shutdown vlan

To shut down local traffic on a specified VLAN, use the **shutdown vlan** command. To restart local traffic on the VLAN, use the **no** form of this command.

shutdown vlan *vlan-id*

no shutdown vlan *vlan-id*

Syntax Description

vlan-id	VLAN number of the VLAN to be locally shut down; valid values are from 2 to 1001.

Command Default

This command has no default settings.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command does not support extended-range VLANs.

Examples

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

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

snmp ifindex clear

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

snmp ifindex clear

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

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.

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 that were previously entered for that specific interface.

When you clear the ifIndex configuration, the ifIndex persistence is enabled for all interfaces as specified by the **snmp-server ifindex persist** command in global configuration mode.

Examples

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

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

This example shows how to disable IfIndex persistence for Ethernet 0/1 only:

```
Router(config)# interface ethernet 0/1
Router(config-if)# no snmp ifindex persist
Router(config-if)# exit
```

This example shows how to clear the ifIndex configuration from the Ethernet 0/1 configuration:

```
Router(config)# interface ethernet 0/1
Router(config-if)# snmp ifindex clear
Router(config-if)# exit
```

Related Commands

Command	Description
snmp ifindex persist	Enables ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) only on a specific interface.
snmp-server ifindex persist	Enables ifIndex values globally so that they will remain constant across reboots for use by SNMP.

snmp ifindex persist

To enable ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) only 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.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

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** command in interface configuration mode 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** command in global configuration mode 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.

IfIndex commands that you configure for an interface apply to all subinterfaces on that interface.

Examples

This example shows how to enable ifIndex persistence for interface Ethernet 0/1 only:

```
Router(config)# interface ethernet 0/1
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 Ethernet 0/1 only:

```
Router(config)# snmp ifindex persist
Router(config)# interface ethernet 0/1
Router(config-if)# no snmp ifindex persist
Router(config-if)# exit
```

Related Commands

Command	Description
snmp ifindex clear	Clears any previously configured **snmp ifindex** commands that were issued for a specific interface.
snmp-server ifindex persist	Enables ifIndex values globally so that they remain constant across reboots for use by SNMP.

snmp-server enable traps

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

snmp-server enable traps [*notification-type*]

no snmp-server enable traps [*notification-type*]

Syntax Description

notification-type	(Optional) Type of notification (trap or inform) to enable or disable. If no type is specified, all notifications that are available on your device are enabled or disabled. See the "Usage Guidelines" section for valid values.

Command Default

This command is disabled by default. Most notification types are disabled. However, some notification types cannot be controlled with this command.

If you enter this command without a *notification-type*, all notification types that are controlled by this command are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

For additional notification types, refer to the *Cisco IOS Release 12.2 Command Reference*.

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.

If you do not enter an **snmp-server enable traps** command, no notifications that are controlled by this command are sent. To configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type that is related to that keyword is enabled. To enable multiple types of notifications, you must issue a separate **snmp-server enable traps** command for each notification type and notification option.

The **snmp-server enable traps** command is used 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.

The following list of MIBs are used for the traps:

- **chassis—**Controls the chassisAlarm traps from the CISCO-STACK-MIB
- **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
- **module—**Controls the SNMP-module traps from the CISCO-STACK-MIB
- **stpx—**Controls all the traps from the CISCO-STP-EXTENSIONS-MIB
- **vlancreate—**Controls the SNMP VLAN-created trap notifications
- **vlandelete—**Controls the SNMP VLAN-deleted trap notifications
- **vtp—**Controls the VTP traps from the CISCO-VTP-MIB

The following SNMP-server enable traps are supported:

- **bridge**—Controls the STP Bridge MIB traps
- **c6kxbar**—Controls the c6kxbar intbus-crcexcd intbus-crcrcvrd swbus trap
- **csg**—Controls the CSG agent quota database traps
- **flex-links**—Controls the flex-links status traps
- **mac-notification**—Controls the MAC-Notification move threshold traps
- **stpx**—Controls the STPX inconsistency root-inconsistency loop-inconsistency traps
- **vlan-mac-limit**—Controls the Layer 2 control VLAN MAC limit notifications traps

Examples

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

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

snmp-server enable traps transceiver type all

To enable all supported SNMP transceiver traps for all transceiver types, use the **snmp-server enable traps transceiver type all** command. To disable the transceiver SNMP trap notifications, use the **no** form of this command.

snmp-server enable traps transceiver type all

no snmp-server enable traps transceiver type all

Syntax Description

The command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **snmp-server enable traps** command is used 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.

Examples

This example shows how to enable all supported SNMP transceiver traps for all transceiver types:

```
Router(config)# snmp-server enable traps transceiver type all
Router(config)#
```

Related Commands

Command	Description
show interfaces transceiver	Displays information about the optical transceivers that have DOM enabled.

snmp-server ifindex persist

To enable ifIndex values globally so that they will remain constant across reboots for use by SNMP, use the **snmp-server ifindex persist** command. To disable ifIndex persistence globally, 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.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

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** command in global configuration mode does not override interface-specific configurations. To override the interface-specific configuration of ifIndex persistence, enter the [**no**] **snmp ifindex persist** and **snmp ifindex clear** commands in interface configuration mode.

Entering the [**no**] **snmp-server ifindex persist** command in global configuration mode 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
Router(config)#
```

Note This example shows that if ifIndex persistence was previously disabled for a specific interface using the **no snmp ifindex persist** command in interface configuration mode, ifIndex persistence remains disabled for that interface. The global ifIndex command does not override the interface-specific commands.

Related Commands

Command	Description
snmp ifindex clear	Clears any previously configured **snmp ifindex** commands that were issued for a specific interface.
snmp ifindex persist	Enables ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) only on a specific interface.

snmp-server source-interface

To specify the interface from which a SNMP trap originates the informs or traps, use the **snmp-server source-interface** command. To remove the source designation, use the **no** form of the comman

snmp-server source-interface {traps | informs} *interface*

no snmp-server source-interface {**traps | informs**} [*interface*]

Syntax Description

traps	Specifies SNMP traps.
informs	Specifies SNMP informs.
interface	Specifies the interface type and the module and port number of the source interface.

Command Default

No interface is designated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The source interface must have an IP address.

Enter the *interface* argument in the following format: *interface-type/module/port*.

An SNMP trap or inform sent from a Cisco SNMP server has a notification IP address of the interface it went out of at that time. Use this command to monitor notifications from a particular interface.

Examples

This example shows how to specify that the interface gigabitethernet5/2 is the source for all informs:

```
Router(config)# snmp-server source-interface informs gigabitethernet5/2
Router(config)#
```

This example shows how to specify that the interface gigabitethernet5/3 is the source for all traps:

```
Router(config)# snmp-server source-interface traps gigabitethernet5/3
Router(config)#
```

This example shows how to remove the source designation for all traps for a specific interface:

```
Router(config)# no snmp-server source-interface traps gigabitethernet5/3
Router(config)#
```

Related Commands

Command	Description
snmp-server trap-source interface	Specifies the interface from which a SNMP trap should originate. This command has been replaced by the **snmp-server source-interface** command.
snmp-server enable traps	Enables a router to send SNMP traps and informs.
snmp-server host	Specifies the recipient of a SNMP notification operation.

snmp-server trap authentication unknown-context

To enable the authorization failure traps during an unknown context error, use the **snmp-server trap authentication unknown-context** command. To disable the the authorization failure traps, use the **no** form of this command.

snmp-server trap authentication unknown-context

no snmp-server trap authentication unknown-context

Syntax Description

This command has no arguments or keywords.

Command Default

No authFail traps are generated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to enable the authorization failure traps during an unknown context error:

```
Router(config)# snmp-server trap authentication unknown-context
Router(config)#
```

This example shows how to disable the authorization failure traps during an unknown context error:

```
Router(config)# no snmp-server trap authentication unknown-context
Router(config)#
```

snmp-server trap link switchover

To enable sending a linkdown trap followed by a linkup trap for every interface in the switch during a switch failover, use the **snmp-server trap link switchover** command. To disable linkdown during a switch failover, use the **no** form of this command.

snmp-server trap link switchover

no snmp-server trap link switchover

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

By default, no link traps are generated during a switchover.

Examples

This example shows how to return to the default setting:

```
Router(config)# snmp-server trap link switchover
Router(config)#
```

This example shows how to disable linkdown followed by a linkup trap for every interface in the switch during a switch failover:

```
Router(config)# no snmp-server trap link switchover
Router(config)#
```

spanning-tree backbonefast

To enable BackboneFast on all Ethernet VLANs, 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.

Command Default

BackboneFast is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Enable BackboneFast on all Catalyst 6500 series switches to allow the detection of indirect link failures to start spanning-tree reconfiguration sooner.

Examples

This example shows how to enable BackboneFast on all Ethernet VLANs:

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

Related Commands

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

spanning-tree bpdufilter

To enable BPDU filtering on the 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.

