



Configuring Port-Based Traffic Control

This chapter describes how to configure the port-based traffic control features on your Catalyst 2950 or Catalyst 2955 switch.



Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:

- [Configuring Storm Control, page 21-1](#)
- [Configuring Protected Ports, page 21-4](#)
- [Configuring Port Blocking, page 21-5](#)
- [Configuring Port Security, page 21-6](#)
- [Displaying Port-Based Traffic Control Settings, page 21-13](#)

Configuring Storm Control

These sections include storm control configuration information and procedures:

- [Understanding Storm Control, page 21-1](#)
- [Default Storm Control Configuration, page 21-2](#)
- [Configuring Storm Control and Threshold Levels, page 21-2](#)

Understanding Storm Control

A packet storm occurs when a large number of broadcast, unicast, or multicast packets are received on a port. Forwarding these packets can cause the network to slow down or to time out. Storm control is configured for the switch as a whole but operates on a per-port basis. By default, storm control is disabled.

Storm control uses rising and falling thresholds to block and then restore the forwarding of broadcast, unicast, or multicast packets. You can also set the switch to shut down the port when the rising threshold is reached.

Storm control uses one of these methods to measure traffic activity:

- Bandwidth based
- Traffic rate at which packets are received (in packets per second) (available only on non-Long-Reach Ethernet [LRE] Catalyst 2950 switches)

The thresholds can either be expressed as a percentage of the total available bandwidth that can be used by the broadcast, multicast, or unicast traffic, or as the rate at which the interface receives multicast, broadcast, or unicast traffic.

When a switch uses the bandwidth-based method, the rising threshold is the percentage of total available bandwidth associated with multicast, broadcast, or unicast traffic before forwarding is blocked. The falling threshold is the percentage of total available bandwidth below which the switch resumes normal forwarding. In general, the higher the level, the less effective the protection against broadcast storms.

When a non-LRE Catalyst 2950 switch running Cisco IOS Release 12.1(14)EA1 or later uses traffic rates as the threshold values, the rising and falling thresholds are in packets per second. The rising threshold is the rate at which multicast, broadcast, and unicast traffic is received before forwarding is blocked. The falling threshold is the rate below which the switch resumes normal forwarding. In general, the higher the rate, the less effective the protection against broadcast storms.

Default Storm Control Configuration

By default, broadcast, multicast, and unicast storm control is disabled on the switch. The default action is to filter traffic and to not send an SNMP trap.

Configuring Storm Control and Threshold Levels

Beginning in privileged EXEC mode, follow these steps to configure storm control and threshold levels:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Specify the port to configure, and enter interface configuration mode.

	Command	Purpose
Step 3	storm-control { broadcast multicast unicast } level { <i>level</i> [<i>level-low</i>] pps <i>pps</i> [<i>pps-low</i>]}	<p>Configure broadcast, multicast, or unicast storm control.</p> <p>The keywords have these meanings:</p> <ul style="list-style-type: none"> For <i>level</i>, specify the rising threshold level for broadcast, multicast, or unicast traffic as a percentage of the bandwidth. The storm control action occurs when traffic utilization reaches this level. (Optional) For <i>level-low</i>, specify the falling threshold level as a percentage of the bandwidth. This value must be less than the rising suppression value. The normal transmission restarts (if the action is filtering) when traffic drops below this level. For pps <i>pps</i>, specify the rising threshold level for broadcast, multicast, or unicast traffic in packets per second. The storm control action occurs when traffic reaches this level. This option is supported only on non-LRE Catalyst 2950 switches running Cisco IOS Release 12.1(14)EA1 or later. (Optional) For <i>pps-low</i>, specify the falling threshold level in packets per second that can be less than or equal to the rising threshold level. The normal transmission restarts (if the action is filtering) when traffic drops below this level. This option is supported only on non-LRE Catalyst 2950 switches. <p>For <i>pps</i> and <i>pps-low</i>, the range is from 0 to 4294967295.</p>
Step 4	storm-control action { shutdown trap }	<p>Specify the action to be taken when a storm is detected. The default is to filter out the traffic and not to send traps.</p> <ul style="list-style-type: none"> Select the shutdown keyword to error-disable the port during a storm. Select the trap keyword to generate an SNMP trap when a storm is detected.
Step 5	end	Return to privileged EXEC mode.
Step 6	show storm-control [interface] [{ broadcast history multicast unicast }]	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable storm control, use the **no storm-control broadcast level**, the **no storm-control multicast level**, or the **no storm-control unicast level** interface configuration command.

