



Configuring Port-Based Traffic Control

This chapter describes how to configure the port-based traffic control features on the Catalyst 2970 switch.



Note

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

This chapter consists of these sections:

- [Configuring Storm Control, page 15-1](#)
- [Configuring Protected Ports, page 15-4](#)
- [Configuring Port Blocking, page 15-6](#)
- [Configuring Port Security, page 15-7](#)
- [Displaying Port-Based Traffic Control Settings, page 15-12](#)

Configuring Storm Control

These sections include storm control configuration information and procedures:

- [Understanding Storm Control, page 15-1](#)
- [Default Storm Control Configuration, page 15-3](#)
- [Enabling Storm Control, page 15-3](#)

Understanding Storm Control

Storm control prevents switchports on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation or in the network configuration can cause a storm.

Storm control (or traffic suppression) monitors incoming traffic statistics over a time period and compares the measurement with a predefined suppression level threshold. The threshold represents the percentage of the total available bandwidth of the port. The switch supports separate storm control thresholds for broadcast, multicast, and unicast traffic. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

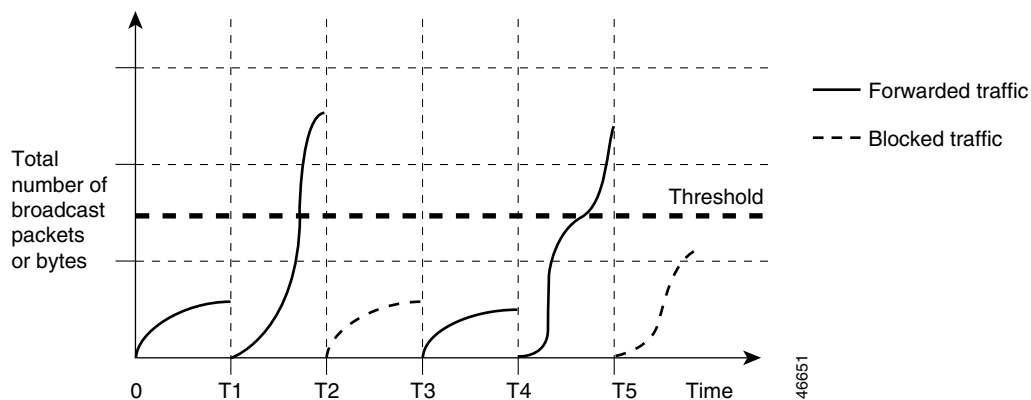
**Note**

When the storm control threshold for multicast traffic is reached, all multicast traffic except control traffic, such as bridge protocol data unit (BDPU) and Cisco Discovery Protocol (CDP) frames, are blocked.

When storm control is enabled, the switch monitors packets passing from an interface to the switching bus and determines if the packet is unicast, multicast, or broadcast. The switch monitors the number of broadcast, multicast, or unicast packets received within a 200-millisecond time interval, and when a threshold for one type of traffic is reached, that type of traffic is dropped. This threshold is specified as a percentage of total available bandwidth that can be used by broadcast (multicast or unicast) traffic.

The graph in [Figure 15-1](#) shows broadcast traffic patterns on an interface over a given period of time. The example can also be applied to multicast and unicast traffic. In this example, the broadcast traffic being forwarded exceeded the configured threshold between time intervals T1 and T2 and between T4 and T5. When the amount of specified traffic exceeds the threshold, all traffic of that kind is dropped for the next time period. Therefore, broadcast traffic is blocked during the intervals following T2 and T5. At the next time interval (for example, T3), if broadcast traffic does not exceed the threshold, it is again forwarded.

Figure 15-1 Broadcast Storm Control Example



The combination of the storm-control suppression level and the 200-millisecond time interval control the way the storm control algorithm works. A higher threshold allows more packets to pass through. A threshold value of 100 percent means that no limit is placed on the traffic. A value of 0.0 means that all broadcast, multicast, or unicast traffic on that port is blocked.

**Note**

Because packets do not arrive at uniform intervals, the 200-millisecond time interval during which traffic activity is measured can affect the behavior of storm control.

The switch continues to monitor traffic on the port, and when the utilization level is below the threshold level, the type of traffic that was dropped is forwarded again.

You use the **storm-control** interface configuration commands to set the threshold value for each traffic type.

**Note**

Although visible in the command-line interface (CLI) online help, the **switchport broadcast**, **switchport multicast**, and **switchport unicast** interface configuration commands for setting suppression levels are not available. These commands are obsolete, replaced by the **storm-control** interface configuration commands.

Default Storm Control Configuration

By default, unicast, broadcast, and multicast storm control is disabled on the switch interfaces; that is, the suppression level is 100 percent.

Enabling Storm Control

You enable storm control on an interface and enter the percentage of total available bandwidth that you want to be used by a particular type of traffic; entering 100 percent allows all traffic. However, because of hardware limitations and the way in which packets of different sizes are counted, threshold percentages are approximations. Depending on the sizes of the packets making up the incoming traffic, the actual enforced threshold might differ from the configured level by several percentage points.

