CHAPTER 48

Port Unicast and Multicast Flood Blocking

This chapter describes how to configure multicast and unicast flood blocking on the Catalyst 4000 family switch. This chapter contains these topics:

Note For complete syntax and usage information for the switch commands used in this chapter, first look at the *Cisco Catalyst 4500 Series Switch Command Reference* and related publications at this location:

http://www.cisco.com/en/US/products//hw/switches/ps4324/index.html

If the command is not found in the Catalyst 4500 Series Switch Command Reference, it will be found in the larger Cisco IOS library. Refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at this location:

http://www.cisco.com/en/US/products/ps6350/index.html

Overview of Flood Blocking

Occasionally, unknown unicast or multicast traffic is flooded to a switch port because a MAC address has timed out or has not been learned by the switch. (This condition is especially undesirable for a private VLAN isolated port.) To guarantee that no unicast and multicast traffic is flooded to the port, use the **switchport block unicast** and **switchport block multicast** commands to enable flood blocking on the switch.

Note The flood blocking feature is supported on all switched ports (including PVLAN ports) and is applied to all VLANs on which the port is forwarding.

Configuring Port Blocking

By default, a switch floods packets with unknown destination MAC addresses to all ports. If unknown unicast and multicast traffic is forwarded to a switch port, there might be security issues. To prevent forwarding such traffic, you can configure a port to block unknown unicast or multicast packets.

Note Blocking of unicast or multicast traffic is not automatically enabled on a switch port; you must explicitly configure it.

Blocking Flooded Traffic on an Interface

Note The interface can be a physical interface (for example, GigabitEthernet 1/1) or an EtherChannel group (such as 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.

Note Starting with Cisco IOS Release 12.2(52)SG, only IPV4 and IPv6 unknown multicast traffic flooding is blocked; Layer 2 unknown multicast flooding is not. This behavior stems from a fix for the following problem: when you configure blocking of unknown multicast flooding on a port, broadcast traffic to the port is also blocked.

To disable the flooding of multicast and unicast packets to an interface, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface` *interface-id*	Enters interface configuration mode and enter the type and number of the switchport interface (for example, **GigabitEthernet 1/1**).
Step 3	`Switch(config-if)# switchport block multicast`	Blocks unknown multicast forwarding to the port.
Step 4	`Switch(config-if)# switchport block unicast`	Blocks unknown unicast forwarding to the port.
Step 5	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	`Switch# show interface` *interface-id* `switchport`	Verifies your entry.
Step 7	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

This example shows how to block unicast and multicast flooding on a GigabitEthernet interface1/1 and how to verify the configuration:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
Switch(config-if)# end
Switch# show interface gigabitethernet1/1 switchport
Name: Gi1/3
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

To resume normal forwarding on a port, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface interface-id`	Enters interface configuration mode and enter the type and number of the switchport interface (GigabitEthernet1/1).
Step 3	`Switch(config-if)# no switchport block multicast`	Enables unknown multicast flooding to the port.
Step 4	`Switch(config-if)# no switchport block unicast`	Enables unknown unicast flooding to the port.
Step 5	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	`Switch# show interface interface-id switchport`	Verifies your entry.
Step 7	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.