



Configuring Broadcast Suppression

This chapter describes how to configure broadcast suppression on the Catalyst 6500 series switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Command Reference* publication.

This chapter consists of these sections:

- [Understanding How Broadcast Suppression Works, page 32-1](#)
- [Configuring Broadcast Suppression on the Switch, page 32-3](#)

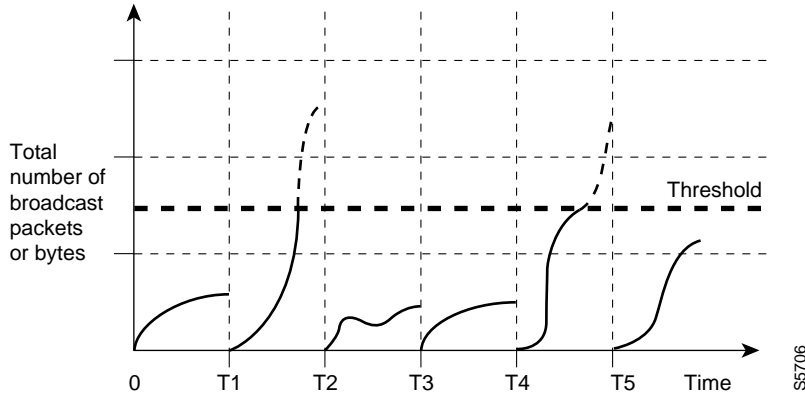
Understanding How Broadcast Suppression Works

Broadcast suppression prevents switched ports on a LAN from being disrupted by a broadcast storm on one of the ports. A LAN broadcast storm occurs when broadcast or multicast 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 broadcast storm.

Broadcast suppression uses filtering that measures broadcast activity on a LAN over a 1-second time period and compares the measurement with a predefined threshold. If the threshold is reached, further broadcast activity is suppressed for the duration of a specified time period. Broadcast suppression is disabled by default.

[Figure 32-1](#) shows the broadcast traffic patterns on a port over a given period of time. In this example, broadcast suppression occurs between time intervals T1 and T2 and between T4 and T5. During those time periods, the amount of broadcast traffic exceeded the configured threshold.

Figure 32-1 Broadcast Suppression



The broadcast suppression threshold numbers and the time interval make the broadcast suppression algorithm work with different levels of granularity. A higher threshold allows more broadcast packets to pass through.

Broadcast suppression on the Catalyst 6500 series switches is implemented in hardware. The suppression circuitry monitors packets passing from a port to the switching bus. Using the Individual/Group bit in the packet destination address, the broadcast suppression circuitry determines if the packet is unicast or broadcast. It keeps track of the current count of broadcasts within the 1-second time interval, and when a threshold is reached, filters out subsequent broadcast packets.

Because hardware broadcast suppression uses a bandwidth-based method to measure broadcast activity, the most significant implementation factor is setting the percentage of total available bandwidth that can be used by broadcast traffic. A threshold value of 100 percent means that no limit is placed on broadcast traffic. Using the **set port broadcast** command, you can set up the broadcast suppression threshold value.

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

On Gigabit Ethernet ports, you can use the broadcast suppression to filter multicast and unicast traffic. You can suppress multicast or unicast traffic separately on a port; both require that you configure broadcast suppression. When you specify a percentage of the total bandwidth to be used for multicast or unicast traffic, the same limit applies to the broadcast traffic.



Note

Multicast suppression does not drop bridge protocol data unit (BPDU) packets.



Note

When broadcast, multicast, or unicast suppression occurs, you can configure ports to go into the *errdisable* state. See the [“Enabling the errdisable State”](#) section on page 32-4 for details.

Configuring Broadcast Suppression on the Switch

These sections describe how to configure broadcast suppression on the Catalyst 6500 series switches:

- [Enabling Broadcast Suppression, page 32-3](#)
- [Disabling Broadcast Suppression, page 32-4](#)
- [Enabling the errdisable State, page 32-4](#)

Enabling Broadcast Suppression

To enable broadcast suppression for one or more ports, perform this task in privileged mode:

	Task	Command
Step 1	Enable broadcast suppression for one or more ports.	set port broadcast <i>mod/port threshold%</i> [violation {drop-packets errdisable}] [multicast {enable disable}] [unicast {enable disable}]
Step 2	Verify the broadcast suppression configuration.	show port broadcast [<i>mod[/port]</i>]



Note

Although you can specify the broadcast suppression threshold to 0.01 percent, not all modules adjust to that level of precision. Most thresholds vary between 0.01 percent and 0.05 percent. If you specify a finer threshold, the threshold percent adjusts as closely as possible.

