

squelch through system jumbomtu

- squelch, on page 3
- srp buffer-size, on page 4
- srp deficit-round-robin, on page 5
- srp loopback, on page 7
- srp priority-map, on page 8
- srp random-detect, on page 10
- srp shutdown, on page 11
- srp tx-traffic-rate, on page 12
- stack-mib portname, on page 13
- storm-control, on page 14
- storm-control level, on page 17
- subslot, on page 19
- switchport, on page 20
- switchport access vlan, on page 25
- switchport autostate exclude, on page 27
- switchport backup, on page 29
- switchport block unicast, on page 32
- switchport capture, on page 33
- switchport capture allowed vlan, on page 35
- switchport dot1q ethertype, on page 37
- switchport mode, on page 39
- switchport port-security, on page 43
- switchport port-security aging, on page 45
- switchport port-security mac-address, on page 47
- switchport port-security maximum, on page 50
- switchport port-security violation, on page 52
- switchport private-vlan host-association, on page 54
- switchport private-vlan mapping, on page 56
- switchport protected, on page 58
- switchport trunk, on page 60
- switchport vlan mapping, on page 67
- switchport vlan mapping enable, on page 70
- switchport voice vlan, on page 72

- sync interval, on page 74
- sync-restart-delay, on page 76
- syscon address, on page 77
- syscon shelf-id, on page 78
- syscon source-interface, on page 79
- system flowcontrol bus, on page 80
- system jumbomtu, on page 81

squelch

To extend the Ethernet twisted-pair 10BASE-T capability beyond the standard 100 meters on the Cisco 4000 platform, use the **squelch** command in interface configuration mode. To restore the default, use the **no** form of this command.

squelch {**normal** | **reduced**}
no squelch

Syntax Description

normal	Allows normal capability. This is the default.
reduced	Allows extended 10BASE-T capability.

Command Default

Normal range

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example extends the twisted-pair 10BASE-T capability on the cable attached to Ethernet interface 2:

```
Router(config
)
# interface ethernet 2
Router(config
-if)
# squelch reduced
```

srp buffer-size

To make adjustments to buffer settings on the receive side for different priority traffic, use the **srpbuffer-size**command in interface configuration mode. To disable buffer size configurations, use the **no** form of this command.

srp buffer-size receive [**low** *buffer* | **medium** *buffer* | **high** *buffer*]
no srp buffer-size receive [**low** *buffer* | **medium** *buffer* | **high** *buffer*]

Syntax Description

receive	Allocates SDRAM buffer for incoming packets.
low *buffer*	(Optional) Specifies buffer size, in kilobytes, for low-priority packets. Any number from 16 to 8192. The default is 8192.
medium *buffer*	(Optional) Specifies buffer size, in kilobytes, for medium-priority packets. Any number from 16 to 8192. The default is 4096.
high *buffer*	(Optional) Specifies buffer size, in kilobytes, for high-priority packets. Any number from 16 to 8192. The default is 4096.

Command Default

low = 8192 kilobytes, medium = 4096 kilobytes, high = 4096 kilobytes

Command Modes

Interface configuration

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.0(7)XE1	This command was implemented on Cisco 7500 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example sets the buffer size for the receive side at the high setting of 17 kilobytes:

```
Router(config-if)# srp buffer-size receive high 17
```

Related Commands

Command	Description
mtu	Adjusts the maximum packet size MTU size.
srp deficit-round-robin	Transfers packets from the internal receive buffer to Cisco IOS software.

srp deficit-round-robin

To transfer packets from the internal receive buffer to Cisco IOS software, use the **srpdeficit-round-robin** command in interface configuration mode. To disable the packet transfer, use the **no** form of this command.

srp deficit-round-robin [**input** | **output**] [**low** | **medium** | **high**] [**quantum** *number* | **deficit** *number*]
no srp deficit-round-robin

Syntax Description

input	(Optional) Specifies input buffer.
output	(Optional) Specifies output buffer.
low	(Optional) Specifies low-priority queue level.
medium	(Optional) Specifies medium-priority queue level.
high	(Optional) Specifies high-priority queue level.
quantum *number*	(Optional) Specifies the Deficit Round Robin (DRR) quantum value. Any number from 9216 to 32767. The default is 9216.
deficit *number*	(Optional) Specifies the DRR deficit value. Any number from 0 to 65535. The default is 16384.

Command Default

quantum : 9216**deficit**: 16384

Command Modes

Interface configuration

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.0(7)XE1	This command was implemented on Cisco 7500 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to configure packets for the medium-priority input queue:

```
Router(config)# srp deficit-round-robin input medium deficit 15000
```

Related Commands

Command	Description
srp buffer-size	Makes adjustments to buffer settings on the receive side for different priority traffic.

Command	Description
srp priority-map	Sets priority mapping for transmitting and receiving packets.
srp random-detect	Configures WRED parameters on packets received through an SRP interface.

srp loopback

To loop the spatial reuse protocol (SRP) interface on an OC-12c DPTIP, use the **srploopback**command in interfaceconfiguration mode. To remove the loopback, use the **no** form of this command.

srp loopback {**internal** | **line**} {**a** | **b**}
no srp loopback

Syntax Description

internal	Sets the loopback toward the network before going through the framer
line	Loops the payload data toward the network.
a	Loops back the A side of the interface (inner tx, outer rx).
b	Loops back the B side of the interface (outer tx, inner rx).

Command Default

No loops are configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.0(7)XE1	This command was introduced on Cisco 7500 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command for troubleshooting purposes.

Examples

The following example configures the loopback test on the A side of the SRP interface:

```
Router(config-if)# srp loopback line a
```

srp priority-map

To set priority mapping for transmitting and receiving packets, use the**srppriority-map**command in interface configuration mode. To disable priority mapping u se the **no** form of this command .

srp priority-map receive {**low** *priority* | **medium** *priority* | **high** *priority* | **transmit** {**medium** *priority* | **high** *priority*}}
no srp priority-map

Syntax Description

receive	Specifies priority mapping for receiving packets.
transmit	Specifies priority mapping for transmitting packets.
low *priority*	(Optional) Specifies mapping for low-priority packets. Any number from 1 to 8. The default is 1.
medium *buffer*	(Optional) Specifies mapping for medium-priority packets. Any number from 1 to 8. The default is 3.
high *buffer*	(Optional) Specifies mapping for high-priority packets. Any number from 1 to 8. The default is 5 for receiving packets, and default is 7 for transmitting packets.

Command Default

receive low : 1**receivemedium**: 3 **receivehigh**: 5 **transmithigh**: 7

Command Modes

Interface configuration

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.0(7)XE1	This command was implemented on Cisco 7500 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The spatial reuse protocol (SRP) interface provides commands to enforce quality of service (QoS) functionality on the transmit side and receive side of Cisco routers. SRP uses the IP type of service (ToS) field values to determine packet priority.

The SRP interface classifies traffic on the transmit side into high- and low-priority traffic. High-priority traffic is rate shaped and has higher priority than low-priority traffic. You have the option to configure high- or low-priority traffic and can rate limit the high-priority traffic.

