md5-signature*]

Syntax Description

/md5	(Optional) Verifies the MD5 signatures.
*flash-filesystem***:**	(Optional) Device where the Flash resides; valid values are **bootflash:**, **slot0:**, **flash:**, or **sup-bootflash:**.
filename	(Optional) Name of the Cisco IOS image.
expected-md5-signature	(Optional) MD5 signature.

Defaults

The current working device is specified.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Each software image that is distributed on the disk uses a single checksum for the entire image. This checksum is displayed only when the image is copied into the Flash memory.

The Readme file, which is included with the image on the disk, lists the name, file size, and checksum of the image. Review the contents of the Readme file before loading or duplicating the new image so that you can verify the checksum when you copy it into the Flash memory or on to a server.

Use the **verify /md5** command to verify the MD5 signature of a file before using it. This command validates the integrity of a copied file by comparing a precomputed MD5 signature with the signature that is computed by this command. If the two MD5 signatures match, the copied file is identical to the original file.

You can find the MD5 signature posted on the Cisco.com page with the image.

You can use the **verify /md5** command in one of the following ways:

- Verify the MD5 signatures manually by entering the **verify /md5** *filename* command.

  Check the displayed signature against the MD5 signature posted on the Cisco.com page.

- Allow the system to compare the MD5 signatures by entering the **verify /md5** {*flash-filesystem***:***filename*} {*expected-md5-signature*} command.

After completing the comparison, the system returns with a verified message. If an error is detected, the output is similar to the following:

```
Switch# verify /md5 slot0:c4-jsv-mz 0f
 ..................................
 ..................................
 ..................................
 ..................................
 ..................................
 ...............................Done!
 %Error verifying slot0:c4-jsv-mz
 Computed signature  = 0f369ed9e98756f179d4f29d6e7755d3
 Submitted signature = 0f
```

To display the contents of the Flash memory, enter the **show flash** command. The Flash contents listing does not include the checksum of the individual files. To recompute and verify the image checksum after the image has been copied into the Flash memory, enter the **verify** command.

A colon (:) is required after the specified device.

Examples

This example shows how to use the **verify** command:

```
Switch# verify cat6k_r47_1.cbi
..........................................................
File cat6k_r47_1.cbi verified OK.
Switch#
```

This example shows how to manually check the MD5 signature:

```
Switch# verify /md5 c4-jsv-mz
 .................................................
 .................................................
 .................................................
 .................................................
 .................................................
 ............................................Done!
 verify /md5 (slot0:c4-jsv-mz) = 0f369ed9e98756f179d4f29d6e7755d3
Switch#
```

This example shows how to allow the system to compare the MD5 signatures:

```
Switch# verify /md5 slot0:c4-jsv-mz 0f369ed9e98756f179d4f29d6e7755d3
 .................................................
 .................................................
 .................................................
 .................................................
 .................................................
 ............................................Done!
 verified /md5 (slot0:c6sup12-jsv-mz) = 0f369ed9e98756f179d4f29d6e7755d3
Switch#
```

Related Commands

show file system (Flash file system) (refer to Cisco IOS documentation)
show flash (refer to Cisco IOS documentation)

vlan (VLAN Database mode)

To configure a specific VLAN, use the **vlan** command. To delete a VLAN, use the **no** form of this command.

vlan *vlan_id* [**are** *hops*] [**backupcrf** *mode*] [**bridge** *type* | *bridge-num*] [**media** *type*] [**mtu** *mtu-size*] [**name** *vlan-name*] [**parent** *parent-vlan-id*] [**ring** *ring-number*] [**said** *said-value*] [**state** {**suspend** | **active**}] [**stp type** *type*] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]

