



Port Blocking

- [Information About Port Blocking, on page 1](#)
- [Blocking Flooded Traffic on an Interface , on page 1](#)
- [Monitoring Port Blocking, on page 3](#)
- [Feature History for Port Blocking, on page 3](#)

Information About Port Blocking

By default, the switch floods packets with unknown destination MAC addresses out of all ports. If unknown unicast and multicast traffic is forwarded to a protected port, there could be security issues. To prevent unknown unicast or multicast traffic from being forwarded from one port to another, you can block a port (protected or nonprotected) from flooding unknown unicast or multicast packets to other ports.

Blocking Flooded Traffic on an Interface

To block flooded traffic on n interface, perform this procedure:

Before you begin

The interface can be a physical interface or an EtherChannel group. When you block multicast or unicast traffic for a port channel, it is blocked on all ports in the port-channel group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *interface-id***
4. **switchport block multicast**
5. **switchport block unicast**
6. **end**
7. **show interfaces *interface-id* switchport**
8. **show running-config**
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Device configure terminal	Enters global configuration mode.
Step 3	interface <i>interface-id</i> Example: Device(config)# interface gigabitethernet 0/2	Specifies the interface to be configured, and enter interface configuration mode.
Step 4	switchport block multicast Example: Device(config-if)# switchport block multicast	Blocks unknown multicast forwarding out of the port. Note Pure Layer 2 multicast traffic as well as multicast packets that contain IPv6 information in the header are blocked.
Step 5	switchport block unicast Example: Device(config-if)# switchport block unicast	Blocks unknown unicast forwarding out of the port.
Step 6	end Example: Device(config-line)# end	Returns to privileged EXEC mode.
Step 7	show interfaces <i>interface-id</i> switchport Example: Device# show interfaces gigabitethernet 0/2 switchport	Verifies your entries.
Step 8	show running-config Example: Device# show running-config	Verifies your entries.
Step 9	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Monitoring Port Blocking

Table 1: Commands for Displaying Port Blocking Settings

Command	Purpose
<code>show interfaces [interface-id] switchport</code>	Displays the administrative and operational status of all switching (nonrouting) ports or the specified port, including port blocking and port protection settings.

Feature History for Port Blocking

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS Release 15.2(5)E	Port Blocking	To prevent unknown unicast or multicast traffic from being forwarded from one port to another, you can block a port (protected or nonprotected) from flooding unknown unicast or multicast packets to other ports.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.