The **srppriority-maptransmit** command enables the user to specify IP packets with values equal to or greater than the ToS value to be considered as high-priority traffic.

On the receive side, when WRED is enabled, SRP hardware classifies packets into high-, medium-, and low-priority packets on the basis of the IP ToS value. After classification, it stores the packet into the internal receive buffer. The receive buffer is partitioned for each priority packet. Cisco routers can employ WRED on the basis of the IP ToS value. Routers also employ the Deficit Round Robin (DRR) algorithm to transfer packets from the internal receive buffer to Cisco IOS software.

The **srppriority-mapreceive** command enables the user to classify packets as high, medium, or low based on the IP ToS value.

Examples

The following example configures Cisco 7500 series routers to transmit packets with priority greater than 5 as high-priority packets:

```
Router(config-if)# srp priority-map transmit high 6
```

Related Commands

Command	Description
srp random-detect	Configures WRED parameters on packets received through an SRP interface.

srp random-detect

To configure weighted RED (WRED) parameters on packets received through an spatial reuse protocol (SRP) interface, use the **srprandom-detect**command in interfaceconfiguration mode. To return the value to the default, use the **no** form of this command.

srp random-detect {**compute-interval** *interval* | **enable** | **input** [**low** | **medium** | **high**] | [**exponential-weight** *weight* | **precedence** *precedence*]}
no srp random-detect

Syntax Description

compute-interval *compute-interval*	Specifies the queue depth compute interval, in nanoseconds. Number in the range from 1 to 128. Default is 128.
enable	Enables WRED.
input	Specifies WRED on packet input path.
low	(Optional) Specifies low-priority queue level.
medium	(Optional) Specifies medium-priority queue level.
high	(Optional) Specifies high-priority queue level.
exponential-weight *weight*	(Optional) Specifies the queue weight, in bits. Number in the range from 0 to 6. The default is 6.
precedence *number*	(Optional) Specifies the input queue precedence. Number in the range from 0 to 7. The default is 7.

Command Default

compute-interval: 128 weight: 6 precedence: 7

Command Modes

Interface configuration

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.0(7)XE1	This command was implemented on Cisco 7500 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures WRED parameters on packets received through an SRP interface with a weight factor of 5:

```
Router(config-if)# srp random-detect input high exponential-weight 5
```

srp shutdown

To disable the spatial reuse protocol (SRP) interface, use the **srpshutdown** command in interface configuration mode. To restart a disabled interface, use the **no** form of this command.

srp shutdown [**a** | **b**]
no srp shutdown [**a** | **b**]

Syntax Description

a	(Optional) Specifies side A of the SRP interface.
b	(Optional) Specifies side B of the SRP interface.

Command Default

The SRP interface continues to be enabled until this command is issued.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.0(7)XE1	This command was introduced on Cisco 7500 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **srpshutdown** command disables all functions on the specified side.

Examples

The following example turns off side A of the SRP interface:

```
Router(config-if)# srp shutdown a
```

srp tx-traffic-rate

To limit the amount of high-priority traffic that the spatial reuse protocol (SRP) interface can handle, use the**srptx-traffic-rate** command in interface configuration mode. Use the **no** form of this command to disable transmitted traffic rate .

srp tx-traffic-rate *number*
no srp tx-traffic-rate *number*

Syntax Description

number	Transmission speed, in kilobits per second. The range is from 1 to 65535. Default is 10.

Command Default

number : 10

Command Modes

Interface configuration

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.0(7)XE1	This command was implemented on Cisco 7500 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures SRP traffic to transmit at 1000 kilobits per second:

```
Router(config-if)# srp tx-traffic-rate 1000
```

stack-mib portname

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

stack-mib portname *portname*

Syntax Description

portname	Name for a port.

Command Default

This command has no default settings.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2917d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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 portall
Router(config-if)#
```

storm-control

To enable broadcast, multicast, or unicast storm control on a port or to specify the action when a storm occurs on a port, use the **storm-control** command in interface configuration mode. To disable storm control for broadcast, multicast, or unicast traffic or to disable the specified storm-control action, use the **no** form of this command.

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

Cisco ME 2600X Series Ethernet Access Switch
storm-control { {**broadcast** | **multicast**} **cir** *cir-value* | **action shutdown**}
no storm-control { {**broadcast** | **multicast**} **cir** *cir-value* | **action shutdown**}

Syntax Description

broadcast	Enables broadcast storm control on the port.
multicast	Enables multicast storm control on the port.
unicast	Enables unicast storm control on the port.
level *level*	Defines the rising and falling suppression levels. • *level* —Rising suppression level as a percent of the total bandwidth (up to two decimal places). The valid values are from 0 to 100. When the value specified for a level is reached, the flooding of storm packets is blocked.
action	Specifies the action to take when a storm occurs on a port. The default action is to filter traffic.
shutdown	Disables the port during a storm.
trap	Sends a Simple Network Management Protocol (SNMP) trap.
cir *cir-value*	Defines the Committed Information Rate (cir). • *cir-value*—The acceptable range is 10000000 -1000000000 for a gigabit ethernet interface, and 100000000-10000000000 for a ten gigabit interface. The recommended maximum value is up to 98 percent.

Command Default

Broadcast, multicast, and unicast storm control is disabled. The default action is to filter traffic.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(2)XT	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support switchport creation.

Release	Modification
12.2(15)ZJ	This command was integrated into Cisco IOS Release 12.2(15)ZJ. The **level** *level* keyword-argument pair, and the **action** and **shutdown** keywords were added.
15.0(1)S	This command was modified. The **trap** keyword was added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.2(02)SA	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

Use the **storm-control** command to enable or disable broadcast, multicast, or unicast storm control on a port. After a port is disabled during a storm, use the **no shutdown** interface configuration command to enable the port.

The suppression levels are entered as a percentage of total bandwidth. A suppression value of 100 percent means that no limit is placed on the specified traffic type. This command is enabled only when the rising suppression level is less than 100 percent. If no other storm-control configuration is specified, the default action is to filter the traffic that is causing the storm.

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

When a multicast or unicast storm occurs and the action is to filter traffic, the networking device blocks all traffic (broadcast, multicast, and unicast traffic) and sends only Spanning Tree Protocol (STP) packets.

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

The trap action is used to send an SNMP trap when a broadcast storm occurs.



Note Adding or removing of storm control configuration under the member link of LACP is not supported.



Note On Cisco Catalyst 3750 Series Switches, when the **storm-control** command is applied, it is rejected and the port is not put into a suspended state.

Examples

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

```
Device(config-if)# storm-control broadcast level 75.67
```

The following example shows how to enable multicast storm control on a port with an 87-percent rising suppression level:

```
Device(config-if)# storm-control multicast level 87
```

The following example shows how to enable the shutdown action on a port:

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

The following example shows how to disable the shutdown action on a port:

```
Device(config-if)# no storm-control action shutdown
```

The following example shows how to enable the trap action on a port:

```
Device(config-if)# storm-control action trap
```

The following example shows how to disable the trap action on a port:

```
Device(config-if)# no storm-control action trap
```

Related Commands

Command	Description
no shutdown	Enables a port.
show storm-control	Displays the packet-storm control information.
shutdown (interface)	Disables an interface.

storm-control level

To set the suppression level, use the **storm-control level** command in interface configuration mode. 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 va lues are from 0 to 99.

Command Default

All packets are passed.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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 Cisco 7600 series router supports storm control for multicast and unicast traffic only on 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 Ethernet LAN ports only. These keywords are not supported on 10 Mbps, 10/100 Mbps, 100 Mbps, or 10-Gigabit Ethernet 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

- A fractional level value of 0.29 or lower is the same as 0.0 on the WS-X6716-10G-3C / 3CXL in Oversubscription Mode.
- 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
```

This example shows how to disable the suppression mode:

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

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.

subslot

To add an IPSec VPN SPA to a Blade Failure Group, use the **subslot** command in redundancy-linecard configuration mode.

subslot *slot subslot*

Syntax Description

slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.
subslot	Secondary slot number on the SIP where the SPA is installed.

Command Default

No default behavior or values.

Command Modes

Redundancy-linecard configuration

Command History

Release	Modification
12.2(18)SXE2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

To complete the configuration of a Blade Failure Group, you must repeat the **subslot** command for each IPSec VPN SPA in the group.

Examples

The following example configures a Blade Failure Group that has a group ID of 1 and consists of two IPSec VPN SPAs--one IPSec VPN SPA is in slot 5, subslot 1 and one IPSec VPN SPA is in slot 6, subslot 1:

```
Router(config)# redundancy
Router
(config-red)# linecard-group 1 feature-card
Router(config-r-lc)# subslot 5/1
Router(config-r-lc)# subslot 6/1
```

Related Commands

Command	Description
linecard-group feature card	Assigns a group ID to a Blade Failure Group.
redundancy	Enters redundancy configuration mode.
show redundancy linecard-group	Displays the components of a Blade Failure Group.

switchport

Cisco 3550, 4000, and 4500 Series Switches

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

switchport
no switchport

Cisco Catalyst 6500 and 6000 Series Switches and Cisco 7600 Series Routers

To modify the switching characteristics of the Layer 2-switched interface, use the **switchport** command (without keywords). Use the **no** form of this command (without keywords) to return the interface to the routed-interface status and cause all further Layer 2 configuration to be erased. Use the **switchport** commands (with keywords) to configure the switching characteristics.

switchport
switchport {**host** | **nonegotiate**}
no switchport
no switchport nonegotiate

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

To configure the server module to communicate with the router over a high-speed Multi Gigabit Fabric (MGF) backplane switch port, use the **switchport** command (with keywords) in interface configuration mode.

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

Cisco 1000 Series Integrated Services Routers with 4 or 8 Front-Panel Switch Ports

To configure the flex Layer 2 and Layer 3 ports to Layer 2 interface, use the **switchport** command (without keywords). To configure to Layer 3 interface, use the **no switchport** command (without keywords).

switchport
no switchport

Syntax Description

Cisco 3550, 4000, and 4500 Series Switches

This command has no arguments or keywords.

Cisco Catalyst 6500 and 6000 Series Switches and Cisco 7600 Series Routers

Table 1: Syntax Description for Cisco Catalyst 6500 and 6000 Series Switches and Cisco 7600 Series Routers

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

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

Table 2: Syntax Description for Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

access	Sets the access mode characteristics of the interface.
mode	Sets the interface type: Access or Trunk.
trunk	Sets trunk characteristics when the interface is in Trunk mode. This is the default mode.

Cisco 1000 Series Integrated Services Routers with 4 or 8 Front-Panel Switch Ports

This command has no arguments or keywords.

Command Default

Cisco 3550, 4000, and 4500 Series Switches

All interfaces are in Layer 2 mode.

Catalyst 6500/6000 Series Switches and 7600 Series Routers

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

Cisco 1000 Series Integrated Services Routers with 4 or 8 Front-Panel Switch Ports

The last two ports of the front-panel switch ports (flex ports) are set to Layer 2 interface by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(15)ZJ	This command was implemented on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
15.1(2)T	Support for IPv6 was added.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Routers (ISR).
Cisco IOS XE Release 17.11.1a	This command was implemented to provide flex support on the last two Layer 2 switch ports of the Cisco 1000 Series ISRs with 4 or 8 Front-Panel Switch Ports.

Usage Guidelines

Cisco 3550, 4000, and 4500 Series Switches

Use the **no switchport** command to put the interface into the routed-interface status and to erase all Layer 2 configurations. You must use this command before assigning an IP address to a routed port. Entering the **no switchport** command shuts down the port and then reenables it, which might generate messages on the device to which the port is connected.

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

Cisco Catalyst 6500 and 6000 Series Switches and Cisco 7600 Series Routers

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 Cisco 7600 series routers, 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, Dynamic Inter-Switch Link Protocol and Dynamic Trunking Protocol (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

Cisco 3550, 4000, and 4500 Series Switches

The following example shows how to cause an interface to cease operating as a Layer 2 port and become a Cisco-routed (Layer 3) port:

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

Cisco Catalyst 6500 and 6000 Series Switches and Cisco 7600 Series Routers

The following 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.

The following 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)#
```

The following example shows how to cause an interface to cease operating as a Cisco-routed port and to convert it into a Layer 2 switched interface:

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

Note The **switchport** command is not used on platforms that do not support Cisco-routed (Layer 3) ports. All physical ports on such platforms are assumed to be Layer 2 switched interfaces.

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

The following example shows how to set the interface to **access** mode:

```
Router#configure terminal
Router(config)# interface ucse 1/0/0
Router(config-if)# switchport mode access
```

The following example shows how to set the interface to **trunk** mode:

```
Router#configure terminal
Router(config)# interface ucse 1/0/0
Router(config-if)# switchport mode trunk
```

Cisco 1000 Series Integrated Services Routers with 4 or 8 Front-Panel Switch Ports

The following example shows how to convert a flex port to a Layer 3 port:

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/6
Device(config-if)# no switchport
Device(config-if)# ip address 10.10.0.1 255.255.255.0
Device(config-if)# exit
```

The following example shows how to convert a flex port to a Layer 2 port:

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/6
Device(config-if)# switchport
Device(config-if)# switchport mode access
Device(config-if)# exit
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
show running-config	Displays the current operating configuration.
switchport access vlan	Sets the VLAN when the interface is in Access mode.
switchport mode	Sets the interface type: Access or Trunk
switchport trunk	Sets trunk characteristics when the interface is in Trunk mode.

switchport access vlan

To set the VLAN when the interface is in access mode, use the **switchport access vlan** command in interface configuration or template configuration mode. 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. Valid values for Cisco UCS E-Series Servers installed in Cisco 4400 Integrated Services Routers are: • 1-2349—VLAN ID Range 1 • 2450-4095—VLAN ID Range 2

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)

Template configuration (config-template)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Routers (ISR).
Cisco IOS XE Release 3.6E	This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode.