Command Default

The setting that is already configured when you enter the **spanning-tree portfast bpdufilter default** command.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

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

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

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

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

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

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

Examples

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

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

Related Commands

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

spanning-tree bpduguard

To enable BPDU guard on the 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.

Command Default

The setting that is already configured when you enter the **spanning-tree portfast bpduguard default** command.

Command Default

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

spanning-tree cost

To set the path cost of the interface for STP calculations, use the **spanning-tree cost** command. To return to the default settings, use the **no** form of this command.

spanning-tree cost *cost*

no spanning-tree cost

Syntax Description

cost	Path cost; valid values are from 1 to 200000000.

Command Default

The default path cost is computed from the interface's bandwidth setting; the default path costs are as follows:

- Ethernet—100
- 16-Mb Token Ring—62
- FDDI—10
- FastEthernet—10
- ATM 155—6
- GigabitEthernet—1
- 10-Gigabit Ethernet—2
- HSSI—647

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

When you configure the *cost*, note that higher values indicate higher costs. This range applies regardless of the protocol type that is specified.

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:

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

Related Commands

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

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 error message, use the **no** form of this command.

spanning-tree etherchannel guard misconfig

no spanning-tree etherchannel guard misconfig

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

EtherChannel uses either PAgP or LACP and does not work if the EtherChannel mode of the interface has been enabled using the **channel-group** *group-number* **mode on** command.

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

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

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

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

Examples

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

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

Related Commands

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

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

spanning-tree extend system-id

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

spanning-tree extend system-id

no spanning-tree extend system-id

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled on systems that do not provide 1024 MAC addresses.

Command Default

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The Catalyst 6500 series switch can support 64 or up to 1024 MAC addresses. For a Catalyst 6500 series switch with 64 MAC addresses, STP uses the extended-system ID and a MAC address to make the bridge ID unique for each VLAN.

You cannot disable the extended-system ID on a Catalyst 6500 series switch that supports 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:

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

Related Commands

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

spanning-tree guard

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

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

no spanning-tree guard

Syntax Description

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

Command Default

Guard mode is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to enable root guard:

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

Related Commands

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

spanning-tree link-type

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

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

no spanning-tree link-type

Syntax Description

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

Command Default

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

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

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:

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

Related Commands

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

spanning-tree loopguard default

To enable loop guard as a default on all ports of a given bridge, use the **spanning-tree loopguard default** command. 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.

Command Default

Loop guard is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

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

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

The individual loop-guard port configuration overrides this command.

Examples

This example shows how to enable loop guard:

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

Related Commands

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

spanning-tree mode

To switch between PVST+, Rapid-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

Syntax Description

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

Command Default

pvst

Command Default

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

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

Examples

This example shows how to switch to MST mode:

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

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

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

Related Commands

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

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) Path cost for an instance; valid values are from 1 to 200000000.
port-priority *prio*	(Optional) Port priority for an instance; valid values are from 0 to 240 in increments of 16.

Command Default

The defaults are as follows:

- *cost* depends on the port speed; the faster interface speeds indicate smaller costs. MST always uses long path costs.
- *prio* is **128**.

Command Default

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

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

Higher **port-priority** *prio* values indicate smaller priorities.

Examples

This example shows how to set the interface path cost:

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

This example shows how to set the interface priority:

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

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree port-priority	Sets an interface priority when two bridges vie for position as the root bridge.

spanning-tree mst configuration

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

spanning-tree mst configuration

no spanning-tree mst configuration

Syntax Description

This command has no keywords or arguments.

Command Default

The default value for the MST configuration is the default value for all its parameters:

- 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 (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The MST configuration consists of three main parameters:

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

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

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

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

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

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

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

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

Examples

This example shows how to enter MST-configuration submode:

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

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

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

Related Commands

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

spanning-tree mst forward-time

To set the forward-delay timer for all the instances on the Catalyst 6500 series switch, 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 6500 series switch; valid values are from 4 to 30 seconds.

Command Default

seconds is **15**.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

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

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

Related Commands

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

spanning-tree mst hello-time

To set the hello-time delay timer for all the instances on the Catalyst 6500 series switch, 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 6500 series switch; valid values are from 1 to 10 seconds.

Command Default

2 seconds

Command Default

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

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:

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

Related Commands

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

spanning-tree mst max-age

To set the max-age timer for all the instances on the Catalyst 6500 series switch, 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 6500 series switch; valid values are from 6 to 40 seconds.

Command Default

20 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

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

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

Related Commands

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

spanning-tree mst max-hops

To specify the number of possible hops in the region before a 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 255 hops.

Command Default

20 hops

Command Default

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

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

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

Related Commands

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

spanning-tree mst pre-standard

To configure a port to transmit only prestandard BPDUs, use the **spanning-tree mst pre-standard** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst pre-standard

no spanning-tree mst pre-standard

Syntax Description

This command has no arguments or keywords.

Command Default

The default is to automatically detect prestandard neighbors.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

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

Prestandard BPDUs are based on the Cisco IOS MST implementation that was created before the IEEE standard was finalized. Standard BPDUs are based on the finalized IEEE standard.

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

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

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

Examples

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

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

Related Commands

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

spanning-tree mst root

To designate the primary and secondary root, set the bridge priority, and set the 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-time*]]

no spanning-tree mst root

Syntax Description

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

Command Default

The defaults are as follows:

- **spanning-tree mst root** has no default settings.
- *prio* is **32768**.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

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

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

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

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

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

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

Examples

This example shows how to set the bridge priority:

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

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

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

Related Commands

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

spanning-tree pathcost method

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

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

no spanning-tree pathcost method

Syntax Description

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

Command Default

short

Command Default

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command applies to all the spanning-tree instances on the Catalyst 6500 series switch.

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

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

Examples

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

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

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

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

Related Commands

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

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

spanning-tree portfast

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

no spanning-tree portfast

Syntax Description

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

Command Default

The settings that are configured by the **spanning-tree portfast default** command.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the Catalyst 6500 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 because 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 in the access mode.

- **no spanning-tree portfast**—This command implicitly enables PortFast if you define the **spanning-tree portfast default** command in global configuration mode 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:

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

Related Commands

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

spanning-tree portfast bpdufilter default

To enable 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.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

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

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

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

When enabled locally on a port, BPDU filtering prevents the Catalyst 6500 series switch from receiving or sending BPDUs on this port.

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

This example shows how to enable BPDU filtering by default:

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

Related Commands

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

spanning-tree portfast bpduguard default

To enable BPDU guard by default on all 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.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Caution Be careful when using this command. You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the Catalyst 6500 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:

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

Related Commands

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

spanning-tree portfast default

To enable PortFast by default on all access ports, use the **spanning-tree portfast default** command. To disable PortFast by 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.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Caution Be careful when using this command. You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the Catalyst 6500 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 enable PortFast by default on all access ports:

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

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree portfast (interface configuration mode)	Enables PortFast mode.

spanning-tree port-priority

To set an interface priority when two bridges vie for position as the root bridge, use the **spanning-tree port-priority** command. The priority you set breaks the tie. To return to the default settings, 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 2 to 255.

Command Default

port-priority is **128**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

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

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

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree mst	Sets the path cost and port-priority parameters for any MST instance (including the CIST with instance ID 0).
spanning-tree vlan	Configures STP on a per-VLAN basis.

spanning-tree transmit hold-count

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

spanning-tree transmit hold-count *value*

no spanning-tree transmit hold-count

Syntax Description

value	Number of BPDUs that can be sent before pausing for 1 second; valid values are from 1 to 20.

Command Default

value is **6**.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is supported on all spanning-tree modes.

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

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

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

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

Examples

This example shows how to specify the transmit hold count:

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

Related Commands

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

spanning-tree uplinkfast

To enable UplinkFast, 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.

Command Default

The defaults are as follows:

- UplinkFast is disabled.
- *packets-per-second* is 150 packets per second.

Command Default

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use this command only on access switches.

When you configure UplinkFast, the bridge priority is changed to 49152 so that this switch is not selected as root. All interface path costs of all spanning-tree interfaces that belong to the specified spanning-tree instances also increase by 3000.

When spanning tree detects that the root interface has failed, UplinkFast 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 that is 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 it is not already enabled) and change the rate at which update packets are sent. Use the **no** form of this command to return to the default rate.

Examples

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

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

Related Commands

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

spanning-tree vlan

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

spanning-tree vlan *vlan-id* [**forward-time** *seconds* | **hello-time** *hello-time* | **max-age** *seconds* | **priority** *priority* | **protocol** *protocol* | {**root** {**primary** | **secondary**} [**diameter** *net-diameter* [**hello-time** *hello-time*]]}]

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

Syntax Description

vlan-id	VLAN identification number; valid values are from 1 to 4094.
forward-time *seconds*	(Optional) Specifies the STP forward-delay time; valid values are from 4 to 30 seconds.
hello-time *hello-time*	(Optional) Specifies the number of seconds between the generation of configuration messages by the root switch; valid values are from 1 to 10 seconds.
max-age *seconds*	(Optional) Specifies the maximum number of seconds that the information in a BPDU is valid; valid values are from 6 to 40 seconds.
priority *priority*	(Optional) Specifies the STP-bridge priority; valid values are from 0 to 65535.
protocol *protocol*	(Optional) Specifies the STP; see the "Usage Guidelines" section for a list of valid values.
root primary	(Optional) Forces this switch to be the root bridge.
root secondary	(Optional) Forces this switch to be the root switch should the primary root fail.
diameter *net-diameter*	(Optional) Specifies the maximum number of bridges between any two points of attachment between end stations; valid values are from 2 through 7.