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

Configuring Protected Ports

Some applications require that no traffic be forwarded between ports on the same switch so that one neighbor does not see the traffic generated by another neighbor. In such an environment, the use of protected ports ensures that there is no exchange of unicast, broadcast, or multicast traffic between these ports on the switch.

Protected ports have these features:

- A protected port does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port. Data traffic cannot be forwarded between protected ports at Layer 2; only control traffic, such as PIM packets, is forwarded because these packets are processed by the CPU and forwarded in software. All data traffic passing between protected ports must be forwarded through a Layer 3 device.
- Forwarding behavior between a protected port and a nonprotected port proceeds as usual.
- Protected ports are supported on 802.1Q trunks.

The default is to have no protected ports defined.

You can configure protected ports on a physical interface or an EtherChannel group. When you enable protected ports for a port channel, it is enabled for all ports in the port-channel group.

Both LRE interface ports and CPE device ports can be configured as protected ports. When you use a Cisco 575 LRE CPE or a Cisco 576 LRE 997 CPE device, the **cpe protected** interface configuration command is not available.

When you use a Cisco 585 LRE CPE device (which has multiple Ethernet interfaces), the **switchport protected** command allows devices on different ports of the same CPE device to exchange data locally.

In some cases, you might want to protect individual CPE device ports. You can do this with the **cpe protected** interface configuration command. Devices connected to different ports on the same CPE device cannot exchange data directly but must forward it through a Layer 3 device.

Beginning in privileged EXEC mode, follow these steps to define a port as a protected port:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Specify the interface to configure, and enter interface configuration mode.
Step 3	switchport protected	Configure the interface to be a protected port.
Step 4	end	Return to privileged EXEC mode.
Step 5	show interfaces <i>interface-id</i> switchport	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable protected port, use the **no switchport protected** interface configuration command.

This example shows how to configure a port as a protected port:

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport protected
Switch(config-if)# end
```

Configuring Port Blocking

By default, the switch floods packets with unknown destination MAC addresses to all ports. If unknown unicast and multicast traffic is forwarded to a protected port, there could be security issues.

To prevent unknown unicast or multicast traffic from being forwarded from one port to another, you can configure a port (protected or nonprotected) to block unknown unicast or multicast packets.



Note

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

The port blocking feature is only supported on these switches:

- Catalyst 2950 Long-Reach Ethernet (LRE) switches running Cisco IOS Release 12.1(14)EA1 or later
- Catalyst 2950G-12-EI, 2950G-24-EI, 2950G-24-EI-DC, 2950G-48-EI, and 2955 switches running Cisco IOS Release 12.1(19)EA1 or later

Blocking Flooded Traffic on an Interface



Note

The interface can be a physical interface or an EtherChannel group. When you block multicast or unicast traffic for a port channel, it is blocked on all ports in the port channel group.

Beginning in privileged EXEC mode, follow these steps to disable the flooding of multicast and unicast packets to an interface:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Specify the interface to configure, and enter interface configuration mode.
Step 3	switchport block multicast	Block unknown multicast forwarding to the port.
Step 4	switchport block unicast	Block unknown unicast forwarding to the port.
Step 5	end	Return to privileged EXEC mode.
Step 6	show interfaces <i>interface-id</i> switchport	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To return the interface to the default condition where no traffic is blocked, use the **no switchport block {multicast | unicast}** interface configuration commands.

This example shows how to block unicast and multicast flooding on a port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
Switch(config-if)# end
```

Resuming Normal Forwarding on a Port

Beginning in privileged EXEC mode, follow these steps to resume normal forwarding on a port:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Specify the interface to configure, and enter interface configuration mode.
Step 3	no switchport block multicast	Enable unknown multicast flooding to the port.
Step 4	no switchport block unicast	Enable unknown unicast flooding to the port.
Step 5	end	Return to privileged EXEC mode
Step 6	show interfaces <i>interface-id</i> switchport	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Configuring Port Security

You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses.