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

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

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



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

The following example shows how to make 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 interface configuration mode:

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

The following example shows how to make a port interface that has already been configured as a switched interface to operate in VLAN 2 instead of the platform's default VLAN, using an interface template in template configuration mode:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# switchport access vlan 2
Device(config-template)# end
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport	Configures a LAN interface as a Layer 2 interface.

switchport autostate exclude

To exclude a port from the VLAN interface link-up calculation, use the **switchportautostateexclude**command in interface configuration mode. 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

Command History

Release	Modification
12.2(17b)SXA	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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 **switchportautostateexclude** 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 MSFC 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 MSFC 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 **showinterface***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
```

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

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

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport	Configures a LAN interface as a Layer 2 interface.

switchport backup

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

switchport backup interface *type number*[**preemption** {**delay** *delay* | **mode** {**bandwidth** | **forced** | **off**}}]
no switchport backup [**interface** *type number* [**preemption** {**delay** | **mode**}]]

Syntax Description

interface *type number*	Specifies the interface type and the module and port number to be configured as a Flexlink backup interface.
preemption delay *delay*	Specifies the preemption delay in seconds. The range is from 0 to 300 seconds.
preemption mode bandwidth	Specifies that a higher bandwidth interface is preferred for preemption.
preemption mode forced	Specifies that an active interface is preferred for preemption.
preemption mode off	Specifies that preemption is turned off.

Command Default

Interfaces are not configured as Flexilink backup interfaces.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)SXF	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1(1)SY	This command was modified. The **no** form was modified so that specific backup configurations can be disabled.

Usage Guidelines

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

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

The *number* arguement 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. Flexlink fast convergence does not impact any other type of network failure.

You must enter the **switchport** command without any keywords to configure a LAN interface as a Layer 2 interface before you can enter the **switchport backup** command.

You can remove all Flexilink configurations on an interface by using the **no switchport backup** command. You can remove specific backup configurations by using the optional keywords in the **no** form of this command.



Note The **switchport** command is used only on platforms that support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2 switched interfaces.

Examples

The following example shows how to enable Flexlink on an interface. This example also shows how to configure a preemption delay of 100 seconds on an interface.

```
Device(config)# interface GigabitEthernet1/1
Device(config-if)# switchport
Device(config-if)# switchport backup interface GigabitEthernet1/2
Device(config-if)# switchport backup interface GigabitEthernet1/2 preemption delay 100
Device(config-if)# end
Device# show running interface GigabitEthernet1/1

Building configuration...

Current configuration : 219 bytes
!
interface GigabitEthernet1/1
 switchport
 switchport backup interface Gi1/2
 switchport backup interface Gi1/2 preemption delay 100
end

Device# show interfaces switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
Gi1/1                   Gi1/2                   Active Up/Backup Down
```

The following example shows how to disable specific backup configurations on an interface:

```
Device(config)# interface GigabitEthernet1/1
Device(config-if)# no switchport backup interface GigabitEthernet1/2 preemption delay
Device(config-if)# end
Device# show running-config interface GigabitEthernet1/1

Building configuration...

Current configuration : 219 bytes
!
interface GigabitEthernet1/1
 switchport
 switchport backup interface Gi1/2
end
```

The following example shows how to disable Flexlink and remove all Flexlink configurations on an interface:

```
Device(config)# interface GigabitEthernet1/1
Device(config-if)# no switchport backup interface GigabitEthernet1/2
Device(config-if)# end
```

```
Device# show running-config interface GigabitEthernet1/1

Building configuration...

Current configuration : 219 bytes
!
interface GigabitEthernet1/1
 switchport
end
```

Related Commands

Command	Description
show interfaces switchport backup	Displays Flexlink pairs.
show running-config	Displays the contents of the current running configuration file or the configuration for a specific module, Layer 2 VLAN, class map, interface, map class, policy map, or VC class.
switchport	Configures a LAN interface as a Layer 2 interface.
switchport autostate exclude	Excludes a port from the VLAN interface link-up calculation.

switchport block unicast

To prevent the unknown unicast packets from being forwarded, use the **switchportblockunicast**command in interface configuration mode. 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 Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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 Cisco 7600 Series Router Cisco IOS Software Configuration Guide.

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

Examples

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

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

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 **switchportcapture**command in interface configuration mode. 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

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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 **switchportcapture** command applies only to Layer 2 switched interfaces.

WAN interfaces support only the capture functionality of VACLs.

Entering the **noswitchport** 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 **switchportcapture** 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 **switchportcapture** and **switchportcaptureallowedvlan**commands. The port does not become a capture port until you enter the **switchportcapture** (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 **noswitchportcapture** 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
```

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	Configures the LAN interface as a Layer 2 switched interface.

switchport capture allowed vlan

To specify the destination VLANs of the VACL-filtered traffic, use the **switchport** capture allowed vlancommand in interface configuration mode. To clear the configured-destination VLAN list and return to the default settings, use the **no** form of this co mmand.

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

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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 **noswitchport** 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 **switchportcaptureallowedvlan1-1000,2000,3000-3100**.

There is no restriction on the order in which you enter the **switchportcapture** and **switchportcaptureallowedvlan**commands. The port does not become a capture port until you enter the **switchportcapture** (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
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport	Configures the LAN interface as a Layer 2 switched interface.
switchport capture	Configures the port to capture VACL-filtered traffic.

switchport dot1q ethertype

To specify the EtherType value to be programmed on the interface, use the **switchportdot1qethertype** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

switchport dot1q ethertype *value*
no 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

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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