Command Default

The defaults are as follows:

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

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Caution When disabling spanning tree on a VLAN using the **no spanning-tree vlan** *vlan-id* command, ensure that all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the same VLAN because switches and bridges with spanning tree enabled have incomplete information about the physical topology of the network.

Caution We do not recommend disabling spanning tree, even in a topology that is free of physical loops. Spanning tree is a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.

When setting the **max-age** *seconds,* 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.

Valid values for *protocol* are **dec**—Digital STP, **ibm**—IBM STP, **ieee**—IEEE Ethernet STP, and **vlan-bridge**—VLAN Bridge STP.

The **spanning-tree root primary** alters this switch's 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 results.

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

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

Examples

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

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

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

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

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

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

Related Commands

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

speed

To set the port speed for an Ethernet interface, use the **speed** command. To disable a speed setting, use the **no** form of this command.

speed {**10** | **100** | **1000**}

speed auto [*speed-list*]

speed [**1000** | **nonegotiate**]

no speed

Syntax Description

10	Specifies the interface transmits at 10 Mbps.
100	Specifies the interface transmits at 100 Mbps.
1000	(Optional) Specifies the interface transmits at 1000 Mbps.
auto	Enables the autonegotiation capability.
speed-list	(Optional) Speed autonegotiation capability to a specific speed; see the "Usage Guidelines" section for valid values.
nonegotiate	(Optional) Enables or disables the link-negotiation protocol on the Gigabit Ethernet ports.

Command Default

See Table 2-93 for a list of default settings.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use the **speed** [**10** | **100**] command for 10/100 ports, the **speed auto** [**10 100** [**1000**]] command for 10/100/1000 ports, and the **speed** [**1000** | **nonegotiate**] command for Gigabit Ethernet ports.

Separate the *speed-list* entries with a space.

The following *speed-list* configurations are supported:

- **speed auto**—Negotiate all speeds.
- **speed auto 10 100**—Negotiate 10 and 100 speeds only.
- **speed auto 10 100 1000**—Negotiate all speeds.

When you enable link negotiation, the speed, duplex, flow control, and clocking negotiations between two Gigabit Ethernet ports are automatically enabled.

Table 2-93 lists the supported command options by interface.

Table 2-93 Supported speed Command Options

Interface Type	Supported Syntax	Default Setting	Usage Guidelines
10/100-Mbps module	**speed** [**10** | **100**] **speed auto** [**10** | **100**]	**auto**	If the speed is set to **auto**, you cannot set **duplex**. If the speed is set to **10** or **100**, and you do not configure the duplex setting, the duplex is set to **half.**
10/100/1000-Mbps interface	**speed auto** [{**10 100**} [**1000**]]	**auto**	If the speed is set to **auto**, you cannot set **duplex**. If the speed is set to **10** or **100**, and you do not configure the duplex setting, the duplex is set to **half** by default. If the speed is set to **10 100**, the interface is not forced to half duplex by default.
100-Mbps fiber modules	Factory set	Not applicable.	
Gigabit Ethernet module	**speed** [**1000** | **nonegotiate**]	Speed is 1000 or negotiation is enabled.	Speed, duplex, flow control, and clocking negotiations are enabled.
10-Mbps ports	Factory set	Not applicable.	

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

If you set the Ethernet interface speed to **auto** on a 10/100-Mbps or 10/100/1000-Mbps Ethernet interface, both speed and duplex are autonegotiated.

The Gigabit Ethernet interfaces are full duplex only. You cannot change the duplex mode on the Gigabit Ethernet interfaces or on a 10/100/1000-Mbps interface that is configured for Gigabit Ethernet.

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

Note Catalyst 6500 series switches cannot automatically negotiate interface speed and duplex mode if either connecting interface is configured to a value other than **auto**.

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

You cannot set the duplex mode to **half** when the port speed is set at 1000 and similarly, you cannot set the port speed to **1000** when the mode is set to half duplex. In addition, if the port speed is set to **auto**, the **duplex** command is rejected.

Table 2-94 describes the relationship between the **duplex** and **speed** commands.

Table 2-94 Relationship Between duplex and speed Commands

duplex Command	speed Command	Resulting System Action
duplex half or **duplex full**	**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 configure the interface to transmit at 100 Mbps:

```
Router(config-if)# speed 100
Router(config-if)#
```

Related Commands

Command	Description
duplex	Configures the duplex operation on an interface.
interface	Selects an interface to configure and enters interface configuration mode.
show interfaces	Displays traffic that is seen by a specific interface.

squeeze

To delete flash files permanently by squeezing a flash file system, use the **squeeze** command.

squeeze *filesystem***:**

Syntax Description

*filesystem***:**	Flash file system; valid values are **bootflash:** and **flash:**.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

When flash memory is full, you might need to rearrange the files so that the space that is used by the files that are marked "deleted" can be reclaimed.

When you enter the **squeeze** command, the router copies all valid files to the beginning of flash memory and erases all files that are marked "deleted." You cannot recover "deleted" files and you can write to the reclaimed flash-memory space.

In addition to removing deleted files, use the **squeeze** command to remove any files that the system has marked as "error." An error file is created when a file write fails (for example, the device is full). To remove error files, you must use the **squeeze** command. The squeeze operation might take as long as several minutes because it can involve erasing and rewriting almost an entire flash-memory space.

The colon is required when entering the *filesystem*.

Examples

This example shows how to permanently erase the files that are marked "deleted" from the flash memory:

```
Router # squeeze flash:
Router #
```

Related Commands

Command	Description
delete	Deletes a file from a flash memory device or NVRAM.
dir	Displays a list of files on a file system.
undelete	Recovers a file that is marked "deleted" on a flash file system.

stack-mib portname

To specify a name string for a port, use the **stack-mib portname** command.

stack-mib portname *portname*

Syntax Description

portname	Name for a port.

Command Default

This command has no default settings.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Using the **stack-mib** command to set a name string to a port corresponds to the portName MIB object in the portTable of CISCO-STACK-MIB. portName is the MIB object in the portTable of CISCO-STACK-MIB. You can set this object to be descriptive text describing the function of the interface.

Examples

This example shows how to set a name to a port:

```
Router(config-if)# stack-mib portname portal_to_paradise
Router(config-if)#
```

standby delay minimum reload

To configure the delay period before the initialization of HSRP groups, use the **standby delay minimum reload** command. To disable the delay period, use the **no** form of this command.

standby delay minimum [*min-delay*] **reload** [*reload-delay*]

no standby delay minimum [*min-delay*] **reload** [*reload-delay*]

Syntax Description

min-delay	(Optional) Minimum time, in seconds, to delay HSRP-group initialization after an interface comes up. This minimum delay applies to all subsequent interface events.
reload-delay	(Optional) Time, in seconds, to delay after the router has reloaded. This delay applies only to the first interface-up event after the router has reloaded.

Command Default

The defaults are as follows:

- *min-delay* is **1** second.
- *reload-delay* is **5** seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

If the active router fails or is removed from the network, the standby router automatically becomes the new active router. If the former active router comes back online, you can control whether it takes over as the active router by using the **standby preempt** command.

However, even if the **standby preempt** command is not configured, the former active router resumes the active role after it reloads and comes back online. Use the **standby delay minimum reload** command to set a delay period for HSRP-group initialization. This command allows time for the packets to get through before the router resumes the active role.

We recommend that you use the **standby delay minimum reload** command if the **standby timers** command is configured in milliseconds or if HSRP is configured on a VLAN interface of a switch.

In most configurations, the default values provide sufficient time for the packets to get through, and it is not necessary to configure longer delay values.

The delay is canceled if an HSRP packet is received on an interface.

Examples

This example shows how to set the minimum delay to 30 seconds and the delay after the first reload to 120 seconds:

```
Router(config-if) # standby delay minimum 30 reload 120
Router(config-if) #
```

Related Commands

Command	Description
show standby delay	Displays HSRP information about the delay periods.
standby preempt	Configures HSRP preemption and preemption delay.
standby timers	Configures the time between hello packets and the time before other routers declare the active Hot Standby or standby router to be down.

standby track

To configure an interface so that the Hot Standby-priority changes are based on the availability of other interfaces, use the **standby track** command. To delete all tracking configuration for a group, use the **no** form of this command.

standby [*group-number*] **track** {*interface-type interface-number* | **designated-router**} [*priority-decrement*]

no standby *group-number* **track**

Syntax Description

group-number	(Optional) Group number on the interface to which the tracking applies; valid values are from 0 to 255.
interface-type interface-number	Interface type and number to be tracked.
designated-router	Specifies that if the designated router becomes nondesignated, the active HSRP router becomes the designated router.
priority-decrement	(Optional) Amount that the Hot Standby priority for the router is decremented (or incremented) when the interface goes down (or comes back up); valid values are from 1 to 255.