**Note**

Storm control is supported only on physical interfaces; it is not supported on EtherChannel port channels even though the command is available in the CLI.

Beginning in privileged EXEC mode, follow these steps to enable a particular type of storm control:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Enter interface configuration mode, and enter the type and number of the physical interface to configure, for example gigabitethernet0/1 .
Step 3	storm-control broadcast level <i>level</i> [<i>.level</i>]	Specify the broadcast traffic suppression level for an interface as a percentage of total bandwidth. The level can be from 1 to 100; the optional fraction of a level can be from 0 to 99. A threshold value of 100 percent means that no limit is placed on broadcast traffic. A value of 0.0 means that all broadcast traffic on that port is blocked.
Step 4	storm-control multicast level <i>level</i> [<i>.level</i>]	Specify the multicast traffic suppression level for an interface as a percentage of total bandwidth. The level can be from 1 to 100; the optional fraction of a level can be from 0 to 99. A threshold value of 100 percent means that no limit is placed on broadcast traffic. A value of 0.0 means that all multicast traffic on that port is blocked.
Step 5	storm-control unicast level <i>level</i> [<i>.level</i>]	Specify the unicast traffic suppression level for an interface as a percentage of total bandwidth. The level can be from 1 to 100; the optional fraction of a level can be from 0 to 99. A threshold value of 100 percent means that no limit is placed on broadcast traffic. A value of 0.0 means that all unicast traffic on that port is blocked.
Step 6	end	Return to privileged EXEC mode.

	Command	Purpose
Step 7	<code>show storm-control [interface-id] [broadcast multicast unicast]</code>	Verify the storm control suppression levels set on the interface for the specified traffic type. If you do not enter a traffic type, broadcast storm control settings are displayed.
Step 8	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

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

This example shows how to set the multicast storm control level at 70.5 percent on Gigabit Ethernet interface 0/17 and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/17
Switch(config-if)# storm-control multicast level 70.5
Switch(config-if)# end
Switch# show storm-control gigabitethernet0/17 multicast
Interface  Filter State    Level    Current
-----  -
Gi0/17    Forwarding  70.50%  0.00%
```

This example shows how to disable the multicast storm control on Gigabit Ethernet interface 0/17 and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/17
Switch(config-if)# no storm-control multicast level
Switch(config-if)# end
Switch# show storm-control gigabitethernet0/17 multicast
Interface  Filter State    Level    Current
-----  -
Gi0/17    inactive    100.00%  N/A
```

Configuring Protected Ports

Some applications require that no traffic be forwarded at Layer 2 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. Traffic cannot be forwarded between protected ports at Layer 2; all 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.

Default Protected Port Configuration

The default is to have no protected ports defined.

Protected Port Configuration Guidelines

You can configure protected ports on a physical interface (for example, Gigabit Ethernet 0/1) or an EtherChannel group (for example, port-channel 5). When you enable protected ports for a port channel, it is enabled for all ports in the port-channel group.

Configuring a Protected Port

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>	Enter interface configuration mode, and enter the type and number of the interface to configure, for example gigabitethernet0/1 .
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 Gigabit Ethernet interface 0/1 as a protected port:

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

Configuring Port Blocking

By default, the switch floods packets with unknown destination MAC addresses out of 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 block a port (protected or nonprotected) from flooding unknown unicast or multicast packets to other ports.

Default Port Blocking Configuration

The default is to not block flooding of unknown multicast and unicast traffic out of a port, but to flood these packets to all ports.

Blocking Flooded Traffic on an Interface



Note

The interface can be a physical interface (for example, Gigabit Ethernet 0/1) or an EtherChannel group (for example, port-channel 5). 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 from an interface:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface interface-id</code>	Enter interface configuration mode, and enter the type and number of the interface to configure, for example <code>gigabitethernet0/1</code> .
Step 3	<code>switchport block multicast</code>	Block unknown multicast forwarding out of the port.
Step 4	<code>switchport block unicast</code>	Block unknown unicast forwarding out of the port.
Step 5	<code>end</code>	Return to privileged EXEC mode.
Step 6	<code>show interfaces interface-id switchport</code>	Verify your entries.
Step 7	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

To return the interface to the default condition where no traffic is blocked and normal forwarding occurs on the port, use the `no switchport block {multicast | unicast}` interface configuration commands.

This example shows how to block unicast and multicast flooding on Gigabit Ethernet interface 0/1:

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

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. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port.

If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, when the MAC address of a station attempting to access the port is different from any of the identified secure MAC addresses, a security violation occurs. Also, if a station with a secure MAC address configured or learned on one secure port attempts to access another secure port, a violation is flagged.

These sections include port security configuration information and procedures:

- [Understanding Port Security, page 15-7](#)
- [Default Port Security Configuration, page 15-8](#)
- [Configuration Guidelines, page 15-9](#)
- [Enabling and Configuring Port Security, page 15-9](#)
- [Enabling and Configuring Port Security Aging, page 15-11](#)

Understanding Port Security

This section contains information about these topics:

- [Secure MAC Addresses, page 15-7](#)
- [Security Violations, page 15-8](#)

Secure MAC Addresses

A secure port can have from 1 to 128 associated secure addresses. You configure the maximum number of secure addresses by using the **switchport port-security maximum *value*** interface configuration command.