no vlan *vlan*

Syntax Description

vlan_id	Number of the VLAN; valid values are from 1 to 4094.
are *hops*	(Optional) Specifies the maximum number of All Route Explorer hops for this VLAN; valid values are from 0 to 13. Zero is assumed if no value is specified.
backupcrf *mode*	(Optional) Enables or disables the backup CRF mode of the VLAN; valid values are **enable** and **disable**.
bridge *type*	(Optional) Specifies the bridging characteristics of the VLAN or identification number of the bridge; valid *type* values are **srb** and **srt**.
bridge_num	(Optional) Valid bridge_num values are from 0 to 15.
media *type*	(Optional) Specifies the media type of the VLAN; valid values are **fast ethernet**, **fd-net**, **fddi**, **trcrf**, and **trbrf**.
mtu *mtu-size*	(Optional) Specifies the maximum transmission unit (packet size, in bytes) that the VLAN can use; valid values are from 576 to 18190.
name *vlan-name*	(Optional) Defines a text string used as the name of the VLAN (1 to 32 characters).
parent *parent-vlan-id*	(Optional) Specifies the ID number of the parent VLAN of FDDI or Token Ring-type VLANs; valid values are from 2 to 1001.
ring *ring-number*	(Optional) Specifies the ring number of FDDI or Token Ring-type VLANs; valid values are from 2 to 1001.
said *said-value*	(Optional) Specifies the security association identifier; valid values are from 1 to 4294967294.
state	(Optional) Specifies the state of the VLAN.
suspend	Specifies that the state of the VLAN is suspended. VLANs in the suspended state do not pass packets.
active	Specifies that the state of the VLAN is active.
stp type *type*	(Optional) Specifies the STP type; valid values are **ieee**, **ibm**, and **auto**.
tb-vlan1 *tb-vlan1-id*	(Optional) Specifies the ID number of the first translational VLAN for this VLAN; valid values are from 2 to 1001. Zero is assumed if no value is specified.
tb-vlan2 *tb-vlan2-id*	(Optional) Specifies the ID number of the second translational VLAN for this VLAN; valid values are from 2 to 1001. Zero is assumed if no value is specified.

Defaults

The defaults are as follows:

- The vlan-name is “VLANxxxx” where “xxxx” represents four numeric digits (including leading zeroes) equal to the VLAN ID number.
- The media type is Fast Ethernet.
- The state is active.
- The said-value is 100,000 plus the VLAN ID number.
- The mtu-size default is dependent upon the VLAN type:
  - fddi—1500
  - trcrf—1500 if V2 is not enabled; 4472 if it is enabled
  - fd-net—1500
  - trbrf—1500 if V2 is not enabled; 4472 if it is enabled
- No ring number is specified.
- No bridge number is specified.
- No parent VLAN is specified.
- No STP type is specified.
- No translational bridge VLAN is specified.

Command Modes

VLAN configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

VLAN 1 parameters are factory configured and cannot be changed.

When you define *vlan-name*, the name must be unique within the administrative domain.

The SAID is documented in 802.10. When the **no** form is used, the VLANs SAID is returned to the default.

When you define the *said-value*, the name must be unique within the administrative domain.

The **bridge** *bridge-number* argument is used only for Token Ring-net and FDDI-net VLANs and is ignored in other types of VLANs. When the **no** form is used, the VLANs source-route bridging number returns to the default.

The parent VLAN resets to the default if the parent VLAN is deleted or the **media** keyword changes the VLAN type or the VLAN type of the parent VLAN.

The *tb-vlan1* and *tb-vlan2* are used to configure translational bridge VLANs of a specified type of VLAN and are not allowed in other types of VLANs. The translational bridge VLANs must be a different VLAN type than the affected VLAN; if two VLANs are specified, the two must be different VLAN types.

A translational bridge VLAN will reset to the default if the translational bridge VLAN is deleted or the **media** keyword changes the VLAN type or the VLAN type of the corresponding translational bridge VLAN.

Examples

This example shows how to add a new VLAN with all the default parameters to the new VLAN database:

```
Switch(vlan)# vlan 2
```

Note If the VLAN already exists, no action occurs.

This example shows how to cause the device to add a new VLAN, specify the media type and parent VLAN ID number 3, and set all the other parameters to the defaults:

```
Switch(vlan)# vlan 2 media fastethernet parent 3
VLAN 2 modified:
    Media type FASTETHERNET
    Parent VLAN 3
```

This example shows how to delete VLAN 2:

```
Switch(vlan)# no vlan 2
Switch(vlan)#
```

This example shows how to return the MTU to the default for its type and the translational bridging VLANs to the default:

```
Switch(vlan)# no vlan 2 mtu tb-vlan1 tb-vlan2
Switch(vlan)#
```

Related Commands

show vlan

vlan access-map

To enter VLAN access-map command mode to create a VLAN access map, use the **vlan access-map** command. To remove a mapping sequence or the entire map, use the **no** form of this command.

vlan access-map *name* [*seq#*]

no vlan access-map *name* [*seq#*]

Syntax Description

name	VLAN access-map tag.
seq#	(Optional) Map sequence number; valid values are from 0 to 65535.

