



CHAPTER 35

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 that are 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 35-1](#)
- [Configuring Broadcast Suppression on the Switch, page 35-3](#)

Understanding How Broadcast Suppression Works



Note

Broadcast and multicast suppression is not supported on the WS-X6148A-GE-TX, WS-X6148A-GE-45A, and WS-X6548-GE-TX modules.

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

Broadcast suppression uses filtering that measures the broadcast activity on a LAN over a time period (15264 nsec to ~1 sec) that varies based on the type of line card and speed setting on the port, 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 35-1](#) shows the broadcast traffic patterns on a port over a given period of time. In this example, broadcast suppression occurs between the time intervals T1 and T2 and between T4 and T5. During those time periods, the amount of broadcast traffic exceeded the configured threshold.

Figure 35-1 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 the hardware. The suppression circuitry monitors the 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, keeps track of the current count of broadcasts within the time interval, and when a threshold is reached, filters out the subsequent broadcast packets.

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

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

On the Gigabit Ethernet ports, you can use the broadcast suppression to filter the multicast and unicast traffic. You can suppress the 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 the multicast or unicast traffic, the same limit applies to the broadcast traffic.

**Note**

When broadcast, multicast, or unicast suppression occurs, you can configure the ports to go into the *errdisable* state. See the [“Enabling the errdisable State”](#) section on page 35-5 for details.

**Note**

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

**Note**

The reception of BPDUs is not guaranteed when multicast suppression is enabled on the following modules: WS-X6724-SFP, WS-X6748-GE-TX, WS-X6748-SFP, WS-X6704-10GE, WS-SUP32-GE-3B, and WS-SUP32-10GE-3B. Enabling multicast suppression on these modules can cause BPDUs to be suppressed when the multicast suppression threshold is exceeded. We strongly advise that you do not use multicast suppression on ports that need to receive BPDUs because potential side effects can be root port loss or spanning tree loops when the suppression threshold is exceeded.

Configuring Broadcast Suppression on the Switch

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

- [Enabling Broadcast Suppression, page 35-3](#)
- [Disabling Broadcast Suppression, page 35-5](#)
- [Enabling the errdisable State, page 35-5](#)



Note

The switch supports multicast and unicast traffic storm control on Gigabit and 10 Gigabit Ethernet LAN ports. Most FastEthernet switching modules do not support multicast and unicast traffic storm control, with the exception of WS-X6148A-RJ-45 and the WS-X6148-SFP.

Enabling Broadcast Suppression

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

	Task	Command
Step 1	Enable the broadcast suppression threshold for one or more ports as a percentage of the total bandwidth.	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</i> [/ <i>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.



Note

On these modules, a level value of 0.33 percent or less suppresses all traffic:

- WS-X6704-10GE
- WS-X6748-SFP
- WS-X6724-SFP
- WS-X6748-GE-TX

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

■ Configuring Broadcast Suppression on the Switch

```
3/6          75.25 %      -      -      0 drop-packets
3/7          -           -      -      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 the ports to either drop the 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 the packets and goes to the errdisable state. The delay period varies; the exact amount of delay 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 the broadcast traffic to 90 percent and error disable 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

Enter 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. Enter the **set errdisable-timeout interval** command to specify the timeout interval.

Enter 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 4-12.