CHAPTER 17

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 *Catalyst 2950 Desktop Switch 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 17-3
- Configuring and Enabling Port Security Aging, page 17-6
- Displaying Port-Based Traffic Control Settings, page 17-7

Configuring 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.

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** *interface-id*	Enter interface configuration mode, and enter the port to configure.
Step 3	**storm-control** {**broadcast** | **multicast** | **unicast**} **level** *level* [*level-low*]	Configure broadcast, multicast, or unicast storm control. Specify the rising threshold level for either 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 out 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 | multicast | unicast | history}]**	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** *interface-id*	Enter interface configuration mode, and enter the port to configure.
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 by the Layer 2 protocol between ports on the same switch. In such an environment, there is no exchange of unicast, broadcast, or multicast traffic between ports on the switch, and traffic between ports on the same switch is forwarded through a Layer 3 device such as a router.

To meet this requirement, you can configure Catalyst 2950 ports as protected ports (also referred to as private VLAN edge ports). Protected ports do not forward any traffic to protected ports on the same switch. This means that all traffic passing between protected ports—unicast, broadcast, and multicast—must be forwarded through a Layer 3 device. Protected ports can forward any type of traffic to nonprotected ports, and they forward as usual to all ports on other switches. Dynamically learnt addresses are not retained if the switch is reloaded.

Note When both SPAN source and SPAN destination ports are protected ports, traffic is forwarded from the SPAN source to the SPAN destination. Therefore, do not configure both SPAN source and SPAN destination as protected ports.

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** *interface-id*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**switchport protected**	Enable protected port on the port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interfaces switchport**	Verify that the protected port option is enabled.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** version of the **switchport protected** interface configuration command to disable the protected port option.

Configuring Port Security

Secured ports restrict a port to a user-defined group of stations. When you assign secure addresses to a secure port, the switch does not forward any packets with source addresses outside the defined group of addresses. If you define the address table of a secure port to contain only one address, the workstation or server attached to that port is guaranteed the full bandwidth of the port. As part of securing the port, you can also define the size of the address table for the port.

Note Port security can only be configured on static access ports.

Secured ports generate address-security violations under these conditions:

- The address table of a secured port is full, and the address of an incoming packet is not found in the table.
- An incoming packet has a source address assigned as a secure address on another port.

Limiting the number of devices that can connect to a secure port has these advantages:

- Dedicated bandwidth—If the size of the address table is set to 1, the attached device is guaranteed the full bandwidth of the port.
- Added security—Unknown devices cannot connect to the port.

These options validate port security or show security violations:

Interface	Port to secure.
Security	Enable port security on the port.
Trap	Issue a trap when an address-security violation occurs.
Shutdown Port	The interface is error-disabled when a security violation occurs. **Note** When a secure port is in the error-disabled state, you can bring it out of this state by entering the **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.
Secure Addresses	Number of addresses in the secure address table for this port. Secure ports have at least one address.
Max Addresses	Number of addresses that the secure address table for the port can contain.
Security Rejects	Number of unauthorized addresses seen on the port.

For the restrictions that apply to secure ports, see the "Avoiding Configuration Conflicts" section on page 26-1.

Note You cannot configure static secure MAC addresses in the voice VLAN.

Defining the Maximum Secure Address Count

A secure port can have from 1 to 132 associated secure addresses. Setting one address in the MAC address table for the port ensures that the attached device has the full bandwidth of the port.

If the secure-port maximum addresses are set between 1 to 132 addresses and some of the secure addresses have not been added by user, the remaining addresses are dynamically learnt and become secure addresses.

Note If the port link goes down, all the dynamically learned addresses are removed.

If you enable port security on a voice VLAN port and if there is a PC connected to the IP phone, you should set the maximum allowed secure addresses on the port to more than 1.

Enabling Port Security

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

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode for the port you want to secure.
Step 3	**switchport port-security**	Enable basic port security on the interface.
Step 4	**switchport port-security maximum** *max_addrs*	Set the maximum number of MAC addresses that is allowed on this interface. The range is 1 to 132; the default is 1.
Step 5	**switchport port-security violation** {**shutdown** | **restrict** | **protect**}	Set the security violation mode for the interface. The default is **shutdown**. For **mode**, select one of these keywords: • **shutdown**—The interface is error-disabled when a security violation occurs. **Note** When a secure port is in the error-disabled state, you can bring it out of this state by entering the **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. • **restrict**—A security violation sends a trap to the network management station. • **protect**—When the port secure addresses reach the allowed limit on the port, all packets with unknown addresses are dropped.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show port security** [**interface** *interface-id*] [**address**]	Verify the entry.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Disabling Port Security

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

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode for the port that you want to unsecure.
Step 3	**no switchport port-security**	Disable port security.
Step 4	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 5	**show port security** [**interface** *interface-id*] [**address**]	Verify the entry.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Configuring and Enabling 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 that port are deleted after the specified aging time.
- Inactivity—The secure addresess on this 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 while still limiting the number of secure addresses on a port. You can enable or disable 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** *interface-id*	Enter interface configuration mode for the port on which you want to enable port security aging.
Step 3	**switchport port-security aging** {**static** | **time** *time* | **type** {**absolute** | **inactivity**}}	Set the aging time, type, and enable or disable static aging for the secure port. Enter **static** to enable aging for statically configured secure addresses on this port. For *time*, specify the aging time for this port. 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: • **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** *interface-id*] [**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 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 17-1.

