



## Configuring Broadcast Suppression

---

This chapter describes how to configure broadcast suppression on the Catalyst 6000 family switches.



### Note

---

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6000 Family Command Reference* publication.

---

This chapter consists of these sections:

- [Understanding How Broadcast Suppression Works, page 32-1](#)
- [Configuring Broadcast Suppression, page 32-2](#)

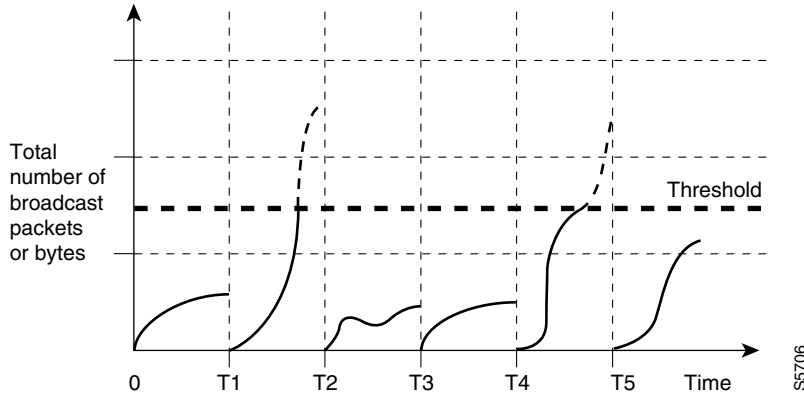
## Understanding How Broadcast Suppression Works

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 one-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 6000 family 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 one-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 one-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.

## Configuring Broadcast Suppression

These sections describe how to configure broadcast suppression on the Catalyst 6000 family switches:

- [Enabling Broadcast Suppression, page 32-3](#)
- [Disabling Broadcast Suppression, 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	Configure the broadcast suppression threshold for one or more ports as a percentage of total bandwidth.	<b>set port broadcast</b> <i>mod/port threshold%</i> [ <b>multicast</b> {enable   disable}] [ <b>unicast</b> {enable   disable}]
Step 2	Verify the broadcast suppression configuration.	<b>show port broadcast</b> [ <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%
Port(s) 3/1-24 broadcast traffic limited to 75.25%.
Console> (enable) show port broadcast 3
```

```
Port      Broadcast-Limit Broadcast-Drop
-----
3/1 75.25 % -
3/2 75.25 % -
3/3 75.25 % -
3/4 75.25 % -
3/5 75.25 % -
3/6 75.25 % -
3/7 0 % -
3/8 0 % -
3/9 0 % -
3/10 0 % -
3/11 0 % -
3/12 0 % -
```

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

```
Console> (enable) set port broadcast 1/2 80% multicast enable
Port 1/2 broadcast and multicast traffic limited to 80.00%.
Console> (enable) show port broadcast 1/2
```

```
Port      Broadcast-Limit Total-Drop      Multicast Unicast
-----
1/2      80.00 %          0      80.00 % -
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.	<b>clear port broadcast</b> <i>mod/port</i>

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

```
Console> (enable) clear port broadcast 3/1  
Port 3/1-8 broadcast traffic unlimited.  
Console> (enable)
```