



Configuring Port-Based Traffic Control

This chapter describes how to configure the port-based traffic control features on your 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 17-1](#)
- [Configuring Protected Ports, page 17-3](#)
- [Configuring Port Security, page 17-4](#)
- [Displaying Port-Based Traffic Control Settings, page 17-12](#)

Configuring Storm Control

These sections include storm control configuration information and procedures:

- [Understanding Storm Control, page 17-1](#)
- [Default Storm Control Configuration, page 17-2](#)
- [Enabling Storm Control, page 17-2](#)
- [Disabling Storm Control, page 17-3](#)

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 a bandwidth-based method to measure traffic activity. The thresholds are expressed as a percentage of the total available bandwidth that can be used by the broadcast, multicast, or unicast traffic.

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.

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.

Enabling Storm Control

Beginning in privileged EXEC mode, follow these steps to enable storm control:

	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.
Step 3	storm-control { broadcast multicast unicast } level <i>level</i> [<i>level-low</i>]	Configure broadcast, multicast, or unicast storm control. Specify the rising threshold level for broadcast, multicast, or unicast traffic. The storm control action occurs when traffic utilization reaches this level. (Optional) Specify the falling threshold level. The normal transmission restarts (if the action is filtering) when traffic drops below this level.
Step 4	storm-control action { shutdown trap }	Specify the action to be taken when a storm is detected. The default is to filter out the traffic and not to send traps. 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.

Disabling Storm Control

Beginning in privileged EXEC mode, follow these steps to disable storm control:

	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.
Step 3	no storm-control { broadcast multicast unicast } level	Disable port storm control.
Step 4	no storm-control action { shutdown trap }	Disable the specified storm control action.
Step 5	end	Return to privileged EXEC mode.
Step 6	show storm-control { broadcast multicast unicast }	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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. 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.

The default is to have no protected ports defined.

A protected port cannot be a secure port.

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.

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 type and number of the physical interface to configure, for example gigabitethernet0/1 , 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.

	Command	Purpose
Step 5	<code>show interfaces interface-id switchport</code>	Verify your entries.
Step 6	<code>copy running-config startup-config</code>	(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 and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport protected
Switch(config-if)# end
Switch# show interfaces gigabitethernet0/1 switchport
Name: Gi0/1
Switchport: Enabled

<output truncated>

Protected: True
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
```

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 17-4](#)
- [Default Port Security Configuration, page 17-6](#)
- [Port Security Configuration Guidelines, page 17-7](#)
- [Enabling and Configuring Port Security, page 17-7](#)
- [Enabling and Configuring Port Security Aging, page 17-10](#)

Understanding Port Security

This section contains information about these topics:

- [Secure MAC Addresses, page 17-5](#)
- [Security Violations, page 17-6](#)

Secure MAC Addresses

A secure port can have from 1 to 132 associated secure addresses. 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.

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.

The switch supports 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 configured, stored only in the address table, and removed when the switch restarts.
- **Sticky secure MAC addresses**—These are dynamically configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, when the switch restarts, the interface does not need to dynamically reconfigure them.

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 interface adds all the sticky secure MAC addresses to the running configuration.

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 sticky secure addresses, they are lost.

This is an example of text from the running configuration when sticky learning is enabled on an interface:

```
<output truncated>
```

```
!  
interface FastEthernet0/2  
  switchport mode access  
  switchport port-security  
  switchport port-security maximum 6  
  switchport port-security aging time 5  
  switchport port-security aging static  
  switchport port-security mac-address sticky  
  switchport port-security mac-address 0000.0000.000b  
  switchport port-security mac-address sticky 0000.0000.4141  
  switchport port-security mac-address sticky 0000.0000.5050  
  no ip address
```