This example shows how to enable bandwidth-based broadcast suppression and verify the configuration:

```
Console> (enable) set port broadcast 3/1-6 75.25%
```

```
Ports 3/1-6 broadcast traffic limited to 75.25%.
```

```
On broadcast suppression ports 3/1-6 are configured to drop-packets.
```

```
Console> (enable) show port broadcast 3
```

Port	Broadcast-Limit	Multicast	Unicast	Total-Drop	Action
3/1	75.25 %	-	-		0 drop-packets
3/2	75.25 %	-	-		0 drop-packets
3/3	75.25 %	-	-		2 drop-packets
3/4	75.25 %	-	-		0 drop-packets
3/5	75.25 %	-	-		0 drop-packets
3/6	75.25 %	-	-		0 drop-packets
3/7	-	-	-		0 drop-packets
3/8	-	-	-		0 drop-packets

```
.<snip>
```

```
Console> (enable)
```

This example shows how to limit the multicast and broadcast traffic to 80 percent for port 1 on module 2 and verify the configuration:

```
Console> (enable) set port broadcast 2/1 80% multicast enable
Port 2/1 broadcast and multicast traffic limited to 80.00%.
On broadcast suppression port 2/1 is configured to drop-packets.
Console> (enable) show port broadcast 2/1
```

Port	Broadcast-Limit	Multicast	Unicast	Total-Drop	Action
2/1	80.00 %	80.00 %	-		0 drop-packets

```
Console> (enable)
```

Disabling Broadcast Suppression

To disable broadcast suppression on one or more ports, perform this task in privileged mode:

Task	Command
Disable broadcast suppression on one or more ports.	clear port broadcast <i>mod/port</i>

This example shows how to disable broadcast suppression on one or more ports:

```
Console> (enable) clear port broadcast 2/1
Port 2/1 traffic unlimited.
Console> (enable)
```

Enabling the errdisable State



Note

A port is in the errdisable state if it is enabled in NVRAM but is disabled at runtime by any process. For example, if UniDirectional Link Detection (UDLD) detects a unidirectional link, the port shuts down at runtime. However, because the NVRAM configuration for the port is enabled (you have not disabled the port), the port status is shown as errdisable.

When broadcast, multicast, or unicast suppression occurs, you can configure ports to either drop packets or go into the errdisable state. The errdisable state feature can be enabled or disabled on a per-port basis and is disabled by default (the **drop-packets** option is enabled by default).



Note

When broadcast, multicast, or unicast suppression occurs and a port is configured for errdisable, there is a delay before the port stops dropping packets and actually goes to errdisable. The delay period varies; the exact amount of delay is not deterministic and can vary from switch to switch.

To enable the errdisable state on a port, perform this task in privileged mode:

	Task	Command
Step 1	Enable the errdisable state.	set port broadcast <i>mod/port threshold%</i> [violation { drop-packets errdisable }] [multicast { enable disable }] [unicast { enable disable }]
Step 2	Verify that the errdisable state is enabled.	show port broadcast [<i>mod[/port]</i>]

This example shows how to limit broadcast traffic to 90 percent and to errdisable the port when broadcast suppression occurs:

```
Console> (enable) set port broadcast 4/6 90% violation errdisable
Port 4/6 broadcast traffic limited to 90.00%.
On broadcast suppression port 4/6 is configured to move to errdisabled state.
Console> (enable)
```



Note Use the **set errdisable-timeout enable bcast-suppression** command to enable the errdisable timeout feature for broadcast suppression.

Once a port is put into errdisable state, it can be reenabled after a specific timeout interval has expired. Use the **set errdisable-timeout interval** command to specify the timeout interval.

Use the **set port errdisable-timeout** command to control on a per-port basis whether a port should be enabled after a certain time or continue to be in the errdisabled state once it has been errdisabled.

For more information, see the [“Configuring a Timeout Period for Ports in errdisable State”](#) section on page 4-11.