Defaults

This command has no default settings.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

If you enter the sequence number of an existing map sequence, you enter VLAN access-map mode. If you do not specify a sequence number, a number is automatically assigned. You can enter one match clause and one action clause per map sequence. If you enter the **no vlan access-map name** [*seq#*] command without entering a sequence number, the whole map is removed. Once you enter VLAN access-map mode, the following commands are available:

- **action**—Sets the action to be taken (forward or drop).
- **default**—Returns a command to its default settings.
- **end**—Exits from configuration mode.
- **exit**—Exits from VLAN access-map configuration mode.
- **match**—Sets the values to match (IP address or MAC address).
- **no**—Negates a command or reset its defaults.

Examples

This example shows how to enter VLAN access-map mode:

```
Switch(config)# vlan access-map cisco
Switch(config-access-map)#
```

Related Commands

match
show vlan access-map

vlan configuration

To configure a service-policy on a VLAN, use the **vlan configuration** command to enter the VLAN feature configuration mode.

vlan configuration {*vlan*}

Syntax Description

vlan	Specifies a list of VLANs. "," "-" operators can be used; such as, 1-10,20.

Defaults

This command has no default settings.

Command Modes

Configuration mode

Command History

Release	Modification
12.2(40)SG	This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6E.

Usage Guidelines

Configuring of service-policies in this mode is supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

In Supervisor Engines V through 10GE and earlier, a service-policy has to attach to SVI to apply VLAN-based policies. Even though an SVI is not needed in all cases, such as when you use your Catalyst 4500 series switch as a pure Layer 2 switch, you are required to create an SVI.

To remove the requirement of creating an SVI, VLAN configuration mode is introduced on the Supervisor Engine 6-E and Catalyst 4900M chassis. With this command you can specify lists of VLANs and the input and output policies that are applied. To configure your system in this mode there is no requirement for you to create SVIs, or create VLAN or VTP mode interactions. Once the VLAN becomes active the configuration becomes active on that VLAN. You can use "-" or "," extensions to specifying VLAN list.

Examples

This example shows how to configure a service policy while in VLAN configuration mode and display the new service policy:

```
Switch#configure terminal
Switch(config)#vlan configuration 30-40
Switch(config-vlan-config)#service-policy input p1
Switch(config-vlan-config)#end
Switch#show running configuration | begin vlan configuration
!
vlan configuration 30-40
   service-policy input p1
!
vlan internal allocation policy ascending !
vlan 2-1000
!
Switch#
```

This example shows how to display the new service policy:

```
Switch#show policy-map vlan 30
vlan 30

  Service-policy input: p1

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets
      police:
         rate 128000 bps, burst 4000 bytes
          conformed 0 packets, 0 bytes; action:
            transmit
          exceeded 0 packets, 0 bytes; action:
            drop
          conformed 0 bps, exceeded 0 bps
Switch#
```

Related Commands

vlan (VLAN Database mode)
policy-map

vlan database

To enter VLAN configuration mode, use the **vlan database** command.

vlan database

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

From VLAN configuration mode, you can access the VLAN database editing buffer manipulation commands, including:

- **abort**—Exits mode without applying the changes.
- **apply**—Applies the current changes and bumps the revision number.
- **exit**—Applies the changes, bumps the revision number, and exits VLAN configuration mode.
- **no**—Negates a command or sets its defaults; valid values are **vlan** and **vtp**.
- **reset**—Abandons the current changes and rereads the current database.
- **show**—Displays the database information.
- **vlan**—Accesses the subcommands to add, delete, or modify values that are associated with a single VLAN. For information about the **vlan** subcommands, see the **vlan (VLAN Database mode)** command.
- **vtp**—Accesses the subcommands to perform VTP administrative functions. For information about the **vtp** subcommands, see the **vtp client** command.