```
<output truncated>
```

If port security is disabled, the sticky secure MAC addresses remain in the running configuration.

To disable sticky learning, enter the **no switchport port-security mac-address sticky** interface configuration command. If sticky learning is disabled or the running configuration is removed, the sticky secure MAC addresses remain part of the running configuration but are removed from the address table. The addresses that were removed can be dynamically reconfigured and added to the address table as dynamic addresses.

**Note**

If sticky learning is disabled, when the switch restarts or the interface shuts down, all the addresses that were dynamically learned are removed.

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 and causes the SecurityViolation counter to increment. It also sends an SNMP trap when an address-security violation occurs.
- **shutdown**—the interface is error-disabled when a security violation occurs. 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.

Default Port Security Configuration

Table 17-1 shows the default port security configuration for an interface.

Table 17-1 Default Port Security Configuration

Feature	Default Setting
Port security	Disabled on a port
Maximum number of secure MAC addresses	1
Violation mode	Shutdown. The interface is error-disabled when a security violation occurs. 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.

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 protected port.
- A secure port cannot be a destination port for Switch Port Analyzer (SPAN).
- A secure port cannot belong to a Fast EtherChannel or 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 enable port security on a voice VLAN port, you must set the maximum allowed secure addresses on the port to at least two. When the port is connected to a Cisco IP phone, the IP phone requires two MAC addresses: one for the access VLAN and the other for the voice VLAN. Connecting a PC to the IP phone requires additional MAC addresses.

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 type and number of the physical interface to configure, for example gigabitethernet0/1 , 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 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 and sends an SNMP trap. • shutdown—The interface is error-disabled when a security 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	<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>switchport port-security mac-address sticky mac-address</code>	<p>(Optional) Enter a sticky secure MAC address, repeating the command as many times as necessary. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned, are converted to sticky secure MAC addresses, and are added to the running configuration.</p> <p>Note If you do not enable sticky learning before this command is entered, an error message appears, and you cannot enter a sticky secure MAC address.</p>
Step 10	<code>end</code>	Return to privileged EXEC mode.
Step 11	<code>show port-security</code> <code>show port-security address</code> <code>show port-security interface interface-id</code>	Verify your entries.
Step 12	<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. The addresses that were removed can be dynamically reconfigured and added to the address table as dynamic addresses.

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 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 **no switchport port-security mac-address** *mac-address* interface configuration command.

To delete a dynamic secure MAC address from the address table, use the **clear port-security dynamic address** *mac-addr* 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 sticky secure MAC addresses from the address table, disable sticky learning, which converts the sticky secure MAC addresses to dynamic secure addresses. Use the **no switchport port-security mac-address sticky** interface configuration command. Delete dynamic secure addresses on an interface by using the **clear port-security dynamic interface** *interface-id* privileged EXEC command. To delete a dynamic secure MAC address, use the **clear port-security dynamic address** *mac-addr* privileged EXEC command.

This example shows how to enable port security on Fast Ethernet port 1 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
Switch# show port-security interface fastethernet0/1
Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses :50
Total MAC Addresses: 11
Configured MAC Addresses: 0
Sticky MAC Addresses :11
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
```

This example shows how to configure a static secure MAC address and a sticky secure MAC address on Fast Ethernet port 12 and verify the configuration:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet0/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
```

```

Switch(config-if)# switchport port-security mac-address 0000.0200.0004
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0008.a343.b581
Switch(config-if)# end
Switch# show port-security address
=
Secure Mac Address Table
-----
Vlan    Mac Address          Type                Ports    Remaining Age
        (mins)
-----
  1     0000.0000.000a      SecureDynamic       Fa0/1    -
  1     0000.0002.0300      SecureDynamic       Fa0/1    -
  1     0000.0200.0003      SecureConfigured    Fa0/1    -
  1     0000.0200.0004      SecureConfigured    Fa0/12   -
  1     0003.fd62.1d40      SecureConfigured    Fa0/5    -
  1     0003.fd62.1d45      SecureConfigured    Fa0/5    -
  1     0003.fd62.21d3      SecureSticky        Fa0/5    -
  1     0005.7428.1a45      SecureSticky        Fa0/8    -
  1     0005.7428.1a46      SecureSticky        Fa0/8    -
  1     0006.1218.2436      SecureSticky        Fa0/8    -
  1     0008.a343.b581      SecureSticky        Fa0/12   -
-----
Total Addresses in System :11
Max Addresses limit in System :1024

```

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 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.
Step 3	switchport port-security aging { static time <i>time</i> type { absolute inactivity }}	<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	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 the Fast Ethernet interface 0/1:

```
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 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 17-2](#).

Table 17-2 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 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.