Table 17-1 Commands for Displaying Traffic Control Status and Configuration

Command	Purpose
show interfaces [*interface-id*] **switchport**	Displays the administrative and operational status of all switching (nonrouting) ports or the specified port, including port protection settings.
show storm-control [*interface-id*] [**broadcast** | **multicast** | **unicast**] [*history*]	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 or to display storm-control history.
show interfaces [*interface-id*] **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 [*interface-id*] **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 [*interface-id*] **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** *interface-id*]	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** *interface-id*] **address**	Displays all secure MAC addresses configured on all switch interfaces or on a specified interface with aging information for each address.

This is a an example of output from the **show interfaces switchport** privileged EXEC command:

```
Switch# show interfaces gigabitethernet0/2 switchport
Name:Gi0/2
Switchport:Enabled
Administrative Mode:dynamic desirable
Operational Mode:down
Administrative Trunking Encapsulation:dot1q
Negotiation of Trunking:On
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled:2-1001

Protected:false

Voice VLAN:none (Inactive)
Appliance trust:none
```

This is an example of output from the **show interfaces counters broadcast** privileged EXEC command:

```
Switch# show interfaces counters broadcast

Port      BcastSuppDiscards
Fa0/1                     0
Fa0/2                     0
Fa0/3                     0
Fa0/4                     0
```

```
<output truncated>
```

This is an example of output from the **show port-security** privileged EXEC command when you do not enter an interface.

```
Switch# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security
Action
                    (Count)        (Count)      (Count)
------------------------------------------------------------------------------
---
     Fa0/1           11            11            0            Shutdown
     Fa0/5           15            5             0            Restrict
     Fa0/11          5             4             0            Protect
------------------------------------------------------------------------------
---
Total Addresses in System :21
Max Addresses limit in System :1024
```

This is an example of output from the **show port-security interface fastethernet0/1** privileged EXEC command for a specified interface.

```
Switch# show port-security interface fastethernet0/1
Port Security :Enabled
Port status :SecureUp
Violation mode :Shutdown
Maximum MAC Addresses :11
Total MAC Addresses :11
Configured MAC Addresses :3
Aging time :20 mins
Aging type :Inactivity
SecureStatic address aging :Enabled
Security Violation count :0
```

This is an example of output from the **show port-security address** privileged EXEC command.

```
Switch# show port-security address
          Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                         (mins)
----    -----------       ----                -----   -------------
   1    0001.0001.0001    SecureDynamic       Fa0/1       15 (I)
   1    0001.0001.0002    SecureDynamic       Fa0/1       15 (I)
   1    0001.0001.1111    SecureConfigured    Fa0/1       16 (I)
   1    0001.0001.1112    SecureConfigured    Fa0/1       -
   1    0001.0001.1113    SecureConfigured    Fa0/1       -
   1    0005.0005.0001    SecureConfigured    Fa0/5       23
   1    0005.0005.0002    SecureConfigured    Fa0/5       23
   1    0005.0005.0003    SecureConfigured    Fa0/5       23
   1    0011.0011.0001    SecureConfigured    Fa0/11      25 (I)
   1    0011.0011.0002    SecureConfigured    Fa0/11      25 (I)
------------------------------------------------------------------------
Total Addresses in System :10
Max Addresses limit in System :1024
```

This is an example of output from the **show storm-control** command when no keywords are entered. Because no traffic type keyword was entered, the broadcast storm control settings are displayed.

```
Switch# show storm-control

Interface  Filter State   Trap State     Upper    Lower    Current  Traps Sent
---------  -------------  -------------  -------  -------  -------  ----------
Fa0/1      inactive       inactive       100.00%  100.00%    0.00%           0
Fa0/2      inactive       inactive       100.00%  100.00%    0.00%           0
Fa0/3      inactive       inactive       100.00%  100.00%    0.00%           0
Fa0/4      inactive       inactive       100.00%  100.00%    0.00%           0
Fa0/5      inactive       inactive       100.00%  100.00%    0.00%           0
Fa0/6      inactive       inactive       100.00%  100.00%    0.00%           0
Fa0/7      inactive       inactive       100.00%  100.00%    0.00%           0
Fa0/8      inactive       inactive       100.00%  100.00%    0.00%           0
Fa0/9      inactive       inactive       100.00%  100.00%    0.00%           0
Fa0/10     inactive       inactive       100.00%  100.00%    0.00%           0
Fa0/11     inactive       inactive       100.00%  100.00%    0.00%           0
Fa0/12     inactive       inactive       100.00%  100.00%    0.00%           0
Gi0/1      inactive       inactive       100.00%  100.00%    0.00%           0
Gi0/2      inactive       inactive       100.00%  100.00%    0.00%           0
<output truncated>
```

This is an example of output from the **show storm-control** command for a specified interface. Because no traffic type keyword was entered, the broadcast storm control settings are displayed.

```
Switch# show storm-control fastethernet0/3
Interface  Filter State   Trap State     Upper    Lower    Current  Traps Sent
---------  -------------  -------------  -------  -------  -------  ----------
Fa0/3     inactive       inactive       100.00%  100.00%    0.00%           0
```

This is an example of output from the **show storm-control** command for a specified interface and traffic type, where no storm control threshold has been set for that traffic type on the specified interface.

```
Switch# show storm-control fastethernet0/4 multicast
Interface  Filter State   Trap State     Upper    Lower    Current  Traps Sent
---------  -------------  -------------  -------  -------  -------  ----------
Fa0/4      inactive       inactive       100.00%  100.00%    0.00%           0
```