

Configuring Broadcast/Multicast Suppression

This chapter describes how to configure broadcast/multicast suppression on the Catalyst 5000, 4000, 2948G, 2926G, and 2926 series switches.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Command Reference* for your switch.

This chapter consists of these sections:

- Understanding How Broadcast/Multicast Suppression Works on page 25-1
- Broadcast/Multicast Suppression Support on page 25-3
- Configuring Broadcast/Multicast Suppression on page 25-3

Understanding How Broadcast/Multicast Suppression Works

These sections describe how broadcast/multicast suppression works:

- Understanding Broadcast/Multicast Traffic Suppression on page 25-1
- Bandwidth-Based (Hardware) Broadcast/Multicast Suppression on page 25-2
- Packet-Based (Software) Broadcast/Multicast Suppression on page 25-3

Understanding Broadcast/Multicast Traffic Suppression

Broadcast/multicast suppression prevents switched ports on a LAN from being disrupted by a broadcast storm. 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/multicast suppression works by measuring incoming broadcast/multicast activity on a switch port. Broadcast/multicast activity can be measured in two ways:

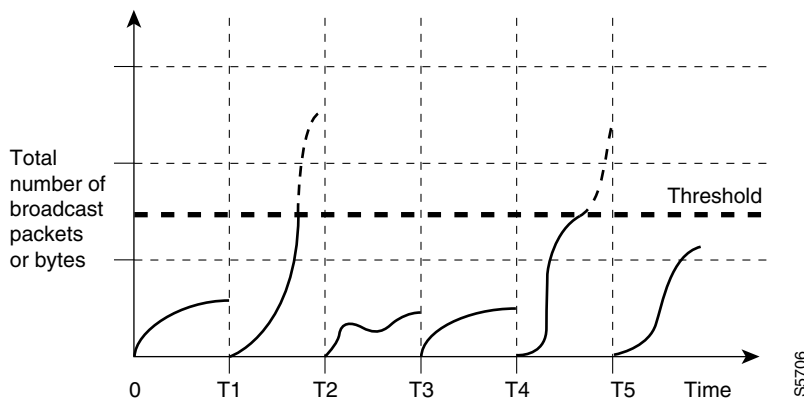
- By the amount of network bandwidth used by broadcast/multicast traffic over a one-second time period (bandwidth-based)
- By the number of broadcast/multicast packets received over a one-second time period (packet-based)

Broadcast/multicast suppression is implemented either in hardware or in software. Hardware broadcast/multicast suppression uses the bandwidth-based method. Software broadcast/multicast suppression uses the packet-based method. Since packet sizes vary, bandwidth-based measurement is more accurate and effective than packet-based measurement.

When broadcast/multicast suppression is enabled, the switch monitors incoming packets on the port over a one-second time period. The switch uses the Individual/Group bit in the packet destination address to determine if the packet is a unicast or a broadcast/multicast. If the total number of broadcasts/multicasts exceeds a user-configured threshold, further activity is suppressed for the duration of a specified period.

Figure 25-1 shows the broadcast/multicast traffic patterns on a port over a given period. In this example, broadcast/multicast suppression occurs between the one-second intervals T1–T2 and T4–T5. During those one-second intervals, the amount of broadcast/multicast traffic exceeded the configured threshold.

Figure 25-1 Broadcast/Multicast Suppression



Broadcast/multicast suppression is disabled by default. Bandwidth-based broadcast/multicast suppression takes precedence over packet-based broadcast/multicast suppression unless you disable bandwidth-based broadcast/multicast suppression (that is, you set the threshold value to 100 percent).

Bandwidth-Based (Hardware) Broadcast/Multicast Suppression

With bandwidth-based broadcast/multicast suppression, if the number of incoming broadcasts/multicasts on a port within a one-second time interval exceeds the configured threshold, the switch filters out all incoming broadcast/multicast packets on the port for the remainder of the one-second period.

Bandwidth-based broadcast/multicast suppression measures broadcast/multicast activity relative to total bandwidth. You can configure the percentage of total available bandwidth that can be used by broadcast/multicast traffic using the **set port broadcast** command. The higher the threshold the more incoming broadcast/multicast packets are allowed to pass. A threshold value of 100 percent means that no limit is placed on broadcast traffic (suppression is disabled).

Note On certain modules (such as the Catalyst 5000 series group-switching Fast Ethernet module, WS-X5223), when you enable bandwidth-based broadcast/multicast suppression, the configured threshold percentage is applied to all ports on the module.

To determine whether your hardware supports bandwidth-based broadcast/multicast suppression, see the documentation for your hardware or use the **show port capabilities** command.