Examples

This example shows how to enter VLAN configuration mode:

```
Switch# vlan database
Switch(vlan)#
```

This example shows how to exit VLAN configuration mode without applying changes after you are in VLAN configuration mode:

```
Switch(vlan)# abort
Aborting....
Switch#
```

This example shows how to delete a VLAN after you are in VLAN configuration mode:

```
Switch(vlan)# no vlan 100
Deleting VLAN 100...
Switch(vlan)#
```

This example shows how to turn off pruning after you are in VLAN configuration mode:

```
Switch(vlan)# no vtp pruning
Pruning switched OFF
Switch(vlan)#
```

Related Commands

show vlan

vlan dot1q tag native

To enable tagging of the native VLAN frames on all 802.1Q trunk ports, use the **vlan dot1q tag native command.** To disable tagging of native VLAN frames, use the **no** form of this command.

vlan dot1q tag native

no vlan dot1q tag native

Syntax Description

This command has no arguments or keywords.

Defaults

802.1Q native VLAN tagging is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(18)EW	This command was first introduced on the Catalyst 4500 series switch.

Usage Guidelines

When enabled, the native VLAN packets exiting all 802.1Q trunk ports are tagged unless the port is explicitly configured to disable native VLAN tagging.

When disabled, the native VLAN packets exiting all 802.1Q trunk ports are not tagged.

You can use this command with 802.1Q tunneling. This feature operates on an edge switch of a service-provider network and expands VLAN space by using a VLAN-in-VLAN hierarchy and by tagging the tagged packets. You must use the 802.1Q trunk ports for sending out the packets to the service-provider network. However, the packets going through the core of the service-provider network might also be carried on the 802.1Q trunks. If the native VLANs of an 802.1Q trunk match the native VLAN of a tunneling port on the same switch, the traffic on the native VLAN is not tagged on the sending trunk port. This command ensures that the native VLAN packets on all 802.1Q trunk ports are tagged.

Examples

This example shows how to enable 802.1Q tagging on the native VLAN frames and verify the configuration:

```
Switch# config terminal
Switch (config)# vlan dot1q tag native
Switch (config)# end
Switch# show vlan dot1q tag native
dot1q native vlan tagging is enabled
```

Related Commands

switchport private-vlan trunk native vlan tag
switchport trunk

vlan filter

To apply a VLAN access map, use the **vlan filter** command. To clear the VLAN access maps from VLANs or interfaces, use the **no** form of this command.

vlan filter *map-name* {**vlan-list** *vlan-list*}

no vlan filter *map-name* {**vlan-list** [*vlan-list*]}

Syntax Description

map-name	VLAN access-map tag.
vlan-list *vlan-list*	Specifies the VLAN list; see the "Usage Guidelines" section for valid values.

Defaults

This command has no default settings.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

When configuring an action clause in a VLAN access map, note the following:

- You can apply the VLAN access map to one or more VLANs.
- The *vlan-list* parameter can be a single VLAN ID, a list of VLAN IDs, or VLAN ID ranges (*vlan-id-vlan-id*). Multiple entries are separated by (-), (hyphen), or (,) (comma).
- You can apply only one VLAN access map to each VLAN.

When entering the **no** form of this command, the *vlan-list* parameter is optional (but the keyword **vlan-list** is required). If you do not enter the *vlan-list* parameter, the VACL is removed from all the VLANs where the *map-name* is applied.

Examples

This example shows how to apply a VLAN access map on VLANs 7 through 9:

```
Switch(config)# vlan filter ganymede vlan-list 7-9
Switch(config)#
```

vlan internal allocation policy

Use the **vlan internal allocation policy** command to configure the internal VLAN allocation scheme. To return to the default setting, use the **no** form of this command.

vlan internal allocation policy {**ascending** | **descending**}

no vlan internal allocation policy

Syntax Description

ascending	Specifies to allocate internal VLANs from 1006 to 4094.
descending	Specifies to allocate internal VLANs from 4094 to 1006.

Defaults

The default is the ascending allocation scheme.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

You can configure internal VLAN allocation to be from 1006 and up or from 4094 and down.

The internal VLANs and user-configured VLANs share the 1006 to 4094 VLAN spaces. A “first come, first served” policy is used in allocating these spaces.

The **vlan internal allocation policy** command allows you to configure the allocation direction of the internal VLAN.