**Note**

If you try to set the maximum value to a number less than the number of secure addresses already configured on an interface, the command is rejected.

After you have set the maximum number of secure MAC addresses on a port, the secure addresses are included in an address table in one of these ways:

- You can configure all secure MAC addresses by using the **switchport port-security mac-address *mac-address*** interface configuration command.
- You can allow the port to dynamically configure secure MAC addresses with the MAC addresses of connected devices.
- You can configure a number of addresses and allow the rest to be dynamically configured.

**Note**

If the port shuts down, all dynamically learned addresses are removed.

Once the maximum number of secure MAC addresses is configured, they are stored in an address table. Setting a maximum number of addresses to one and configuring the MAC address of an attached device ensures that the device has the full bandwidth of the port.

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 maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value.
- **restrict**—a port security violation restricts data.
- **shutdown**—a port security violation causes the interface to shut down immediately. 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 shut down** interface configuration commands. This is the default mode.



Note

When the maximum number of secure addresses on an interface is reached and a user tries to configure an address, the command has no effect.

Default Port Security Configuration

Table 15-1 shows the default port security configuration for an interface.

Table 15-1 Default Port Security Configuration

Feature	Default Setting
Port security	Disabled on a port.
Maximum number of secure MAC addresses per port	1. (The range is from 1 to 128.)
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded.
Port security aging	Disabled. Aging time is 0. Static aging is disabled. Type is absolute.

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 Switch Port Analyzer (SPAN).
- A secure port cannot belong to a Gigabit EtherChannel port group.
- A secure port cannot be an 802.1X port.
- You cannot configure static secure MAC addresses in the voice VLAN.
- When you enter a maximum secure address value for an interface, if the new value is greater than the previous value, the new value overrides the previously configured value. If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.
- Although the maximum number of secured addresses per port is 128, the maximum number per system is 1024.

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>	Enter interface configuration mode, and enter the physical interface to configure, for example gigabitethernet0/1 .
Step 3	switchport mode access	Set the interface switchport mode as access; an interface in the default mode (dynamic auto) 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 128; the default is 1.

	Command	Purpose
Step 6	switchport port-security violation {protect restrict shutdown}	<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 port secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value. • restrict—A port security violation restricts data and causes the SecurityViolation counter to increment. • shutdown—The interface is error-disabled when a violation occurs. <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	switchport port-security mac-address mac-address	(Optional) Enter a secure MAC address for the interface. 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.
Step 8	end	Return to privileged EXEC mode.
Step 9	show port-security show port-security address show port-security interface interface-id	Verify your entries.
Step 10	copy running-config startup-config	(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. 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 {protocol | restrict}** interface configuration command.

To delete a static secure MAC address from the address table, use the **no switchport port-security mac-address mac-address** interface configuration command. Enter the command once for each static MAC address to be deleted.

This example shows how to enable port security on Gigabit Ethernet port 0/1 and to set the maximum number of secure addresses to 50. The violation mode is the default and no static secure MAC addresses are configured.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 50
```

This example shows how to configure a static secure MAC address on Gigabit Ethernet port 0/12:

```
Switch(config)# interface gigabitethernet0/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 0000.02000.0004
```

Enabling and Configuring Port Security Aging

You can use port security aging to set the aging time for all 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 devices 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	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface interface-id</code>	Enter interface configuration mode for the port on which you want to enable port security aging.
Step 3	<code>switchport port-security aging {static time time type {absolute inactivity}}</code>	<p>Enable or disable static aging for the secure port, or set the aging time or type.</p> <p>Enter static to enable aging for statically configured secure addresses on this port.</p> <p>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.</p> <p>For type, select one of these keywords:</p> <ul style="list-style-type: none"> • absolute—Sets the aging type as absolute aging. All the secure addresses on this port age out exactly after the time (minutes) specified lapses and are removed from the secure address list. • 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	<code>end</code>	Return to privileged EXEC mode.
Step 5	<code>show port-security [interface interface-id] [address]</code>	Verify your entries.
Step 6	<code>copy running-config startup-config</code>	(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 Gigabit Ethernet interface 0/1:

```
Switch(config)# interface gigabitethernet0/1
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 interfaces counters** privileged EXEC commands display the count of discarded packets. 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 15-2](#).

Table 15-2 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 interfaces [<i>interface-id</i>] counters broadcast	Displays the storm-control broadcast suppression discard counter with the number of packets discarded for all interfaces or the specified interface.
show interfaces [<i>interface-id</i>] counters multicast	Displays the storm-control multicast suppression discard counter with the number of packets discarded for all interfaces or the specified interface.
show interfaces [<i>interface-id</i>] counters unicast	Displays the storm-control unicast suppression discard counter with the number of packets discarded for all interfaces or the specified interface.
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.