



Configuring Traffic Suppression and Traffic Control

This chapter describes how to configure traffic suppression and traffic control characteristics on your switch.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 3550 Multilayer Switch Command Reference* for this release.

This chapter consists of these sections:

- [Understanding Traffic Suppression, page 11-1](#)
- [Configuring Traffic Suppression, page 11-2](#)
- [Configuring Protected Ports, page 11-6](#)
- [Configuring Port Blocking, page 11-7](#)

Understanding Traffic Suppression

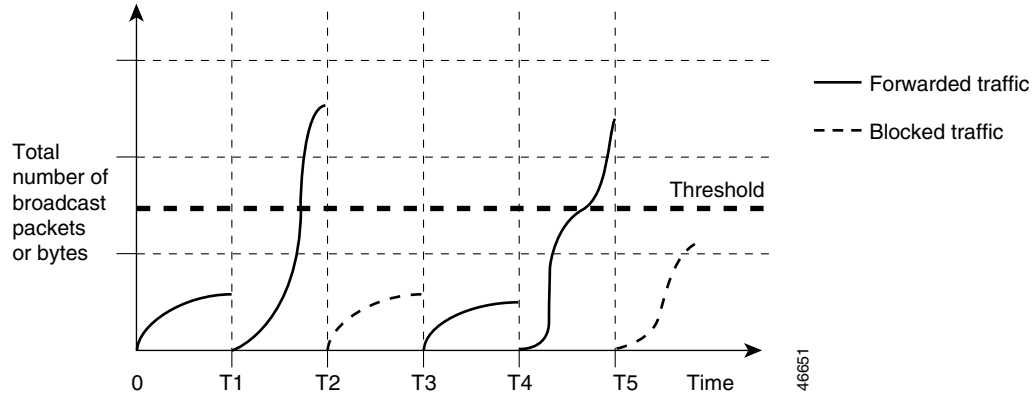
Traffic suppression prevents switchports on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation or in the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

Traffic suppression (or storm control) 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. 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. Traffic suppression is disabled by default.

The switch supports traffic suppression for broadcast, multicast, and unicast traffic. This example of broadcast suppression can also be applied to multicast and unicast traffic.

The graph in [Figure 11-1](#) shows broadcast traffic patterns on an interface over a given period of time. In this example, the broadcast traffic 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. Therefore, broadcast traffic is blocked during those intervals. At the next time interval, if broadcast traffic does not exceed the threshold, it is again forwarded.

Figure 11-1 Broadcast Suppression Example



When traffic suppression 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 the 1-second 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 combination of broadcast suppression threshold numbers and the 1-second time interval control the way the suppression 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.

**Note**

Because packets do not arrive at uniform intervals, the 1-second time interval during which traffic activity is measured can affect the behavior of traffic suppression.

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.

**Note**

When the rate of multicast traffic exceeds a set threshold, all incoming traffic (broadcast, multicast, and unicast) is dropped until the level drops below the threshold level. Only spanning-tree packets are forwarded. When broadcast and unicast thresholds are exceeded, traffic is blocked only for the type of traffic that exceeded the threshold.

You use the **switchport broadcast**, **switchport multicast**, and **switchport unicast** interface configuration commands to set up the traffic suppression threshold value.

Configuring Traffic Suppression

These sections include broadcast suppression configuration information and procedures:

- [Default Traffic Suppression Configuration, page 11-3](#)
- [Enabling Traffic Suppression, page 11-3](#)
- [Disabling Traffic Suppression, page 11-4](#)
- [Displaying Traffic Suppression Configurations, page 11-5](#)

Default Traffic Suppression Configuration

By default, unicast, broadcast, and multicast suppression is disabled on the switch.

Enabling Traffic Suppression

You enable traffic suppression 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 would allow all traffic.



Note

The interface can be a physical interface (for example, GigabitEthernet 0/1) or an EtherChannel (for example, port-channel 5). When you specify a suppression level for a port channel, the threshold value is applied to each physical port in the EtherChannel, but traffic is measured and blocked for each port independently.