Command Default

The defaults are as follows:

- The *group* is **0**.
- The *priority-decrement* is **10**.
- The **designated-router** keyword is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Prior to entering the **designated-router** keyword, you must ensure that the new designated router has a higher HSRP priority than the current designated router to take over.

When a tracked interface goes down, the Hot Standby priority decreases by the number that is specified by the *priority-decrement* argument. If an interface is not tracked, its state changes do not affect the Hot Standby priority. For each interface that is configured for Hot Standby, you can configure a separate list of interfaces to be tracked.

When multiple tracked interfaces are down, the decrements are cumulative whether they are configured with *priority-decrement* values or not.

A tracked interface is considered down if the IP address is disabled on that interface.

You must enter the *group-number* when using the **no** form of this command.

If you configure HSRP to track an interface, and that interface is physically removed as in the case of an OIR operation, then HSRP regards the interface as always down. You cannot remove the HSRP interface-tracking configuration. To prevent this situation, use the **no standby track** *interface-type interface-number* command before you physically remove the interface.

When you enter a *group-number* **0**, no group number is written to NVRAM, providing backward compatibility.

Examples

This example shows how to enable HSRP tracking for group 1 on an interface:

```
Router(config-if)# standby 1 track Ethernet0/2
Router(config-if)#
```

This example shows how to specify that if the designated router becomes nondesignated, the active HSRP router becomes the designated router:

```
Router(config-if)# standby 1 track designated-router 15
Router(config-if)#
```

Related Commands

Command	Description
show standby	Displays HSRP information.

standby use-bia

To configure the HSRP to use the burned-in address of the interface as its virtual MAC address instead of the preassigned MAC address (on Ethernet and FDDI) or the functional address (on Token Ring), use the **standby use-bia** command. To return to the default virtual MAC address, use the **no** form of this command.

standby use-bia [**scope interface**]

no standby use-bia

Syntax Description

scope interface	(Optional) Configures this command for the subinterface on which it was entered instead of the major interface.

Command Default

HSRP uses the preassigned MAC address on Ethernet and FDDI or the functional address on Token Ring.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is not supported on Catalyst 6500 series switches that are configured with a PFC2.

The PFC2 supports a maximum of 16 unique HSRP-group numbers. You can use the same HSRP-group numbers in different VLANs. If you configure more than 16 HSRP groups, this restriction prevents use of the VLAN number as the HSRP-group number.

Note Identically numbered HSRP groups use the same virtual MAC address, which might cause errors if you configure bridge groups.

Hardware Layer 3 switching supports the following ingress and egress encapsulations:

- Ethernet V2.0 (ARPA)
- 802.3 with 802.2 with 1 byte control (SAP1)
- 802.3 with 802.2 and SNAP

Hardware Layer 3 switching is permanently enabled. No configuration is required.

Examples

This example shows how to configure the HSRP to use the burned-in address of the interface as the virtual MAC address that is mapped to the virtual IP address:

```
Router(config-if) # standby use-bia
Router(config-if) #
```

storm-control level

To set the suppression level, use the **storm-control level** command. To turn off the suppression mode, use the **no** form of this command.

storm-control {**broadcast** | **multicast** | **unicast**} **level** *level*[**.***level*]

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

Syntax Description

broadcast	Specifies the broadcast traffic.
multicast	Specifies the multicast traffic.
unicast	Specifies the unicast traffic.
level	Integer-suppression level; valid values are from 0 to 100 percent.
.*level*	(Optional) Fractional-suppression level; valid values are from 0 to 99.

Command Default

All packets are passed.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You can enter this command on switch ports and router ports.

Enter the **storm-control level** command to enable traffic storm control on the interface, configure the traffic storm-control level, and apply the traffic storm-control level to all traffic storm-control modes that are enabled on the interface.

Only one suppression level is shared by all three suppression modes. For example, if you set the broadcast level to 30 and set the multicast level to 40, both levels are enabled and set to 40.

The Catalyst 6500 series switch supports storm control for multicast and unicast traffic only on Gigabit and 10-Gigabit Ethernet LAN ports. The switch supports storm control for broadcast traffic on all LAN ports.

The **multicast** and **unicast** keywords are supported on Gigabit and 10-Gigabit Ethernet LAN ports only. Unicast and multicast suppression is also supported on the WS-X6148A-RJ-45 and the WS-X6148-SFP modules.

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 means that no limit is placed on traffic. A threshold value of 0 or 0.0 (fractional) percent means that all specified traffic is blocked on a port, with the following guidelines:

- A fractional level value of 0.33 or lower is the same as 0.0 on the following modules:
  - WS-X6704-10GE
  - WS-X6748-SFP
  - WS-X6724-SFP
  - WS-X6748-GE-TX
- Enter 0 on all other modules to block all specified traffic on a port.

Enter the **show interfaces counters broadcast** 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 *level* to 100 percent for the specified traffic type.
- Use the **no** form of this command.

Examples

This example shows how to enable and set the suppression level:

```
Router(config-if)# storm-control broadcast level 30
Router(config-if)#
```

This example shows how to disable the suppression mode:

```
Router(config-if)# no storm-control multicast level
Router(config-if)#
```

Related Commands

Command	Description
show interfaces counters	Displays the traffic that the physical interface sees.
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

switchport

To modify the switching characteristics of the Layer 2-switched interface, use the **switchport** command (without parameters).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). Use the **switchport** commands (with parameters) to configure the switching characteristics.

switchport

switchport {**host** | **nonegotiate**}

no switchport

no switchport nonegotiate

Syntax Description

host	Optimizes the port configuration for a host connection.
nonegotiate	Specifies that the device will not engage in a negotiation protocol on this interface.

Command Default

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

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

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 additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

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

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

Because spanning-tree PortFast is enabled, you should enter the **switchport host** command only on ports that are connected to a single host. Connecting other Catalyst 6500 series switches, hubs, concentrators, switches, and bridges to a fast-start port can cause temporary spanning-tree loops.

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

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

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

You must force a port to trunk before you can configure it as a SPAN-destination port. Use the **switchport nonegotiate** command to force the port to trunk.

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:

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

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.

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

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

This example shows how to cause a port interface that has already been configured as a switched interface to refrain from negotiating trunking mode and act as a trunk or access port (depending on the **mode** set):

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

Related Commands

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

switchport access vlan

To set the VLAN when the 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*

no switchport access vlan

Syntax Description

vlan-id	VLAN to set when the interface is in access mode; valid values are from 1 to 4094.

Command Default

The defaults are as follows:

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

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

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 entered the **switchport** command for the interface.

Entering the **no switchport** command shuts down the port and then reenables it. This action may 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.

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:

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

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.

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 in the interface-configuration mode:

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

Related Commands

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

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.

Command Default

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

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

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.

A VLAN interface configured on the PISA is considered up if there are ports forwarding in the associated VLAN. When all ports on a VLAN are down or blocking, the VLAN interface on the PISA is considered down. For the VLAN interface to be considered up, all the ports in the VLAN need to be up and forwarding. You can enter the **switchport autostate exclude** command to exclude a port from the VLAN interface link-up calculation.

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:

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

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

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

Related Commands

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

switchport backup

To configure an interface as a Flexlink backup interface, use the **switchport backup** command. To disable Flexlink, use the **no** form of this command.

switchport backup interface *interface-type interface-number*

no switchport backup interface *interface-type interface-number*

Syntax Description

interface *interface-type interface-number*	Specifies the interface type and the module and port number to configure as a Flexlink backup interface.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

When you enable Flexlink, both the active and the standby links are up physically and mutual backup is provided.

Flexlink is supported on Layer 2 interfaces only and does not support routed ports.

Flexlink does not switch back to the original active interface after recovery.

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

Flexlink is designed for simple access topologies (two uplinks from a leaf node). You must ensure that there are no loops from the wiring closet to the distribution/core network to enable Flexlink to perform correctly.

Flexlink converges faster for directly connected link failures only. Any other network failure has no improvement with Flexlink fast convergence.

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.

Examples

This example shows how to enable Flexlink on an interface:

```
Router(config-if)# switchport backup interface fastethernet 4/1
Router(config-if)#
```

This example shows how to disable Flexlink on an interface:

```
Router(config-if)# switchport backup interface fastethernet 4/1
Router(config-if)#
```

Related Commands

Command	Description
show interfaces switchport backup	Displays Flexlink pairs.

switchport block unicast

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

switchport block unicast

no switchport block unicast

Syntax Description

This command has no arguments or keywords.

Command Default

The default settings are as follows:

- Unknown unicast traffic is not blocked.
- All traffic with unknown MAC addresses is sent to all ports.