- WS-X6748-GE-TX
- WS-X6724-SFP
- WS-X6704-10GE
- WS-X6816-GBIC

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
```

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 in interface configuration mode. Use the appropriate **no** form of this command to reset the mode to the appropriate default mode for the device.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers
switchport mode {**access** | **trunk**}
no switchport mode

Cisco Catalyst 6500/6000 Series Switches
switchport mode {**access** | **dot1q-tunnel** | **dynamic** {**auto** | **desirable**} | **trunk**}
no switchport mode

Cisco 7600 Series Routers
switchport mode {**access** | **dot1q-tunnel** | **dynamic** {**auto** | **desirable**} | **private-vlan** | **trunk**}
no switchport mode
switchport mode private-vlan {**host** | **promiscuous**}
no switchport mode private-vlan

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers
switchport mode {**access** | **trunk**}
no switchport mode {**access** | **trunk**}

Syntax Description

access	Sets a nontrunking, nontagged single VLAN Layer 2 interface.
trunk	Specifies a trunking VLAN Layer 2 interface.
dot1q-tunnel	Sets the trunking mode to TUNNEL unconditionally.
dynamic auto	Sets the interface to convert the link to a trunk link.
dynamic desirable	Sets the interface to actively attempt to convert the link to a trunk link.
private vlan host	Specifies that the ports with a valid private VLAN (PVLAN) association become active host private VLAN ports.
private vlan promiscuous	Specifies that the ports with a valid PVLAN mapping become active promiscuous ports.

Table 3: Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

access	Sets a nontrunking, nontagged single VLAN Layer 2 interface.
trunk	Specifies a trunking VLAN Layer 2 interface.

Command Default

The default is **access** mode.

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

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
12.0(7)XE	This command was introduced on the Cisco Catalyst 6000 family switches.
12.1(1)E	This command was integrated on the Cisco Catalyst 6000 family switches.
12.1(8a)EX	The switchport mode **private-vlan** {**host** | **promiscuous**} syntax was added.
12.2(2)XT	Creation of switchports became available on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T for creation of switchports on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Routers (ISR).

Usage Guidelines

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

If you enter a forced mode, the interface does not negotiate the link to the neighboring interface. Ensure that the interface ends match.

The **no** form of the command is not supported on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Cisco Catalyst 6500/6000 Switches and Cisco 7600 Series Routers

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, PortFast Bridge Protocol Data Unit (BPDU) filtering is enabled and Cisco Discovery Protocol (CDP) is disabled on protocol-tunneled interfaces.

Examples

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The following example shows how to set the interface to **access** mode:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)#switchport mode access
```

The following example shows how to set the interface to **trunk** mode:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)#switchport mode trunk
```

Cisco Catalyst 6500/6000 Switches and Cisco 7600 Series Routers

The following example shows how to set the interface to dynamic desirable mode:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)# switchport mode dynamic desirable
```

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

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)# switchport mode private-vlan host
```

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

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)# switchport mode private-vlan promiscuous
```

Integrated Series Routers Generation 2 (ISR G2) Platforms with EHWIC-4/8ESG

The following example shows how to configure tunneling on port 4/1 and verify the configuration:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)# switchport mode dot1q-tunnel
Router(config-if)# end
```

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

The following example shows how to set the interface to **access** mode:

```
Router#configure terminal
Router(config)# interface ucse 1/0/0
Router(config-if)# switchport mode access
```

The following example shows how to set the interface to **trunk** mode:

```
Router#configure terminal
Router(config)# interface ucse 1/0/0
Router(config-if)# switchport mode trunk
```

Related Commands

Command	Description
show dot1q-tunnel	Displays a list of 802.1Q tunnel-enabled ports.
show interfaces switchport	Displays administrative and operational status of a switching (nonrouting) port.
show interfaces trunk	Displays trunk information.
switchport	Modifies the switching characteristics of the Layer 2-switched interface.
switchport private vlan host association	Defines a PVLAN association for an isolated or community port.
switchport private vlan mapping	Defines the PVLAN mapping for a promiscuous port.
switchport trunk	Sets trunk characteristics when the interface is in trunking mode.

switchport port-security

To enable port security on an interface, use the **switchportport-security** command in i nterface configuration mode . 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

D isabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Follow these guidelines when configuring port security:

- With Release 12.2(18)SXE and later releases, port security is supported on trunks.
- With releases earlier than Release 12.2(18)SXE, port security is not supported on trunks.
- With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
- With releases earlier than Release 12.2(18)SXE, port security is not 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
```

This example shows how to disable port security:

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 time command in interface configuration mode . To disable aging, use the **no** form of this command.

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

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, t he defaults are as follows:
  - *time* is 0.
  - **type** is **absolute**

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports. • The **type**, **absolute**, and **inactivity** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Follow these guidelines when configuring port security:

- With Release 12.2(18)SXE and later releases, port security is supported on trunks. With releases earlier than Release 12.2(18)SXE, port security is not supported on trunks.
- With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports. With releases earlier than Release 12.2(18)SXE, port security is not 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
```

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

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

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

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

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

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

Related Commands

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

switchport port-security mac-address

To add a MAC address to the list of secure MAC addresses, use the **switchportport-securitymac-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* [**voice**]*vlan-list*]}
no switchport port-security mac-address {*mac-addr* | **sticky** [*mac-addr*] [**vlan** *vlan* [**voice**]*vlan-list*]}

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.

Command Default

MAC-addresses are not classified as secured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports. • The **vlan***vlan* | *vlan-list*keyword and arguments were added. • The **sticky** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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 **switchportmodetrunk** command and then enter the **switchportnonegotiate** 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 **switchportport-securitymac-addresssticky** 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.

For trunk ports, if you enter the **noswitchportport-securitymac-addresssticky** command, a search is conducted for the MAC address in the native VLAN. An error message is displayed if the MAC address is not found in the native VLAN. You must specify the VLAN in the **no** form of the **switchportport-securitymac-addresssticky** command to remove the MAC address.

For voice ports, you must specify the **vlanvoice** keywords in the **no** form of the command.

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 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
```

The following example shows how to configure a VLAN in the voice port:

```
Router(config-if)# switch port-security mac-address 0.0.1 vlan voice
```

To remove the MAC address 0.0.1 from the voice port, use the following command:

```
Router(config-if)# no switchport port-security mac-address 0.0.1 vlan voice
```

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 **switchportport-securitymaximum**command in interface configuration mode. To return to the default settings, use the **no** form of this command.

switchport port-security maximum *maximum* [**vlan** *vlanvlan-list*]
no switchport port-security maximum

Syntax Description

maximum	M aximum 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

This command has no default setings .

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720 only: • The maximum number of secure MAC addresses was changed from 1024 to 4097. • The **vlan***vlan* | *vlan-list*keyword and arguments were added. • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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 **switchportport-securitymaximum***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 **switchportmodetrunk** command and then enter the **switchportnonegotiate** 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
```

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

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

Related Commands

Command	Description
show port-security	Display information about the port-security setting.
switchport nonegotiate	Configures the LAN port into permanent trunking mode.

switchport port-security violation

To set the action to be taken when a security violation is detected, use the **switchportport-securityviolation** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

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

The port security violation is shutdown.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SXH	**Platform port-security disable traps** was introduced as part of protect violation mode.

Usage Guidelines

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. Platform port-security disable traps is configurable only when the violation mode is set to **protect**. When this option is configured, drop entries will not be installed into hardware for violating addresses, thus allowing traffic to continue to flow to violating address from legitimate ports. To protect switch CPU against overload when this option is enabled, we recommend that you configure the port-security rate-limiter to 2000 packets per second with a burst rate of 10.

Note This feature also permits traffic to legitimate ports from insecure 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 **errdisablerecoverycausepsecure-violation** global configuration command or you can manually reenable it by entering the **shutdown** and **noshutdown** 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
```

This example allows the traffic to a secured MAC address on one port to flow even in the presence of violations on other ports while in protect mode.

```
Router(config-if)# switchport port-security violation protect
Router(config-if)# platform port-security disable traps
```

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.
errdisable recovery cause psecure-violation (global configuration)	Removes a secure port from an error-disabled state.
platform port-security disable traps	Modifies the behavior of protect violation mode.

switchport private-vlan host-association

To define a PVLAN association for an isolated or community port, use the **switchportprivate-vlanhost-association**command in i nterface configuration mode . 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

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to t Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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
```

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

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

Related Commands

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

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

switchport private-vlan mapping

To define the PVLAN mapping for a promiscuous port, use the **switchportprivate-vlanmapping** command in interface configuration mode. 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- list	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

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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
```

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

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

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

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

Related Commands

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

switchport protected

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

switchport protected
no switchport protected

Syntax Description

This command has no arguments or keywords.