Packet-Based (Software) Broadcast/Multicast Suppression

With packet-based broadcast/multicast suppression, if the number of incoming broadcasts/multicasts on a port within a one-second time interval exceeds the configured threshold, the switch filters out *all* incoming traffic (including unicast packets) on the port for the remainder of the one-second period.

Packet-based broadcast/multicast suppression measures broadcast/multicast activity relative to the total number of packets received on the port. You can configure the total number of packets that can be used by broadcast/multicast traffic using the **set port broadcast** command. The higher the threshold the more incoming broadcast/multicast packets are allowed to pass. A threshold value of 0 packets means that no limit is placed on broadcast traffic (suppression is disabled on the port).

To determine whether your hardware supports packet-based broadcast/multicast suppression, see the documentation for your hardware or use the **show port capabilities** command.

Broadcast/Multicast Suppression Support

Broadcast/multicast suppression capability is not available on all platforms and is hardware-dependent. Table 25-1 shows which switches have available hardware that supports broadcast/multicast suppression.

To determine whether a specific piece of hardware supports broadcast/multicast suppression, see the documentation for your hardware or use the **show port capabilities** command.

Table 25-1 Broadcast/Multicast Suppression Support

Suppression Method	Catalyst 5000 Series	Catalyst 4000 Series	Catalyst 2948G Series	Catalyst 2926G Series	Catalyst 2926 Series
Bandwidth-based (hardware) suppression	Yes	No	No	Yes	No
Packet-based (software) suppression	Yes	No	No	Yes	Yes

Configuring Broadcast/Multicast Suppression

These sections describe how to configure broadcast/multicast suppression:

- Enabling Bandwidth-Based Broadcast/Multicast Suppression on page 25-4
- Enabling Packet-Based Broadcast/Multicast Suppression on page 25-4
- Disabling Broadcast/Multicast Suppression on page 25-5

Enabling Bandwidth-Based Broadcast/Multicast Suppression

Note Configuring broadcast/multicast suppression on the Catalyst 5000 series Gigabit EtherChannel module (WS-X5410) limits only the amount of broadcast/multicast traffic that the module can send to the switch backplane for forwarding to other modules. Traffic switched between ports on the module is never suppressed.

To enable bandwidth-based broadcast/multicast suppression, perform this task in privileged mode:

Task	Command
Step 1 Specify the broadcast/multicast suppression threshold for one or more ports as a percentage of total bandwidth.	set port broadcast <i>mod_num/port_num threshold%</i>
Step 2 Verify the broadcast/multicast suppression configuration.	show port broadcast [<i>mod_num</i>][<i>/port_num</i>]

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

```

Console> (enable) set port broadcast 3/1 75%
Port(s) 3/1-24 broadcast traffic limited to 75%.
Console> (enable) show port broadcast 3

Port      Broadcast-Limit Broadcast-Drop
-----
3/1-8          75 %          -
3/9-16         75 %          -
3/17-24       75 %          -
Console> (enable)
    
```

Enabling Packet-Based Broadcast/Multicast Suppression

To enable packet-based broadcast/multicast suppression, perform this task in privileged mode:

Task	Command
Step 1 Specify the broadcast/multicast suppression threshold for one or more ports as a maximum number of broadcast or multicast packets allowed in a one-second period.	set port broadcast <i>mod_num/port_num threshold</i>
Step 2 Verify the broadcast/multicast suppression configuration.	show port broadcast [<i>mod_num</i>][<i>/port_num</i>]

This example shows how to enable packet-based broadcast/multicast suppression and verify the configuration:

```

Console> (enable) set port broadcast 2/6 500
Port(s) 2/6 broadcast traffic limited to 500 packets/second.
Console> (enable) set port broadcast 2/7 500
Port(s) 2/7 broadcast traffic limited to 500 packets/second.
Console> (enable) set port broadcast 2/8 500
Port(s) 2/8 broadcast traffic limited to 500 packets/second.
    
```

```

Console> (enable) show port broadcast

Port      Broadcast-Limit Broadcast-Drop
-----
1/1      -              -
1/2      -              -
2/1      -              0
2/2      -              0
2/3      -              0
2/4      -              0
2/5      -              0
2/6      500 p/s       0
2/7      500 p/s       0
2/8      500 p/s       0
2/9      -              0
2/10     -              0
2/11     -              0
2/12     -              0
Console> (enable)

```

Disabling Broadcast/Multicast Suppression

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

Task	Command
Step 1 Disable broadcast/multicast suppression on one or more ports.	clear port broadcast <i>mod_num/port_num</i>
Step 2 Verify the broadcast/multicast suppression configuration.	show port broadcast

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

```

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

```