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

	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 switchport interface or EtherChannel to configure, for example GigabitEthernet 0/1.
Step 3	switchport broadcast <i>broadcast suppression level</i>	Specify the broadcast suppression level for an interface as a percentage of total bandwidth. A threshold value of 100 percent means that no limit is placed on broadcast traffic.
Step 4	switchport multicast <i>multicast suppression level</i>	Specify the multicast suppression level for an interface as a percentage of total bandwidth.
Step 5	switchport unicast <i>unicast suppression level</i>	Specify the unicast suppression level for an interface as a percentage of total bandwidth.
Step 6	end	Return to privileged EXEC mode.
Step 7	show interfaces <i>interface</i> switchport	(Optional) View switchport characteristics, including traffic suppression levels set on the interface.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to enable bandwidth-based multicast suppression at 70 percent on Gigabit Ethernet interface 1 and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport multicast 70
Switch(config-if)# end
Switch# show interface 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

Port Protected: Off
Unknown Unicast Traffic: Allowed
Unknown Multicast Traffic: Not Allowed

Broadcast Suppression Level: 100
Multicast Suppression Level: 70
Unicast Suppression Level: 100
```

Disabling Traffic Suppression

Beginning in privileged EXEC mode, follow these steps to disable traffic suppression on an interface:

	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 switchport interface to configure, for example GigabitEthernet 0/1.
Step 3	no switchport broadcast	Disable broadcast suppression for the interface.
Step 4	no switchport multicast	Disable multicast suppression for the interface.
Step 5	no switchport unicast	Disable unicast suppression for the interface.
Step 6	end	Return to privileged EXEC mode.
Step 7	show interfaces <i>interface</i> switchport	(Optional) View switchport characteristics, including traffic suppression levels set on the interface.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Displaying Traffic Suppression Configurations

The **show interface *interface-id* switchport** privileged EXEC commands display (among other characteristics) the interface traffic suppression configuration. The **show interface counters** privileged EXEC commands display the count of discarded packets.

Beginning in privileged EXEC mode, follow these steps to display traffic suppression statistics on an interface:

Command	Purpose
show interface [<i>interface-id</i>] counters broadcast	Display the broadcast suppression discard counter for all interfaces or a specific interface. Display the number of packets discarded.
show interface [<i>interface-id</i>] counters multicast	Display the multicast suppression discard counter for all interfaces or a specific interface. Display the number of packets discarded.
show interface [<i>interface-id</i>] counters unicast	Display the unicast suppression discard counter for all interfaces or a specific interface. Display the number of packets discarded.

This is a sample output from the **show interface switchport** privileged EXEC command:

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

Port Protected: Off
Unknown Unicast Traffic: Allowed
Unknown Multicast Traffic: Not Allowed

Broadcast Suppression Level: 100
Multicast Suppression Level: 100
Unicast Suppression Level: 100
```

This is a sample output from the **show interface counters broadcast** privileged EXEC command:

```
Switch# show interface counters broadcast

Port      BcastSuppDiscards
Gi0/1          0
Gi0/2          0
Gi0/3          0
Gi0/4          0
```

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.



Note

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

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.



Note

There could be times when unknown unicast or multicast traffic from a nonprotected port is flooded to a protected port because a MAC address has timed out or has not been learned by the switch. Use the **switchport block unicast** and **switchport block multicast** commands to guarantee that no unicast and multicast traffic is flooded to the port in such a case.

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 switchport interface to configure, for example GigabitEthernet 0/1.
Step 3	switchport protected	Configure the interface to be a protected port.
Step 4	end	Return to privileged EXEC mode.
Step 5	show interface <i>interface-id</i> switchport	Verify your entry.
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 0/3 as a protected port and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# switchport protected
Switch(config-if)# end
Switch# show interface gigabitethernet0/3 switchport
Name: Gi0/3
Switchport: Enabled

<output truncated>

Port Protected: On
Unknown Unicast Traffic: Allowed
Unknown Multicast Traffic: Allowed

Broadcast Suppression Level: 100
Multicast Suppression Level: 100
```

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.

Blocking Flooded Traffic on an Interface



Note

The interface can be a physical interface (for example, GigabitEthernet 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 to 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 switchport interface to configure, for example <code>gigabitethernet 0/1</code> .
Step 3	<code>switchport block multicast</code>	Block unknown multicast forwarding to the port.
Step 4	<code>switchport block unicast</code>	Block unknown unicast forwarding to the port.
Step 5	<code>end</code>	Return to privileged EXEC mode.

	Command	Purpose
Step 6	show interface <i>interface-id</i> switchport	Verify your entry.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
Switch(config-if)# end
Switch# show interface gigabitethernet0/1 switchport
Name: Gi0/3
Switchport: Enabled

<output truncated>

Port Protected: On
Unknown Unicast Traffic: Not Allowed
Unknown Multicast Traffic: Not Allowed

Broadcast Suppression Level: 100
Multicast Suppression Level: 100
Unicast Suppression Level: 100
```

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>	Enter interface configuration mode and enter the type and number of the switchport interface to configure, for example gigabitethernet0/1 .
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 interface <i>interface-id</i> switchport	Verify your entry.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.