This section includes information about these topics:

- [Understanding Port Security, page 21-6](#)
- [Default Port Security Configuration, page 21-8](#)
- [Port Security Configuration Guidelines, page 21-8](#)
- [Enabling and Configuring Port Security, page 21-9](#)
- [Enabling and Configuring Port Security Aging, page 21-11](#)

Understanding Port Security

This section includes information about:

- [Secure MAC Addresses, page 21-6](#)
- [Security Violations, page 21-7](#)

Secure MAC Addresses

You can configure these types of secure MAC addresses:

- Static secure MAC addresses—These are manually configured by using the **switchport port-security mac-address** *mac-address* interface configuration command, stored in the address table, and added to the switch running configuration.
- Dynamic secure MAC addresses—These are dynamically learned, stored only in the address table, and removed when the switch restarts.

- *Sticky* secure MAC addresses—These can be dynamically learned or manually configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, the interface does not need to dynamically relearn them when the switch restarts. Although sticky secure addresses can be manually configured, we do not recommend it.

You can configure an interface to convert the dynamic MAC addresses to sticky secure MAC addresses and to add them to the running configuration by enabling *sticky learning*. To enable sticky learning, enter the **switchport port-security mac-address sticky** interface configuration command. When you enter this command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses.

The sticky secure MAC addresses do not automatically become part of the configuration file, which is the startup configuration used each time the switch restarts. If you save the sticky secure MAC addresses in the configuration file, when the switch restarts, the interface does not need to relearn these addresses. If you do not save the configuration, they are lost.

If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.

A secure port can have from 1 to 132 associated secure addresses. The total number of available secure addresses on the switch is 1024.

Security Violations

It is a security violation when one of these situations occurs:

- The maximum number of secure MAC addresses have been added to the address table, and a station whose MAC address is not in the address table attempts to access the interface.
- An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.

You can configure the interface for one of three violation modes, based on the action to be taken if a violation occurs:

- **protect**—When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.
- **restrict**—When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. In this mode, you are notified that a security violation has occurred. Specifically, an SNMP trap is sent, a syslog message is logged, and the violation counter increments.
- **shutdown**—In this mode, a port security violation causes the interface to immediately become error-disabled, and turns off the port LED. It also sends an SNMP trap, logs a syslog message, and increments the violation counter. When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shutdown** interface configuration commands. This is the default mode.

Table 21-1 shows the violation mode and the actions taken when you configure an interface for port security.

Table 21-1 Security Violation Mode Actions

Violation Mode	Traffic is forwarded ¹	Sends SNMP trap	Sends syslog message	Displays error message ²	Violation counter increments	Shuts down port
protect	No	No	No	No	No	No
restrict	No	Yes	Yes	No	Yes	No
shutdown	No	Yes	Yes	No	Yes	Yes

1. Packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses.
2. The switch will return an error message if you manually configure an address that would cause a security violation.

Default Port Security Configuration

Table 21-2 shows the default port security configuration for an interface.

Table 21-2 Default Port Security Configuration

Feature	Default Setting
Port security	Disabled.
Maximum number of secure MAC addresses	One.
Violation mode	Shutdown.
Sticky address learning	Disabled.
Port security aging	Disabled. Aging time is 0. When enabled, the default type is absolute .

Port Security Configuration Guidelines

Follow these guidelines when configuring port security:

- Port security can only be configured on static access ports.
- A secure port cannot be a dynamic access port or a trunk port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Fast EtherChannel or Gigabit EtherChannel port group.
- You cannot configure static secure or sticky secure MAC addresses on a voice VLAN.
- When you enable port security on an interface that is also configured with a voice VLAN, you must set the maximum allowed secure addresses on the port to at least two plus the maximum number of secure addresses allowed on the access VLAN. When the port is connected to a Cisco IP phone, the IP phone requires up to two MAC addresses. The address of the IP phone is learned on the voice VLAN, and it might or might not be learned on the access VLAN. Connecting a PC to the IP phone requires additional MAC addresses
- If any type of port security is enabled on the access VLAN, dynamic port security is automatically enabled on the voice VLAN.