Command Default

No protected port is defined. All ports are nonprotected.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(4)EA1	This command was first introduced.
12.4(15)T	This command was implemented on the following platforms: the Cisco 1841 Integrated Services Router (ISR), Cisco 2800 series ISRs, and Cisco 3800 series ISRs.

Usage Guidelines

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

Beginning with Cisco IOS Release 12.4(15)T, the following Cisco ISRs support port protection when an appropriate high-speed WAN interface card (HWIC) is installed:

- Cisco 1841 ISR
- Cisco 2800 Series ISRs, including models 2801, 2811, 2821, and 2851
- Cisco 3800 Series ISRs, including models 3825 and 3845

To support port protection, the Cisco routers listed above must be equipped with one of the following HWICs:

- HWIC-4ESW
- HWIC-D-9ESW

Note Only the ports attached to the HWICs can be configured with port protection.

A protected port does not forward any unicast, multicast, or broadcast traffic to any other protected port. A protected port continues to forward unicast, multicast, and broadcast traffic to unprotected ports and vice versa.

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

A protected port is different from a secure port.

Examples

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

```
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# switchport protected
```

You can verify the previous command by entering the**showinterfacesswitchport**privileged EXEC command.

Related Commands

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

switchport trunk

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

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers
switchport trunk {**encapsulation dot1q** | **native vlan** | **allowed vlan**}
no switchport trunk {**encapsulation dot1q** | **native vlan** | **allowed vlan**}

Cisco 7600 Series Routers and Catalyst 6500 Series Switches
{**switchport trunk encapsulation** {**isl** | **dot1q** [**ethertype** *value*] | **negotiate**} | **native vlan** {**tag***vlan-id*} | **allowed vlan** *vlan-list* | **pruning vlan** *vlan-list*}
no switchport trunk {**encapsulation** {**isl** | **dot1q** [**ethertype** *value*] | **negotiate**} | **native vlan** [**tag**] | **allowed vlan** | **pruning vlan**}

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers
switchport trunk {**native vlan** *vlan-id* | **allowed vlan** *vlan-list*}
no switchport trunk {**native vlan** *vlan-id* | **allowed vlan** *vlan-list*}

Syntax Description

encapsulation isl	Sets the trunk encapsulation format to Inter-Switch Link (ISL).
encapsulation dot1q	Sets the trunk encapsulation format to 802.1Q.
native vlan	Sets the native VLAN for the trunk in 802.1Q trunking mode.
allowed vlan *vlan list*	Sets the list of allowed VLANs that transmit traffic from this interface in tagged format when in trunking mode.
ethertype *value*	(Optional) Sets the EtherType value; valid values are from 0x0 to 0x5EF-0xFFFF.
encapsulation negotiate	Specifies that if the Dynamic Inter-Switch Link (DISL) protocol and Dynamic Trunking Protocol (DTP) negotiation do not resolve the encapsulation format, ISL is the selected format.
native vlan tag	Enables the native VLAN tagging state on the interface.
native vlan *vlan id*	The particular native VLAN.
pruning vlan *vlan list*	Sets the list of VLANs that are enabled for VLAN Trunking Protocol (VTP) pruning when the interface is in trunking mode. See the “Usage Guidelines” section for the *vlanlist*argument formatting guidelines.

Table 4: Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

native vlan *vlan-id*	The particular native VLAN. Valid values are: • 1-2349—VLAN ID Range 1 • 2450-4095—VLAN ID Range 2

allowed vlan *vlan-list*	Sets the list of allowed VLANs that transmit traffic from this interface in tagged format when in trunking mode. **Note** For *vlan-list* format, see **Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers** section under **Usage Guidelines**.

Command Default

- The default encapsulation type is dot1q.
- The default access VLAN and trunk interface native VLAN are default VLANs that correspond to the platform or interface hardware.
- The default for all VLAN lists is to include all VLANs.
- 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.
- The default for all VLAN lists is to include all VLANs.
- **ethertype** *value* for 802.1Q encapsulation is 0x8100.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6500 series switches.
12.1(1)E	Switchport creation on Catalyst 6500 series switches was added.
12.2(2)XT	This command was introduced to support switchport creation on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support switch port creation on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX to support the Supervisor Engine 720 on the Cisco 7600 series routers and Catalyst 6500 series switches.
12.2(17a)SX	This command was modified to include the following: • Restriction of ISL trunk-encapsulation. • Addition of the **dot1q** keyword and **ethertype***value* keyword and argument.
12.2(17d)SXB	Support for the Supervisor Engine 2 on the Cisco 7600 series routers and Catalyst 6500 series switches was added.
12.2(18)SXD	This command was modified to allow the **switchport trunk allowed vlan**command to be entered on interfaces where the span destination port is either a trunk or an access port.

Release	Modification
12.2(18)SXE	This command added a restriction that Gigabit Ethernet (GE) Optimized Layer 2 WAN ports are not supported on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	This command was modified to extend the range of valid VLAN IDs from 1 to 4094 for specified platforms.
12.2(33)SXH	This command was changed as follows: • Allowed the tagging of native VLAN traffic on a per-port basis. • Introduced on the Supervisor Engine 720-10GE.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Routers (ISR).

Usage Guidelines

802.1Q Trunks

- When you connect Cisco switches through an 802.1Q trunk, make sure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.
- Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can cause spanning-tree loops. Cisco recommends that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk. If this is not possible, disable spanning tree on every VLAN in the network. Make sure that your network is free of physical loops before disabling spanning tree.
- When you connect two Cisco switches through 802.1Q trunks, the switches exchange spanning-tree bridge protocol data units (BPDUs) on each VLAN allowed on the trunks. The BPDUs on the native VLAN of the trunk are sent untagged to the reserved IEEE 802.1d spanning-tree multicast MAC address (01-80-C2-00-00-00). The BPDUs on all other VLANs on the trunk are sent tagged to the reserved Shared Spanning Tree Protocol (SSTP) multicast MAC address (01-00-0c-cc-cc-cd).
- The 802.1Q switches that are not Cisco switches maintain only a single instance of spanning-tree (Mono Spanning Tree [MST]) that defines the spanning-tree topology for all VLANs. When you connect a Cisco switch to a switch through an 802.1Q trunk without a Cisco switch, the MST of the switch and the native VLAN spanning tree of the Cisco switch combine to form a single spanning-tree topology known as the Common Spanning Tree (CST).
- Because Cisco switches transmit BPDUs to the SSTP multicast MAC address on VLANs other than the native VLAN of the trunk, switches that are not Cisco switches do not recognize these frames as BPDUs and flood them on all ports in the corresponding VLAN. Other Cisco switches connected to the 802.1Q cloud receive these flooded BPDUs. This condition allows Cisco switches to maintain a per-VLAN spanning-tree topology across a cloud of 802.1Q switches that are not Cisco switches. The 802.1Q cloud of switches separating the Cisco switches is treated as a single broadcast segment among all switches connected to the 802.1Q cloud of switches that are not Cisco switches through 802.1Q trunks.
- Make sure that the native VLAN is the same on *all* of the 802.1Q trunks that connect the Cisco switches to the 802.1Q cloud of switches that are not Cisco switches.