Command Default

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

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

Blocking the unknown 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 *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

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

Examples

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

```
Router(config-if)# switchport block unicast
Router(config-if)#
```

Related Commands

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

switchport capture

To configure the port to capture VACL-filtered traffic, use the **switchport capture** command. To disable the capture mode on the port, use the **no** form of this command.

switchport capture

no switchport capture

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

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

The VACL capture function for the NAM is supported on the Supervisor Engine 720 but is not supported with the IDSM-2.

The **switchport capture** command applies only to Layer 2-switched interfaces.

WAN interfaces support only the capture functionality of VACLs.

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

Entering the **switchport capture** command sets the capture function on the interface so that the packets with the capture bit set are received by the interface.

There is no restriction on the order that you enter the **switchport capture** and **switchport capture allowed vlan** commands. The port does not become a capture port until you enter the **switchport capture** (with no arguments) command.

The capture port must allow the destination VLANs of the captured packets. Once you enable a capture port, the packets are allowed from all VLANs by default, the capture port is on longer in the originally configured mode, and the capture mode enters monitor mode. In monitor mode, the capture port does the following:

- Does not belong to any VLANs that it was in previously.
- Does not allow incoming traffic.

- Preserves the encapsulation on the capture port if you enable the capture port from a trunk port and the trunking encapsulation was ISL or 802.1Q. The captured packets are encapsulated with the corresponding encapsulation type. If you enable the capture port from an access port, the captured packets are not encapsulated.
- When you enter the **no switchport capture** command to disable the capture function, the port returns to the previously configured mode (access or trunk).
- Packets are captured only if the destination VLAN is allowed on the capture port.

Examples

This example shows how to configure an interface to capture VACL-filtered traffic:

```
Router(config-if)# switchport capture
Router(config-if)#
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport capture allowed vlan	Specifies the destination VLANs of the VACL-filtered traffic.

switchport capture allowed vlan

To specify the destination VLANs of the VACL-filtered traffic, use the **switchport capture allowed vlan** command. To clear the configured-destination VLAN list and return to the default settings, use the **no** form of this command.

switchport capture allowed vlan {**add** | **all** | **except** | **remove**} *vlan-id* [**,***vlan-id*[**,***vlan-id*[**,**...]]

no switchport capture allowed vlan

Syntax Description

add	Adds the specified VLANs to the current list.
all	Adds all VLANs to the current list.
except	Adds all VLANs except the ones that are specified.
remove	Removes the specified VLANs from the current list.
vlan-id	VLAN IDs of the allowed VLANs when this port is in capture mode; valid values are from 1 to 4094.

Command Default

all

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

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

The **switchport capture allowed vlan** command applies only to Layer 2-switched interfaces.

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

You can enter the *vlan-id* as a single VLAN, a group of VLANs, or both. For example, you would enter **switchport capture allowed vlan 1-1000, 2000, 3000-3100**.

There is no restriction on the order that you enter the **switchport capture** and **switchport capture allowed vlan** commands. The port does not become a capture port until you enter the **switchport capture** (with no arguments) command.

WAN interfaces support only the capture functionality of VACLs.

Examples

This example shows how to add the specified VLAN to capture VACL-filtered traffic:

```
Router(config-if)# switchport capture allowed vlan add 100
Router(config-if)#
```

Related Commands

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

switchport dot1q ethertype

To specify the EtherType value to be programmed on the interface, use the **switchport dot1q ethertype** command. To return to the default settings, use the **no** form of this command.

switchport dot1q ethertype *value*

Syntax Description

value	EtherType value for 802.1Q encapsulation; valid values are from 0x600 to 0xFFFF.

Command Default

The *value* is 0x8100.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You can configure a custom EtherType-field value on trunk ports and on access ports.

Each port supports only one EtherType-field value. A port that is configured with a custom EtherType-field value does not recognize frames that have any other EtherType-field value as tagged frames.

Caution A port that is configured with a custom EtherType-field value considers frames that have any other EtherType-field value to be untagged frames. A trunk port that is configured with a custom EtherType-field value puts frames that are tagged with any other EtherType-field value into the native VLAN. An access port or tunnel port that is configured with a custom EtherType-field value puts frames that are tagged with any other EtherType-field value into the access VLAN.

You can configure a custom EtherType-field value on the following modules:

- Supervisor engines
- WS-X6516A-GBIC
- WS-X6516-GBIC

Note The WS-X6516A-GBIC and WS-X6516-GBIC modules apply a configured custom EtherType-field value to all ports that are supported by each port ASIC (1 through 8 and 9 through 16).

- WS-X6516-GE-TX

You cannot configure a custom EtherType-field value on the ports in an EtherChannel.

You cannot form an EtherChannel from ports that are configured with custom EtherType-field values.

Examples

This example shows how to set the EtherType value to be programmed on the interface:

```
Router (config-if)# switchport dot1q ethertype 1234
Router (config-if)#
```

Related Commands

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

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** | **trunk** | {**dynamic** {**auto** | **desirable**}} | **dot1q-tunnel**}

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

no switchport mode

no switchport mode private-vlan

Syntax Description

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

Command Default

The defaults are as follows:

- The mode is dependent on the platform; it should either be **dynamic auto** for platforms that are intended for wiring closets or **dynamic desirable** for platforms that are intended as backbone switches.
- No mode is set for PVLAN ports.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

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 agree to 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 agree to 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 configure a port as a promiscuous or host-PVLAN port and one of the following applies, the port becomes inactive:

- The port does not have a valid PVLAN association or mapping configured.
- The port is a SPAN destination.

If you delete a private-port PVLAN association or mapping, or if you configure a private port as a SPAN destination, the deleted private-port PVLAN association or mapping or the private port that is configured as a SPAN destination becomes inactive.

If you enter **dot1q-tunnel** mode, BPDU filtering is enabled and CDP is disabled on protocol-tunneled interfaces.

Examples

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

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

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

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

This example shows how to set a port to PVLAN-promiscuous mode:

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

Related Commands

Command	Description
show dot1q-tunnel	Displays a list of 802.1Q tunnel-enabled ports.
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport	Modifies the switching characteristics of the Layer 2-switched interface.
switchport private-vlan host-association	Modifies the switching characteristics of the Layer 2-switched interface.
switchport private-vlan mapping	Defines the PVLAN mapping for a promiscuous port.

switchport port-security

To enable port security on an interface, use the **switchport port-security** command. To disable port security, use the **no** form of this command.

switchport port-security

no switchport port-security

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Follow these guidelines when configuring port security:

- Port security is supported on trunks.
- Port security is supported on 802.1Q tunnel ports.
- A secure port cannot be a destination port for a Switch Port Analyzer (SPAN).
- A secure port cannot belong to an EtherChannel.
- A secure port cannot be a trunk port.
- 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.

Examples

This example shows how to enable port security:

```
Router(config-if)# switchport port-security
Router(config-if)#
```

This example shows how to disable port security:

```
Router(config-if)# no switchport port-security
Router(config-if)#
```

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.

switchport port-security aging

To configure the port security aging, use the **switchport port-security aging** command. To disable aging, use the **no** form of this command.

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

Syntax Description

time *time*	Sets the duration for which all addresses are secured; valid values are from 1 to 1440 minutes.
type	Specifies the type of aging.
absolute	Specifies absolute aging; see the "Usage Guidelines" section for more information.
inactivity	Specifies that the timer starts to run only when there is no traffic; see the "Usage Guidelines" section for more information.

Command Default

The defaults are as follows:

- Disabled
- If enabled, the defaults are as follows:
  - *time* is 0.
  - **type** is **absolute**.

Command Default

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Follow these guidelines when configuring port security:

- Port security is supported on trunks.
- Port security is supported on 802.1Q tunnel ports.
- You can apply one of two types of aging for automatically learned addresses on a secure port:
- Absolute aging times out the MAC address after the age-time has been exceeded, regardless of the traffic pattern. This default is for any secured port, and the age-time is set to 0.
- Inactivity aging times out the MAC address only after the age_time of inactivity from the corresponding host has been exceeded.

Examples

This example shows how to set the aging time as 2 hours:

```
Router(config-if)# switchport port-security aging time 120
Router(config-if)#
```

This example shows how to set the aging time as 2 minutes:

```
Router(config-if)# switchport port-security aging time 2
Router(config-if)#
```

This example shows how to set the aging type on a port to absolute aging:

```
Router(config-if) switchport port-security aging type absolute
Router(config-if)#
```

This example shows how to set the aging type on a port to inactivity:

```
Router(config-if) switchport port-security aging type inactivity
Router(config-if)#
```

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.

switchport port-security mac-address

To add a media access control (MAC) address to the list of secure MAC addresses, use the **switchport port-security mac-address** command. To remove a MAC address from the list of secure MAC addresses, use the **no** form of this command.

switchport port-security mac-address {*mac-addr* | {**sticky** [*mac-addr*]} [**vlan** *vlan* | *vlan-list* | {**voice** | **access**}]}

no switchport port-security mac-address {*mac-addr* | {**sticky** [*mac-addr*]} [**vlan** *vlan* | *vlan-list* | {**voice** | **access**}]}

Syntax Description

mac-addr	MAC addresses for the interface; valid values are from 1 to 1024.
sticky	Configures the dynamic MAC addresses as sticky on an interface.
vlan *vlan* | *vlan-list*	(Optional) Specifies a VLAN or range of VLANs; see the "Usage Guidelines" section for additional information.
access	(Optional) Configures the MAC address in the access VLAN.
voice	(Optional) Configures the MAC address in the voice VLAN.

Defaults

This command has no default settings.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.
12.2(18)ZYA1	The **access** and **voice** keywords were added.

Usage Guidelines

If you configure fewer secure MAC addresses than the maximum number of secure MAC addresses on all interfaces, the remaining MAC addresses are dynamically learned.

To clear multiple MAC addresses, you must enter the **no** form of this command once for each MAC address to be cleared.

The *vlan-list* argument is visible only if the port has been configured and is operational as a trunk. Enter the **switchport mode trunk** command and then enter the **switchport nonegotiate** command.

The **sticky** keyword configures the dynamic MAC addresses as sticky on an interface. Sticky MAC addresses configure the static Layer 2 entry to stay sticky to a particular interface. This feature can prevent MAC moves or prevent the entry from being learned on a different interface.

You can configure the sticky feature even when the port security feature is not enabled on the interface. It becomes operational once port security is enabled on the interface.

Note You can enter the **switchport port-security mac-address sticky** command only if sticky is enabled on the interface.

When port security is enabled, disabling the sticky feature causes all configured and learned sticky addresses to be deleted from the configuration and converted into dynamic secure addresses.

When port security is disabled, disabling the sticky feature causes all configured and learned sticky addresses to be deleted from the configuration.

The **access** and **voice** keywords are introduced in Cisco IOS Release 12.2(18)ZYA1, and are only available if the port has been configured and is operational as an access port.

Examples

This example shows how to configure a secure MAC address:

```
Router(config-if)# switchport port-security mac-address 1000.2000.3000
```

This example shows how to delete a secure MAC address from the address table:

```
Router(config-if)# no switchport port-security mac-address 1000.2000.3000
```

This example shows how to configure a secure MAC address in the voice VLAN in Cisco IOS Release 12.2(18)ZYA1:

```
Router(config-if)# switchport port-security mac-address 1000.2000.3000 vlan voice
```

This example shows how to enable the sticky feature on an interface:

```
Router(config-if)# switchport port-security mac-address sticky
```

This example shows how to disable the sticky feature on an interface:

```
Router(config-if)# no switchport port-security mac-address sticky
```

This example shows how to make a specific MAC address as a sticky address:

```
Router(config-if)# switchport port-security mac-address sticky 0000.0000.0001
```

This example shows how to delete a specific sticky address:

```
Router(config-if)# no switchport port-security mac-address sticky 0000.0000.0001
```

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

```
Router(config-if)# no switchport port-security mac-address
```

Related Commands

Command	Description
clear port-security	Deletes configured secure MAC addresses and sticky MAC addresses from the MAC address table.
show port-security	Displays information about the port-security setting.
switchport mode trunk	Configures the port as a trunk member.
switchport nonegotiate	Configures the LAN port into permanent trunking mode.

switchport port-security maximum

To set the maximum number of secure MAC addresses on a port, use the **switchport port-security maximum** command. To return to the default settings, use the **no** form of this command.

switchport port-security maximum *maximum* [**vlan** *vlan* | *vlan-list*]

no switchport port-security maximum

Syntax Description

maximum	Maximum number of secure MAC addresses for the interface; valid values are from 1 to 4097.
vlan *vlan* | *vlan-list*	(Optional) Specifies a VLAN or range of VLANs; see the "Usage Guidelines" section for additional information.

Command Default

vlan is **1**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

If you enter this command more than once, subsequent use of this command overrides the previous value of *maximum*. If the new *maximum* argument is larger than the current number of the secured addresses on this port, there is no effect except to increase the value of the *maximum*.

If the new *maximum* is smaller than the old *maximum* and there are more secure addresses on the old *maximum*, the command is rejected.

If you configure fewer secure MAC addresses than the maximum number of secure MAC addresses on the port, the remaining MAC addresses are dynamically learned.

Once the maximum number of secure MAC addresses for the port is reached, no more addresses are learned on that port even if the per-VLAN port maximum is different from the aggregate maximum number.

You can override the maximum number of secure MAC addresses for the port for a specific VLAN or VLANs by entering the **switchport port-security maximum** *maximum* **vlan** *vlan* | *vlan-list* command.

The *vlan-list* argument allows you to enter ranges, commas, and delimited entries such as 1,7,9-15,17.

The *vlan-list* argument is visible only if the port has been configured and is operational as a trunk. Enter the **switchport mode trunk** command and then enter the **switchport nonegotiate** command.

Examples

This example shows how to set the maximum number of secure MAC addresses that are allowed on this port:

```
Router(config-if)# switchport port-security maximum 5
```

```
Router(config-if)#
```

This command shows how to override the maximum set for a specific VLAN:

```
Router(config-if)# switchport port-security maximum 3 vlan 102
Router(config-if)#
```

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.

switchport port-security violation

To set the action to be taken when a security violation is detected, use the **switchport port-security violation** command. To return to the default settings, use the **no** form of this command.

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

Syntax Description

shutdown	Shuts down the port if there is a security violation.
restrict	Drops all the packets from the insecure hosts at the port-security process level and increments the security-violation count.
protect	Drops all the packets from the insecure hosts at the port-security process level but does not increment the security-violation count.

Command Default

shutdown

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Port-security violations occur because of the following reasons:

- If the number of source MAC addresses seen on an interface is more than the port-security limit.
- If a source MAC address secured on one port appears on another secure port. The violation occurs in this situation because in restrict/protect mode the software is hit by the violation traffic. The software can be protected from this condition by using **mls rate-limit layer2 port-security** command.

When a security violation is detected, one of the following actions occurs:

- Protect—When the number of port-secure MAC addresses reaches the maximum limit that is allowed on the port, the packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses.
- Restrict—A port-security violation restricts data and causes the security-violation counter to increment.
- Shutdown—The interface is error disabled when a security violation occurs.

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

Examples

This example shows how to set the action to be taken when a security violation is detected:

```
Router(config-if)# switchport port-security violation restrict
Router(config-if)#
```

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.

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

Command Default

No PVLAN is configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

There is no run-time effect on the port unless it is in PVLAN-host mode. If the port is in PVLAN-host mode but neither of the VLANs 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):

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

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

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

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport mode	Sets the interface type for this command.

switchport private-vlan mapping

To define the PVLAN mapping for a promiscuous port, use the **switchport private-vlan mapping** command. To clear all mappings 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*}

no switchport private-vlan mapping

Syntax Description

primary-vlan-id	Number of the primary VLAN of the PVLAN relationship; valid values are from 1 to 4094.
secondary-vlan-id	Number of the secondary VLAN of the private VLAN relationship; valid values are from 1 to 4094.
add	Maps the secondary VLANs to the primary VLAN.
remove	Clears mapping between the secondary VLANs and the primary VLAN.

Command Default

No PVLAN mappings are configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

There is no run-time effect on the port unless it is in PVLAN-promiscuous mode. If the port is in PVLAN-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.

Examples

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

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

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

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

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