- When a voice VLAN is configured on a secure port that is also configured as a sticky secure port, all addresses seen on the voice VLAN are learned as dynamic secure addresses, and all addresses seen on the access VLAN (to which the port belongs) are learned as sticky secure addresses.
- You cannot configure port security on a per-VLAN basis.
- The switch does not support port security aging of sticky secure MAC addresses.
- The **protect** and **restrict** options cannot be simultaneously enabled on an interface.

Table 21-3 summarizes port security compatibility with other features configured on a port.

Table 21-3 Port Security Compatibility with Other Catalyst 2950 and 2955 Features

Type of Port	Compatible with Port Security
DTP ¹ port ²	No
Trunk port	No
Dynamic-access port ³	No
SPAN source port	Yes
SPAN destination port	No
EtherChannel	No
Protected port	Yes
802.1x port	Yes
Voice VLAN port ⁴	Yes

1. DTP = Dynamic Trunking Protocol
2. A port configured with the **switchport mode dynamic** interface configuration command.
3. A VLAN Query Protocol (VQP) port configured with the **switchport access vlan dynamic** interface configuration command.
4. You must set the maximum allowed secure addresses on the port to two plus the maximum number of secure addresses allowed on the access VLAN.

Enabling and Configuring Port Security

Beginning in privileged EXEC mode, follow these steps to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Specify the interface to configure, and enter interface configuration mode.
Step 3	switchport mode access	Set the interface mode as access ; an interface in the default mode (dynamic desirable) cannot be configured as a secure port.
Step 4	switchport port-security	Enable port security on the interface.
Step 5	switchport port-security maximum <i>value</i>	(Optional) Set the maximum number of secure MAC addresses for the interface. The range is 1 to 132; the default is 1.

	Command	Purpose
Step 6	<code>switchport port-security violation {protect restrict shutdown}</code>	<p>(Optional) Set the violation mode, the action to be taken when a security violation is detected, as one of these:</p> <ul style="list-style-type: none"> • protect—When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred. • restrict—When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. In this mode, you are notified that a security violation has occurred. Specifically, an SNMP trap is sent, a syslog message is logged, and the violation counter increments. • shutdown—In this mode, a port security violation causes the interface to immediately become error-disabled, and turns off the port LED. It also sends an SNMP trap, logs a syslog message, and increments the violation counter. <p>Note When a secure port is in the error-disabled state, you can bring it out of this state by entering the errdisable recovery cause psecure-violation global configuration command, or you can manually re-enable it by entering the shutdown and no shutdown interface configuration commands.</p>
Step 7	<code>switchport port-security mac-address mac-address</code>	<p>(Optional) Enter a static secure MAC address for the interface, repeating the command as many times as necessary. You can use this command to enter the maximum number of secure MAC addresses. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned.</p> <p>Note If you enable sticky learning after you enter this command, the secure addresses that were dynamically learned are converted to sticky secure MAC addresses and are added to the running configuration.</p>
Step 8	<code>switchport port-security mac-address sticky</code>	(Optional) Enable sticky learning on the interface.
Step 9	<code>end</code>	Return to privileged EXEC mode.
Step 10	<code>show port-security</code>	Verify your entries.
Step 11	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

To return the interface to the default condition as not a secure port, use the **no switchport port-security** interface configuration command. If you enter this command when sticky learning is enabled, the sticky secure addresses remain part of the running configuration but are removed from the address table. All addresses are now dynamically learned.

To return the interface to the default number of secure MAC addresses, use the **no switchport port-security maximum value** interface configuration command.

To return the violation mode to the default condition (shutdown mode), use the **no switchport port-security violation {protect | restrict}** interface configuration command.

To disable sticky learning on an interface, use the **no switchport port-security mac-address sticky** interface configuration command. The interface converts the sticky secure MAC addresses to dynamic secure addresses.

To delete a static secure MAC address from the address table, use the **clear port-security configured address mac-address** privileged EXEC command. To delete all the static secure MAC addresses on an interface, use the **clear port-security configured interface interface-id** privileged EXEC command.