- If you are connecting multiple Cisco switches to a 802.1Q cloud of switches that are not Cisco switches, all of the connections must be through 802.1Q trunks. You cannot connect Cisco switches to an 802.1Q cloud of switches that are not Cisco switches through ISL trunks or through access ports. Doing so will cause the switch to place the ISL trunk port or access port into the spanning-tree "port inconsistent" state and no traffic will pass through the port.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

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

The *vlanlist* format is **all** | **none** | **add** | **remove** | **except***vlanlist*[,*vlanlist*...] where:

- **all** --Specifies all VLANs from 1 to 1005. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094.
- **none** --Indicates an empty list. This keyword is not supported in the **switchport trunk allowed vlan** form of the 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.
- **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 1005 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen that represents the VLAN IDs of the allowed VLANs when this port is in trunking mode. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094.

Cisco 7600 Series Routers and Catalyst 6500 Series Switches

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

You can enter the **switchport trunk** command only on the PO. If you enter the **switchport trunk** command on a port member the following message is displayed:

```
Configuration is not allowed on Port members. Remove the interface from the Port Channel
to modify its config
```

The **switchport trunk encapsulation dot1q**command is supported only for platforms and interface hardware that can support both ISL and 802.1Q formats. Only 802.1Q encapsulation is supported by shared port adapters (SPAs).

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.

You can enter the **switchport trunk native vlan tag** command to enable the tagging of native VLAN traffic on a per-port basis. When tagging is enabled, all the packets on the native VLAN are tagged and all incoming untagged data packets are dropped, but untagged control packets are accepted. When tagging is disabled, the native VLAN packets going out on trunk ports are not tagged and the incoming untagged packets are allowed and assigned to the native VLAN. The **no switchport trunknative vlan tag** command overrides the **vlan dot1q tag native** command for global tagging.

Note The **switchport trunk native vlan tag** interface configuration mode command does not enable native VLAN tagging unless you first configure the switch to tag native VLAN traffic globally. To enable native VLAN tagging globally, use the **vlan dot1q tag native** command in global configuration mode.

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** keyword and DISL and Dynamic Trunking Protocol (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 to the default.

- The **no** form of the **switchport trunk native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.
- The **no** form of the **switchport trunk native vlan tag** command configures the Layer 2 port not to tag native VLAN traffic.
- The **no** form of the **switchport trunk allowed vlan** command resets the list to the default list, which allows all VLANs.
- The **no** form of the **switchport trunk pruning vlan**command resets the list to the default list, which enables all VLANs for VTP pruning.
- The **no** form of the **switchport trunk encapsulation dot1qethertype***value* command resets the list to the default value.

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

- **all** --Specifies all the appropriate VLANs. This keyword is not supported in the **switchporttrunkpruningvlan** command.
- **none** --Indicates an empty list. This keyword is not supported in the **switchporttrunkallowedvlan** command.
- **add** *vlan-list* **,** *vlan-list*...]-- Adds the defined list of VLANs to those currently set instead of replacing the list.
- **remove** *vlan-list* **,** *vlan-list*...]-- 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, Cisco Discovery Protocol, version 3; VTP; Port Aggregation Protocol, version 4 (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** *vlan-list* **,** *vlan-list...*] --Excludes the specified list of VLANs from those currently set instead of replacing the list.
- *vlan-list* **,** *vlan-list...* -- Specifies a single VLAN number from 1 to 4094 or a continuous range of VLANs that are described by two VLAN numbers from 1 to 4094. You can specify multiple VLAN numbers or ranges of numbers using a comma-separated list.

To specify a range of VLANs, enter the smaller VLAN number first, separated by a hyphen and the larger VLAN number at the end of the range.

Do not enable the reserved VLAN range (1006 to 1024) on trunks when connecting a Cisco 7600 series router running the Cisco IOS software on both the supervisor engine and the Multilayer Switch Feature Card (MSFC) to a Cisco 7600 series router running the Catalyst operating system. These VLANs are reserved in Cisco 7600 series routers running the Catalyst operating system. If enabled, Cisco 7600 series routers running the Catalyst operating system may disable the ports if a trunking channel is between these systems.

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

Note To set trunk characteristics, the interface must be in trunk mode.

The *vlan-list* format is **all** | **none** | **add** | **remove** | **except** | **WORD**, where:

- **all**—Specifies all VLANs: 1-2349—VLAN IDs in range 1; and 2450-4095—VLAN IDs in range 2.
- **none**—Indicates an empty list.
- **add**—Adds the defined list of VLANs to those currently set instead of replacing the list.
- **remove**—Removes the defined list of VLANs from those currently set instead of replacing the list.
- **except**—Lists the VLANs that should be calculated by inverting the defined list of VLANs.
- **WORD**—Is either a single VLAN number from 1 to 4095 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen that represents the VLAN IDs of the allowed VLANs when this port is in trunking mode.

Examples

The following example shows how to cause a port interface 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

The following example shows how to configure the Layer 2 port to tag native VLAN traffic:

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

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

Note To set trunk characteristics, the interface must be in trunk mode.

The following example shows how to allow trunking on specified VLANs:

```
Router(config)# interface ucse 1/0/0
Router(config-if)# switchport mode trunk
Router(config-if)# switchport trunk allowed vlan 1-2,40,60,1002-1005
```

Related Commands

Command	Description
show interfaces switchport	Displays administrative and operational status of a switching (nonrouting) port.
vlan dot1q tag native	Enables dot1q tagging for all VLANs in a trunk.

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 **switchportvlanmapping** command in interface configuration mode. 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

Command History

Release	Modification
12.2(17b)SXA	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXE	This command is not supported on GE Layer 2 WAN ports.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

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 **switchportvlanmappingenable** 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.

The table below 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 5: 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-X6704-10GE	Per port	4	1 port in each group	128	ISL and 802.1Q
WS-X6501-10GEX4	Per port	1	1 port in 1 group	32	802.1Q

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-X6502-10GE	Per port	1	1 port in 1 group	32	802.1Q
WS-X6724-SFP	Per port group	2	1-12, 13-24	128	ISL and 802.1Q
WS-X6816-GBIC	Per port group	4	1-8, 9-16	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-X6748-GE-TX	Per port group	4	1-12, 13-24, 25-36, 37-48	128	ISL and 802.1Q
WS-X6516-GE-TX	Per port group	2	1-8, 9-16	32	802.1Q
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 **switchportvlanmapping** 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
```

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

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

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

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

Related Commands

Command	Description
show interfaces vlan mapping	Display 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 **switchportvlanmappingenable** command in interface configuration mode. To disable VLAN mapping per switch port, use the **no** form of this command.

switchport vlan mapping enable
no switchport vlan mapping enable

Syntax Description

This command has no arguments or keywords.

Command Default

VLAN mapping is disabled on all switch ports.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17b)SXA	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

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

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
```

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

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

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.