```
Router(config-if)# no switchport private-vlan mapping
Router(config-if)#
```

Related Commands

Command	Description
show interfaces private-vlan mapping	Displays the information about the PVLAN mapping for VLAN SVIs.

switchport trunk

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

switchport trunk encapsulation {**isl** | {**dot1q** [**ethertype** *value*]} | **negotiate**}

switchport trunk native vlan *vlan-id*

switchport trunk allowed vlan *vlan-list*

switchport trunk pruning vlan *vlan-list*

no switchport trunk {**encapsulation** {**isl** | **dot1q** | **negotiate**}} | {**native vlan**} | {**allowed vlan**} | {**pruning vlan**}

Syntax Description

encapsulation isl	Sets the trunk-encapsulation format to ISL.
encapsulation dot1q	Sets the switch port-encapsulation format to 802.1Q.
ethertype *value*	Sets the EtherType value; valid values are from 0x0 to 0x5EF-0xFFFF.
encapsulation negotiate	Specifies that if DISL and DTP negotiations do not resolve the encapsulation format, then ISL is the selected format.
native vlan *vlan-id*	Sets the native VLAN for the trunk in 802.1Q trunking mode; valid values are from 1 to 4094.
allowed vlan *vlan-list*	Allowed VLANs that transmit this interface in tagged format when in trunking mode; valid values are from 1 to 4094.
pruning vlan *vlan-list*	List of VLANs that are enabled for VTP pruning when in trunking mode; valid values are from 1 to 4094.

Command Default

The defaults are as follows:

- The encapsulation type is dependent on the platform or interface hardware.
- The access VLAN and trunk-interface native VLAN are default VLANs that correspond to the platform or interface hardware.
- All VLAN lists include all VLANs.
- **ethertype** *value* for 802.1Q encapsulation is 0x8100.

Command Default

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is not supported on GE Layer 2 WAN ports.

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 **switchport trunk encapsulation isl** command on a port channel containing an interface that does not support ISL-trunk encapsulation, the command is rejected.

You can enter the **switchport trunk allowed vlan** command on interfaces where the span destination port is either a trunk or an access port.

Note The **switchport trunk pruning vlan** *vlan-list* command does not support extended-range VLANs; valid *vlan-list* values are from 1 to 1005.

The **dot1q ethertype** *value* keyword and argument are not supported on port-channel interfaces. You can enter the command on the individual port interface only. Also, you can configure the ports in a channel group to have different EtherType configurations.

Caution Be careful when configuring the custom EtherType value on a port. If you enter the **negotiate** keywords and DISL and DTP negotiation do not resolve the encapsulation format, then ISL is the selected format and may pose as a security risk. 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.

The **no** form of the **dot1q ethertype** *value* command resets the list to the default value.

The *vlan-list* format is **all | none | add | remove | except** *vlan-list*[*,vlan-list...*] and is described as follows:

- **all** specifies all the appropriate VLANs. This keyword is not supported in the **switchport trunk pruning vlan** command.
- **none** indicates an empty list. This keyword is not supported in the **switchport trunk allowed vlan** command.
- **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. You can remove VLAN 1. If you remove VLAN 1 from a trunk, the trunk interface continues to send and receive management traffic (for example, CDP3, VTP, PAgP4, and DTP) in VLAN 1.

  Note You can remove any of the default VLANs (1002 to 1005) from a trunk; this action is not allowed in earlier releases.

- **except** lists the VLANs that should be calculated by inverting the defined list of VLANs.
- *vlan-list* is either a single VLAN number from 1 to 4094 or a continuous range of VLANs that are described by two VLAN numbers. The smaller number is first, separated by a hyphen that represents the VLAN IDs of the allowed VLANs when this port is in trunking mode.

Do not enable the reserved VLAN range (1006 to 1024) on trunks when connecting a Catalyst 6500 series switch running the Cisco IOS software on both the supervisor engine and the PISA to a Catalyst 6500 series switch running the Catalyst operating system. These VLANs are reserved in Catalyst 6500 series switches running the Catalyst operating system. If enabled, Catalyst 6500 series switches running the Catalyst operating system may error disable the ports if there is a trunking channel between these systems.

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:

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

Related Commands

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

switchport vlan mapping

To map the traffic arriving on the VLAN *original-vlan-id* to the VLAN *translated-vlan-id* and the traffic that is internally tagged with the VLAN *translated-vlan-id* with the VLAN *original-vlan-id* before leaving the port, use the **switchport vlan mapping** command. To clear the mapping between a pair of VLANs or clear all the mappings that are configured on the switch port, use the **no** form of this command.

switchport vlan mapping *original-vlan-id translated-vlan-id*

no switchport vlan mapping {{*original-vlan-id translated-vlan-id*} | **all**}

Syntax Description

original-vlan-id	Original VLAN number; valid values are from 1 to 4094.
translated-vlan-id	Translated VLAN number; valid values are from 1 to 4094.
all	Clears all the mappings that are configured on the switch port.

Command Default

No mappings are configured on any switch port.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is not supported on GE Layer 2 WAN ports.

You must enable VLAN translation on the port where you want VLAN translation to work. Use the **switchport vlan mapping enable** command to enable VLAN translation.

Do not remove the VLAN that you are translating from the trunk. When you map VLANs, make sure that both VLANs are allowed on the trunk that carries the traffic.

Table 2-95 lists the VLAN translation, the type of VLAN translation support, the number of ports that you can configure per port group, and the trunk type for each module that supports VLAN translation.

Table 2-95 Modules that Support VLAN Translation

Product Number	VLAN Translation Support Type	Number of Port Groups	Port Ranges per Port Group	Translations per Port Group	VLAN Translation Trunk-Type Support
WS-SUP720	Per port group	1	1-2	32	802.1Q
WS-X6501-10GEX4	Per port	1	1 port in 1 group	32	802.1Q
WS-X6502-10GE	Per port	1	1 port in 1 group	32	802.1Q
WS-X6516A-GBIC	Per port group	2	1-8, 9-16	32	802.1Q
WS-X6516-GBIC	Per port group	2	1-8, 9-16	32	802.1Q
WS-X6516-GE-TX	Per port group	2	1-8, 9-16	32	802.1Q

Table 2-95 Modules that Support VLAN Translation (continued)

Product Number	VLAN Translation Support Type	Number of Port Groups	Port Ranges per Port Group	Translations per Port Group	VLAN Translation Trunk-Type Support
WS-X6524-100FX-MM	Per port group	1	1-24	32	ISL and 802.1Q
WS-X6548-RJ-45	Per port group	1	1-48	32	ISL and 802.1Q
WS-X6548-RJ-21	Per port group	1	1-48	32	ISL and 802.1Q

The mapping that you configured using the **switchport vlan mapping** command does not become effective until the switch port becomes an operational trunk port.

The VLAN mapping that is configured on a port may apply to all the other ports on the same ASIC. In some cases, a mapping that is configured on one of the ports on an ASIC can overwrite a mapping that is already configured on another port on the same ASIC.

The port VLAN mapping is applied to all the ports on a port ASIC if that ASIC does not support per-port VLAN mapping.

If you configure VLAN mapping on the port ASIC that is a router port, the port-VLAN mapping does not take effect until the port becomes a switch port.

You can map any two VLANs regardless of the trunk types carrying the VLANs.

Examples

This example shows how to map the original VLAN to the translated VLAN:

```
Router(config-if)# switchport vlan mapping 100 201
Router(config-if)#
```

This example shows how to clear the mappings that are between a pair of VLANs:

```
Router(config-if)# no switchport vlan mapping 100 201
Router(config-if)#
```

This example shows how to clear all the mappings that are configured on the switch port:

```
Router(config-if)# no switchport vlan mapping 100 201
Router(config-if)#
```

Related Commands

Command	Description
show interfaces vlan mapping	Displays the status of a VLAN mapping on a port.
show vlan mapping	Registers a mapping of an 802.1Q VLAN to an ISL VLAN.
switchport vlan mapping enable	Enables VLAN mapping per switch port.

switchport vlan mapping enable

To enable VLAN mapping per switch port, use the **switchport vlan mapping enable** command. To disable VLAN mapping per switch port, use the **no** form of this command.

switchport vlan mapping enable

no switchport vlan mapping enable

Command Default VLAN mapping is disabled on all switch ports.

Command Default Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Note You must enter the **switchport vlan mapping enable** command on the port where you want the mapping to take place.

See Table 2-95 for a list of modules that support this command.

The **switchport vlan mapping enable** command enables or disables VLAN-mapping lookup in the hardware regardless of whether the mapping is configured by the global VLAN mapping command or the switchport VLAN mapping command.

This command is useful on the hardware that supports VLAN mapping per ASIC only because you can turn on or off VLAN translation selectively on ports that are connected to the same port ASIC.

Examples This example shows how to enable VLAN mapping per switch port:

```
Router(config-if)# switchport vlan mapping enable
Router(config-if)#
```

This example shows how to disable VLAN mapping per switch port:

```
Router(config-if)# no switchport vlan mapping enable
Router(config-if)#
```

Related Commands

Command	Description
show interfaces vlan mapping	Displays the status of a VLAN mapping on a port.
show vlan mapping	Registers a mapping of an 802.1Q VLAN to an ISL VLAN.
switchport vlan mapping	Maps the traffic arriving on the VLAN *original-vlan-id* to the VLAN *translated-vlan-id* and the traffic that is internally tagged with the VLAN *translated-vlan-id* with the VLAN *original-vlan-id* before leaving the port.

switchport voice vlan

To configure a voice VLAN on a multiple-VLAN access port, use the **switchport voice vlan** command. To remove the voice VLAN from the switch port, use the **no** form of this command.

switchport voice vlan {**dot1p** | **none** | **untagged** | *vvid*}

no switchport voice vlan

Syntax Description

dot1p	Sends CDP packets that configure the IP phone to transmit voice traffic in the default VLAN in 802.1p frames that are tagged with a Layer 2 CoS value.
none	Allows the IP phone to use its own configuration and transmit untagged voice traffic in the default VLAN.
untagged	Sends CDP packets that configure the IP phone to transmit untagged voice traffic in the default VLAN.
vvid	Voice VLAN identifier; valid values are from 1 to 4094. Sends CDP packets that configure the IP phone to transmit voice traffic in the voice VLAN in 802.1Q frames that are tagged with a Layer 2 CoS value.

Command Modes

none

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The default Layer 2 CoS is 5. The default Layer 3 IP-precedence value is 5.

This command does not create a voice VLAN. You can create a voice VLAN in VLAN-configuration mode by entering the **vlan (global configuration mode)** command. If you configure both the native VLAN and the voice VLAN in the VLAN database and set the switch port to multiple-VLAN access mode, this command brings up the switch port as operational.

If you enter **dot1p**, the switch port is enabled to receive 802.1p packets only.

If you enter **none**, the switch port does not send CDP packets with VVID TLVs.

If you enter **untagged**, the switch port is enabled to receive untagged packets only.

If you enter *vvid*, the switch port receives packets that are tagged with the specified *vvid*.

Examples

This example shows how to create an operational multiple-VLAN access port:

```
Router(config-if)# switchport
Router(config-if)# switchport mode access
```

```
Router(config-if)# switchport access vlan 100
Router(config-if)# switchport voice vlan 101
Router(config-if)
```

This example shows how to change the multiple-VLAN access port to a normal access port:

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# no switchport voice vlan
Router(config-if)
```

Related Commands

Command	Description
switchport access vlan	Sets the VLAN when the interface is in access mode.
switchport mode	Sets the interface type.

sync-restart-delay

To set the synchronization-restart delay timer to ensure accurate status reporting, use the **sync-restart-delay** command.

sync-restart-delay *timer*

Syntax Description

timer	Interval between status-register resets; valid values are from 200 to 60000 milliseconds.

