squelch through system jumbomtu

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 6500/6000 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

Syntax Description

This command has no arguments or keywords.

Syntax Description

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

Command Default

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.

Command Modes

Interface configuration

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.

Usage Guidelines

Cisco 3550, 4000, and 4500 Series Switches

Use the **noswitchport**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 **noswitchport**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 **showrunning-config** privileged EXEC command.

Cisco Catalyst 6500/6000 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 **noswitchport** 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 **switchporthost** 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 **switchporthost** 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 **switchporthost** 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 **switchportnonegotiate** command to force the port to trunk.

Examples

Examples   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
```

Examples   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.

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.

Command	Description
show running-config	Displays the current operating configuration.
switchport mode	Sets the interface type.
switchport trunk	Sets trunk characteristics when the interface is in trunking mode.

switchport access vlan

To set the VLAN when the interface is in access mode, use the **switchportaccessvlan**command in interface 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.

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

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 interface before you can enter the **switchportaccessvlan**command. This action is required only if you have not entered the **switchport** command for the interface.

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.

The no form of the **switchportaccessvlan** com mand resets the access-mode VLAN to the appropriate default VLAN for the device.

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

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

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

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

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

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 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

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.

Command Default   The default is **access** mode.

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

Command Default   The defaults are as follows:

- The mode is dependent on the platform; it should either be **dynamicauto** for platforms that are intended for wiring closets or **dynamicdesirable** for platforms that are intended as backbone switches.

- No mode is set for PVLAN ports.

Command Modes   Interface configuration

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.

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 **dynamicauto** mode, the interface converts the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode.

If you enter **dynamicdesirable** 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

Examples   The following example shows how to set the interface to **access** desirable 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
```

Examples   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
```

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
```

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.

Release	Modification
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 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.
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 **switchporttrunk** 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}**

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.

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.

Command Default

- 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.

Release	Modification
12.2(18)SXD	This command was modified to allow the **switchporttrunkallowedvlan**command to be entered on interfaces where the span destination port is either a trunk or an access port.
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.
12.2(33)SXI4	This command was modified to allow the **switchporttrunk** command to only be applied on the port channel (PO) itself.

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**switchporttrunkencapsulation** 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 **switchporttrunkallowedvlan** 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 **switchporttrunk** command only on the PO. If you enter the **switchporttrunk** 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 **switchporttrunkencapsulationdot1q**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 **switchporttrunkencapsulationisl** command on a port channel containing an interface that does not support ISL-trunk encapsulation, the command is rejected.

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

You can enter the **switchporttrunknativevlantag** 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 **noswitchporttrunknativevlantag** command overrides the **vlandot1qtagnative** command for global tagging.

Note The **switchporttrunknativevlantag** 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 **vlandot1qtagnative** command in global configuration mode.

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

The**dot1qethertype***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 **switchporttrunknativevlan** command resets the native mode VLAN to the appropriate default VLAN for the device.
- The **no** form of the **switchporttrunknativevlantag**command c onfigures the Layer 2 port not to tag native VLAN traffic.
- The **no** form of the **switchporttrunkallowedvlan** command resets the list to the default list, which allows all VLANs.
- The **no** form of the **switchporttrunkpruningvlan**command resets the list to the default list, which enables all VLANs for VTP pruning.
- The **no** form of the **switchporttrunkencapsulationdot1qethertype***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.

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
```

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 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.

Release	Modification
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.