Command	Description
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 **switchportvoicevlan** command in interface configuration mode. To remove the voice VLAN from the switch port, use the **no** form of the command.

switchport voice vlan {*vlan-id* | **dot1p** | **none** | **untagged**}
no switchport voice vlan

Syntax Description

vlan id	Voice VLAN identifier (VVID) of the VLAN used for voice traffic. Valid IDs are from 1 to 1005 (IDs 1006 to 4096 are not supported). Do not enter leading zeros. The switch port is an 802.1Q trunk port.
dot1p	The telephone uses priority tagging and uses VLAN 0. The switch port is an 802.1Q trunk port.
none	The telephone is not instructed through the command line interface (CLI) about the voice VLAN. The telephone uses its own configuration from the telephone keypad and transmits untagged voice traffic in the default VLAN.
untagged	The telephone does not tag frames; it uses VLAN 4095. The switch port can be an access port or an 802.1Q trunk port.

Command Default

The switch default is to not automatically configure the telephone (**none**).

The Cisco IP 7960 telephone default is to generate an 802.1Q/802.1P frame.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XT	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support creation of switchports .
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX and introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was integrated into Cisco IOS Release 12.2(17d)SXB and introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

This command does not create a voice VLAN. You can create a voice VLAN in VLAN-configuration mode by entering the **vlan(globalconfigurationmode)** 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 a voice VLAN identifier, the switch port 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 . The default Layer 2 CoS is 5. The default Layer 3 IP-precedence value is 5.

If you enter dot1p, the switch port 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.

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.

Examples

This example shows how to create an operational multiple-VLAN access port with VLAN 101 as the voice VLAN:

```
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 interval

To specify an interval for the device to exchange Precision Time Protocol synchronization messages, use the **sync interval** command in PTP port configuration mode. To disable a sync interval configuration, use the **no** form of this command.

sync interval *interval-value*
no sync interval *interval-value*

Syntax Description

interval-value	Value of the interval at which the device sends sync packets. The intervals are set using log base 2 values, as follows: • 4—1 packet every 16 seconds • 3—1 packet every 8 seconds • 2—1 packet every 4 seconds • 1—1 packet every 2 seconds • 0—1 packet every second • -1—1 packet every 1/2 second, or 2 packets per second • -2—1 packet every 1/4 second, or 4 packets per second • -3—1 packet every 1/8 second, or 8 packets per second • -4—1 packet every 1/16 seconds, or 16 packets per second • -5—1 packet every 1/32 seconds, or 32 packets per second • -6—1 packet every 1/64 seconds, or 64 packets per second The recommended value is -6.

Command Default

The default value is 1.

Command Modes

PTP port configuration (config-ptp-port)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Examples

The following example shows how to configure the PTP sync interval:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# clock-port slave slaveport
Device(config-ptp-port)# sync interval -4
Device(config-ptp-port)# end
```

Related Commands

Command	Description
clock-port	Specifies the mode of a PTP clock port.

sync-restart-delay

To set the synchronization-restart delay timer to ensure accurate status reporting, use the **sync-restart-delay** command in interface configuration mode. To disable the synchronization-restart delay timer, use the **no** form of this command.

sync-restart-delay *timer*
no 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

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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
```

Related Commands

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

syscon address

To specify the system controller for a managed shelf, use the **sysconaddress** command in global configuration mode. To stop the management of the shelf by the system controller, use the **no** form of this command.

syscon address *ip-address password*
no syscon address

Syntax Description

ip-address	IP address of the system controller.
password	Password string.

Command Default

No system controller is specified.

Command Modes

Global configuration

Command History

Release	Modification
11.3AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is required in order for the shelf to be managed by the system controller.

Examples

The following example configures a shelf to be managed by a system controller at 10.2.3.4 using the password green:

```
Router# syscon address 10.2.3.4 green
```

Related Commands

Command	Description
show syscon sdp	Displays information about the Shelf Discovery Protocol.
syscon source-interface	Specifies the interface to use for the source address in SDP packets.

syscon shelf-id

To specify a shelf ID for a managed shelf, use the **sysconshelf-id**command in global configuration mode. To remove the shelf ID, use the **no** form of this command.

syscon shelf-id *number*
no syscon shelf-id

Syntax Description

number	Shelf ID. The value ranges from 0 to 9999.

Command Default

No shelf ID is specified.

Command Modes

Global configuration

Command History

Release	Modification
11.3AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to specify a shelf ID for a managed shelf. Some platforms, such as the Cisco AS5800, use other commands to assign a shelf ID. In these situations, do not specify a shelf ID with the **sysconshelf-id** command. Use the platform-specific command instead.

Examples

The following example configures a shelf ID of 5 for the managed shelf:

```
Router# syscon shelf-id 5
```

Related Commands

Command	Description
show syscon sdp	Displays information about the Shelf Discovery Protocol.
syscon address	Specifies the system controller for a managed shelf.

syscon source-interface

To specify the interface to use for the source address in Shelf Discovery Protocol (SDP) packets, use the **sysconsource-interface**command in global configuration mode. To return to the default source interface for a packet (the interface that sent the packet from the shelf), use the **no** form of this command.

syscon source-interface *type number*
no syscon source-interface

Syntax Description

type number	Type and number of the interface to use for the source IP address.

Command Default

SDP packets use the IP address of the output interface.

Command Modes

Global configuration

Command History

Release	Modification
11.3AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to ensure that all SDP packets sent by the managed shelf have the same source IP address.

Examples

The following example configures a shelf to use the IP address of Ethernet interface 99/1/0:

```
Router# syscon source-address Ethernet99/1/0
```

Related Commands

Command	Description
show syscon sdp	Displays information about the Shelf Discovery Protocol.
syscon shelf-id	Specifies a shelf ID for a managed shelf.

system flowcontrol bus

To set the FIFO overflow error count, use the **system flowcontrol bus** command in global configuration mode. 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	Specifies the original FIFO threshold settings.

Command Default

auto

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXF	Support for this command was introduced on the Supervisor Engine 720 and the Supervisor Engine 32.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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
```

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

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

system jumbomtu

To set the maximum size of the Layer 2 and Layer 3 packets, use the system **jumbo**mtu command in global configuration mode. 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 packet s; valid values are from 1500 to 9216 bytes.

Command Default

mtu-size is **9216** bytes.

Command Modes

Global configuration

Command History

Release	Modification
1.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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 jumbo**mtucommand.

The **system jumbo**mtucommand 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 anything larger than 4000 bytes.

Examples

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

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

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

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

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 g lobal MTU setting.