Command Default

timer is **210** milliseconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is supported on Gigabit Ethernet fiber ports only.

The status register records the current status of the link partner.

Examples

This example shows how to set the Gigabit Ethernet synchronization-restart delay timer:

```
Router(config-if)# sync-restart-delay 2000
Router(config-if)#
```

Related Commands

Command	Description
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

system flowcontrol bus

To set the FIFO overflow error count, use the **system flowcontrol bus** command. To return to the original FIFO threshold settings, use the **no** form of this command.

[**default**] **system flowcontrol bus** {**auto** | **on**}

no system flowcontrol bus

Syntax Description

default	(Optional) Specifies the default settings.
auto	Monitors the FIFO overflow error count and sends a warning message if the FIFO overflow error count exceeds a configured error threshold in 5-second intervals.
on	(Optional) Specifies the original FIFO threshold settings.

Command Default

auto

Command Default

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Note We recommend that you leave the system flow control in auto mode and use the other modes under the advice of Cisco TAC only.

Examples

This example shows how to monitor the FIFO overflow error count and send a warning message if the FIFO overflow error count exceeds a configured error threshold in 5-second intervals:

```
Router(config)# system flowcontrol bus auto
Router(config)#
```

This example shows how to specify the original FIFO threshold settings:

```
Router(config)# system flowcontrol bus on
Router(config)#
```

system jumbomtu

To set the maximum size of the Layer 2 and Layer 3 packets, use the **system jumbomtu** command. To revert to the default MTU setting, use the **no** form of this command.

system jumbomtu *mtu-size*

no system jumbomtu

Syntax Description

mtu-size	Maximum size of the Layer 2 and Layer 3 packets; valid values are from 1500 to 9216 bytes.

Command Default

mtu-size is **9216** bytes.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The *mtu-size* parameter specifies the Ethernet packet size, not the total Ethernet frame size. The Layer 3 MTU is changed as a result of entering the **system jumbomtu** command.

The **system jumbomtu** command enables the global MTU for port ASICs. On a port ASIC after jumbo frames are enabled, the port ASIC accepts any size packet on the ingress side and checks the outgoing packets on the egress side. The packets on the egress side that exceed the global MTU are dropped by the port ASIC.

For example, if you have port A in VLAN 1 and Port B in VLAN 2, and if VLAN 1 and VLAN 2 are configured for **mtu 9216** and you enter the **system jumbomtu 4000** command, the packets that are larger than 4000 bytes are not transmitted out because Ports B and A drop packets that are larger than 4000 bytes.

Examples

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

```
Router(config)# system jumbomtu 1550
Router(config)# end
Router#
```

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

```
Router(config)# no system jumbomtu
Router(config)#
```

Related Commands

Command	Description
mtu	Adjusts the maximum packet size or MTU size.
show interfaces	Displays traffic that is seen by a specific interface.
show system jumbomtu	Displays the global MTU setting.

tcam priority

To prioritize the interfaces that are forwarded to the software in the event of TCAM entry or label exhaustion, use the **tcam priority** command.

tcam priority {**high** | **normal** | **low**}

Syntax Description

high	Sets priority to high.
normal	Sets priority to normal.
low	Sets priority to low.

Command Default

normal

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The interfaces are chosen in this order:

1. Low-priority interfaces without VACLs and without multicast
2. Low-priority interfaces without VACLs and approved by multicast
3. Low-priority interfaces with VACLs and approved by multicast
4. Low-priority interfaces (not approved by multicast)
5. Normal-priority interfaces without VACLs and without multicast
6. Normal-priority interfaces without VACLs and approved by multicast
7. Normal-priority interfaces with VACLs and approved by multicast
8. Normal-priority interfaces (not approved by multicast)
9. High-priority interfaces without VACLs and without multicast
10. High-priority interfaces without VACLs and approved by multicast
11. High-priority interfaces with VACLs and approved by multicast
12. High-priority interfaces (not approved by multicast)

Examples

This example shows how to set the priority:

```
Router(config-if)# tcam priority low
Router(config-if)#
```

Related Commands

Command	Description
show tcam interface	Displays information about the interface-based TCAM.

test cable-diagnostics

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

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

Syntax Description

tdr	Activates the TDR test for copper cables on 48-port 10/100/1000 BASE-T modules.
interface *interface*	Specifies the interface type; see the "Usage Guidelines" section for valid values.
interface-number	Module and port number.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Cable diagnostics can help you detect whether your cable has connectivity problems.

The TDR test guidelines are as follows:

- TDR can test cables up to a maximum length of 115 meters.
- See the Release Notes for Cisco IOS Release 12.2 ZY for the list of the modules that support TDR.
- 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 up before running the TDR test. If the port is down, the **test cable-diagnostics tdr** command is rejected and the following message is displayed:

```
Router# test cable-diagnostics tdr interface gigabitethernet2/12
% Interface Gi2/12 is administratively down
% Use 'no shutdown' to enable interface before TDR test start.
```

- If the port speed is 1000 and the link is up, do not disable the auto-MDIX feature.
- For fixed 10/100 ports, before running the TDR test, disable auto-MDIX on both sides of the cable. Failure to do so can lead to misleading results.

- For all other conditions, you must disable the auto-MDIX feature on both ends of the cable (use the **no mdix auto** command). Failure to disable auto-MDIX will interfere with the TDR test and generate false results.
- If a link partner has auto-MDIX enabled, this action will interfere with the TDR-cable diagnostics test and test results will be misleading. The workaround is to disable auto-MDIX on the link partner.
- If you change the port speed from 1000 to 10/100, enter the **no mdix auto** command before running the TDR test. Note that entering the **speed 1000** command enables auto-MDIX regardless of whether the **no mdix auto** command has been run.

Examples

This example shows how to run the TDR-cable diagnostics:

```
Router # test cable-diagnostics tdr interface gigabitethernet2/1
TDR test started on interface Gi2/1
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
Router #
```

Related Commands

Command	Description
clear cable-diagnostics tdr	Clears a specific interface or clears all interfaces that support TDR.
show cable-diagnostics tdr	Displays the test results for the TDR cable diagnostics.

time-range

To enable time-range configuration mode and define time ranges for functions (such as extended access lists), use the **time-range** command. To remove the time limitation, use the **no** form of this command.

time-range *time-range-name*

no time-range *time-range-name*

Syntax Description

time-range-name	Name for the time range.

Command Default

This command has no default settings.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **time-range** entries are identified by a name, which is referred to by one or more other configuration commands. Multiple time ranges can occur in a single access list or other feature.

The *time-range-name* cannot contain a space or quotation mark and must begin with an alphabetical character.

Note IP and IPX-extended access lists are the only types of access lists that can use time ranges.

After you use the **time-range** command, use the **periodic** time-range configuration command, the **absolute** time-range configuration command, or some combination of those commands to define when the feature is in effect. Multiple **periodic** commands are allowed in a time range; only one **absolute** command is allowed.

Tips To avoid confusion, use different names for time ranges and named access lists.

Examples

This example shows how to deny HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m. and allow UDP traffic on Saturday and Sunday from noon to midnight only:

```
Router(config)# time-range no-http
Router(config)# periodic weekdays 8:00 to 18:00
!
Router(config)# time-range udp-yes
Router(config)# periodic weekend 12:00 to 24:00
!
Router(config)# ip access-list extended strict
```

```
Router(config)# deny tcp any any eq http time-range no-http
Router(config)# permit udp any any time-range udp-yes
!
Router(config)# interface ethernet 0
Router(config)# ip access-group strict in
```

Related Commands

Command	Description
absolute	Specifies an absolute time when a time range is in effect.
ip access-list	Defines an IP access list by name.
periodic	Specifies a recurring (weekly) time range for functions that support the time-range feature.
permit (IP)	Sets conditions for a named IP access list.