During system bootup, the internal VLANs that are required for features in the startup-config file are allocated first. The user-configured VLANs in the startup-config file are configured next. If you configure a VLAN that conflicts with an existing internal VLAN, the VLAN that you configured is put into a nonoperational status until the internal VLAN is freed and becomes available.

After you enter the **write mem** command and the system reloads, the reconfigured allocation scheme is used by the port manager.

Examples

This example shows how to configure the VLANs in a descending order as the internal VLAN allocation policy:

```
Switch(config)# vlan internal allocation policy descending
Switch(config)#
```

Related Commands

show vlan internal usage

vmps reconfirm (global configuration)

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

vmps reconfirm *interval*

no vmps reconfirm

Syntax Description

interval	Queries to the VLAN Membership Policy Server (VMPS) to reconfirm dynamic VLAN assignments; valid values are from 1 to 120 minutes.

Defaults

The reconfirmation interval is 60 minutes.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

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

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

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

Related Commands

show vmps
vmps reconfirm (privileged EXEC)

vmps reconfirm (privileged EXEC)

To immediately send VLAN Query Protocol (VQP) queries to reconfirm allthe dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS), use the **vmps reconfirm** command.

vmps reconfirm

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

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

Examples

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

```
Switch# vmps reconfirm
Switch#
```

Related Commands

show vmps
vmps reconfirm (global configuration)

vmps retry

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

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; valid values are from 1 to 10.

Defaults

The retry count is 3.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

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

Examples

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

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

Related Commands

show vmps

vmps server

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

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

no vmps server *ipaddress*

Syntax Description

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

Defaults

No primary or secondary VMPS servers are defined.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(4)EA1	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The first server that you entered is automatically selected as the primary server whether or not **primary** is entered. You can override the first server address by using **primary** in a subsequent command.

If a member switch in a cluster configuration does not have an IP address, the cluster does not use the VMPS server that is configured for that member switch. Instead, the cluster uses the VMPS server on the command switch, and the command switch proxies the VMPS requests. The VMPS server treats the cluster as a single switch and uses the IP address of the command switch to respond to requests.

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 the packets from the new sources on these ports because it cannot query the VMPS.

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

Examples

This example shows how to configure the server with 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
Switch(config)#
```

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

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

Related Commands

show vmps

vtp (global configuration mode)

To modify the name of a VTP configuration storage file, use the **vtp** command. To clear a filename, use the **no** form of this command.

vtp {{**file** *filename*} | {**if-id** *name*}}

no vtp {{**file** *filename*} | {**if-id** *name*}}

Syntax Description

file *filename*	Specifies the IFS file where VTP configuration will be stored.
if-id *name*	Specifies the name of the interface providing the VTP updater ID for this device, where the **if-id** *name* is an ASCII string limited to 255 characters.

Defaults

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

You cannot use the **vtp file** command to load a new database. You can use it only to rename the file in which the existing database is stored.

You can use the **vtp if-id** command to specify the name of the interface providing the VTP updater ID for this device. The VTP updater is the device that adds, deletes, or modifies VLANs to a network, and triggers a VTP updater to inform the rest of the system of the changes.

Examples

This example shows how to specify the IFS file system file where VTP configuration is stored:

```
Switch(config)# vtp file vtpconfig
Setting device to store VLAN database at filename vtpconfig.
Switch(config)#
```

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

```
Switch(config)# vtp if-id fastethernet
Switch(config)#
```

Related Commands

show vtp

vtp client

To place a device in VTP client mode, use the **vtp client** command. To return to VTP server mode, use the **no** form of this command.

vtp client

no vtp client

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

VLAN configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. If you have switches in client mode, make sure to make all VTP or VLAN configuration changes on a switch in server mode.

The **vtp server** command is the functional equivalent of **no vtp client** except that it does not return an error if the device is not in client mode.

Examples

This example shows how to place the device in VTP client mode:

```
Switch(vlan-config)# vtp client
Switch(vlan-config)#
```

Related Commands

show vtp
vtp (global configuration mode)

vtp domain

To configure the administrative domain name for a device, use the **vtp domain** command.

vtp domain *domain-name*

Syntax Description

domain-name	Name of the domain.

Defaults

This command has no default settings.

Command Modes

VLAN configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

When you define the *domain-name*, the domain name is case sensitive and can be from 1 to 32 characters.

You must set a domain name before you can transmit any VTP advertisements.

Even if you do not set a domain name, the device will leave the no-management-domain state upon receiving the first VTP summary packet on any port that is currently trunking.

If the device receives its domain from a summary packet, it resets its configuration revision number to zero. Once the device leaves the no-management-domain state, it can never be configured to reenter the number except by cleaning NVRAM and reloading.

Examples

This example shows how to set the devices administrative domain:

```
Switch(vlan-config)# vtp domain DomainChandon
Switch(vlan-config)#
```

Related Commands

show vtp
vtp (global configuration mode)

vtp password

To create a VTP domain password, use the **vtp password** command. To delete the password, use the **no** form of this command.

vtp password *password-value*

no vtp password

Syntax Description

password-value	An ASCII string, from 1 to 32 characters, identifying the administrative domain for the device.

Defaults

Disabled

Command Modes

VLAN configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to create a VTP domain password:

```
Switch(vlan-config)# vtp password DomainChandon
Switch(vlan-config)#
```

This example shows how to delete the VTP domain password:

```
Switch(vlan-config)# no vtp password
Clearing device VLAN database password.
Switch(vlan-config)#
```

Related Commands

show vtp
vtp (global configuration mode)

vtp pruning

To enable pruning in the VLAN database, use the **vtp pruning** command. To disable pruning in the VLAN database, use the **no** form of this command.

vtp pruning

no vtp pruning

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

VLAN configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN.

Examples

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

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

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

```
Switch(vlan-config)# no vtp pruning
Pruning switched OFF
Switch(vlan-config)#
```

Related Commands

show vtp
vtp (global configuration mode)

vtp server

To place the device in VTP server mode, use the **vtp server** command.

vtp server

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

VLAN configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

If you make a change to the VTP or VLAN configuration on a switch in server mode, that change is propagated to all the switches in the same VTP domain.

You can set VTP to either server or client mode only when you disable dynamic VLAN creation.

If the receiving switch is in server mode, the configuration is not changed.

The **vtp server** command is the functional equivalent of **no vtp client**, except that it does not return an error if the device is not in client mode.

Examples

This example shows how to place the device in VTP server mode:

```
Switch(vlan-config)# vtp server
Switch(vlan-config)#
```

Related Commands

show vtp
vtp (global configuration mode)

vtp transparent

To place a device in VTP transparent mode, use the **vtp transparent** command. To return to VTP server mode, use the **no** form of this command.

vtp transparent

no vtp transparent

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

VLAN configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The **vtp transparent** command disables VTP from the domain but does not remove the domain from the switch.

If the receiving switch is in transparent mode, the configuration is not changed. The switches in transparent mode do not participate in VTP. If you make VTP or VLAN configuration changes on a switch in transparent mode, the changes are not propagated to the other switches in the network.

The **vtp server** command is similar to the **no vtp transparent** command, except that it does not return an error if the device is not in transparent mode.

Examples

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

```
Switch(vlan-config)# vtp transparent
Switch(vlan-config)#
```

This example shows how to return the device to VTP server mode:

```
Switch(vlan-config)# no vtp transparent
Switch(vlan-config)#
```

Related Commands

show vtp
vtp (global configuration mode)

vtp v2-mode

To enable version 2 mode, use the **vtp v2-mode** command. To disable version 2 mode, use the **no** form of this command.

vtp v2-mode

no vtp v2-mode

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

VLAN configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

All switches in a VTP domain must run the same version of VTP. VTP version 1 and VTP version 2 do not operate on switches in the same VTP domain.

If all switches in a domain are VTP version 2-capable, you only need to enable VTP version 2 on one switch; the version number is then propagated to the other version 2-capable switches in the VTP domain.

If you toggle the version 2 mode, the parameters of certain default VLANs will be modified.

Examples

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

```
Switch(vlan-config)# vtp v2-mode
Switch(vlan-config)#
```

This example shows how to disable version 2 mode in the VLAN database:

```
Switch(vlan-config)# no vtp v2-mode
Switch(vlan-config)#
```

Related Commands

show vtp
vtp (global configuration mode)