To delete a dynamic secure MAC address from the address table, use the **clear port-security dynamic address mac-address** privileged EXEC command. To delete all the dynamic addresses on an interface, use the **clear port-security dynamic interface interface-id** privileged EXEC command.

To delete a sticky secure MAC addresses from the address table, use the **clear port-security sticky address mac-address** privileged EXEC command. To delete all the sticky addresses on an interface, use the **clear port-security sticky interface interface-id** privileged EXEC command.

This example shows how to enable port security on a port and to set the maximum number of secure addresses to 50. The violation mode is the default, no static secure MAC addresses are configured, and sticky learning is enabled.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 50
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# end
```

This example shows how to configure a static secure MAC address on a port and enable sticky learning:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 0000.02000.0004
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# end
```

Enabling and Configuring Port Security Aging

You can use port security aging to set the aging time for static and dynamic secure addresses on a port. Two types of aging are supported per port:

- Absolute—The secure addresses on the port are deleted after the specified aging time.
- Inactivity—The secure addresses on the port are deleted only if the secure addresses are inactive for the specified aging time.

Use this feature to remove and add PCs on a secure port without manually deleting the existing secure MAC addresses and to still limit the number of secure addresses on a port. You can enable or disable the aging of statically configured secure addresses on a per-port basis.

Beginning in privileged EXEC mode, follow these steps to configure port security aging:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Specify the port on which you want to enable port security aging, and enter interface configuration mode. Note The switch does not support port security aging of sticky secure addresses.
Step 3	switchport port-security aging { static time <i>time</i> type { absolute inactivity } }	Enable or disable static aging for the secure port, or set the aging time or type. Enter static to enable aging for statically configured secure addresses on this port. For <i>time</i> , specify the aging time for this port. The valid range is from 0 to 1440 minutes. If the time is equal to 0, aging is disabled for this port. For type , select one of these keywords: <ul style="list-style-type: none">• absolute—Sets the aging type as absolute aging. All the secure addresses on this port age out after the specified time (minutes) lapses and are removed from the secure address list. Note The absolute aging time could vary by 1 minute, depending on the sequence of the system timer. <ul style="list-style-type: none">• inactivity—Sets the aging type as inactivity aging. The secure addresses on this port age out only if there is no data traffic from the secure source addresses for the specified time period.
Step 4	end	Return to privileged EXEC mode.
Step 5	show port-security [interface <i>interface-id</i>] [address]	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable port security aging for all secure addresses on a port, use the **no switchport port-security aging time** interface configuration command. To disable aging for only statically configured secure addresses, use the **no switchport port-security aging static** interface configuration command.

This example shows how to set the aging time as 2 hours for the secure addresses on a port:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport port-security aging time 120
```

This example shows how to set the aging time as 2 minutes for the inactivity aging type with aging enabled for the configured secure addresses on the interface:

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

You can verify the previous commands by entering the **show port-security interface** *interface-id* privileged EXEC command.

Displaying Port-Based Traffic Control Settings

The **show interfaces *interface-id* switchport** privileged EXEC command displays (among other characteristics) the interface traffic suppression and control configuration. The **show storm-control** and **show port-security** privileged EXEC commands display those features.

To display traffic control information, use one or more of the privileged EXEC commands in [Table 21-4](#).

Table 21-4 Commands for Displaying Traffic Control Status and Configuration

Command	Purpose
show interfaces [<i>interface-id</i>] switchport	Displays the administrative and operational status of all switching (nonrouting) ports or the specified port, including port blocking and port protection settings.
show storm-control [<i>interface-id</i>] [broadcast multicast unicast]	Displays storm control suppression levels set on all interfaces or the specified interface for the specified traffic type or for broadcast traffic if no traffic type is entered.
show port-security [interface <i>interface-id</i>]	Displays port security settings for the switch or for the specified interface, including the maximum allowed number of secure MAC addresses for each interface, the number of secure MAC addresses on the interface, the number of security violations that have occurred, and the violation mode.
show port-security [interface <i>interface-id</i>] address	Displays all secure MAC addresses configured on all switch interfaces or on a specified interface with aging information for each address.

