Configuring Switchport Blocking

About Switchport Blocking

By default, the router floods packets with unknown destination MAC addresses to all ports. To prevent the forwarding of such traffic, you can configure a port to block unknown multicast or unicast packets.

Occasionally, unknown multicast or unicast traffic is flooded to a switch port because a MAC address has timed out or has not been learned by the switch. Security issues could arise if unknown multicast and unicast traffic is forwarded to a switch port. You can enable switchport blocking to guarantee that no multicast or unicast traffic is flooded to the port. 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.

Configuring Switchport Blocking

Follow these steps to configure switchport blocking. Blocking of unicast or multicast traffic is not automatically enabled on a switch port.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enter global configuration mode.
Step 2	**interface** {*interface-id* | **port-channel** *number*} **Example:** `Router(config)# interface gigabitethernet 0/1/1`	Enters interface configuration mode.
Step 3	**switchport mode access** **Example:**	Configures the interface as an access port.

	Command or Action	Purpose
	`Router(config-if)# switchport mode access`	
Step 4	**switchport access vlan** *vlan-id* **Example:** `Router(config-if)# switchport access vlan 20`	Specifies the VLAN for which this access port will carry traffic.

Step 5	[**no**] **switchport block** {**multicast** | **unicast**}
	Example:
	`Router(config-if)# switchport block multicast`
	`Router(config-if)# switchport block unicast`
		Prevents the flooding of unknown multicast or unicast packets on the specified interface.
		Use the no form of this command to resume normal forwarding on the port.

Step 6	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 7	(Optional) **show interface** {*interface-id* | **port-channel** *number*} **switchport** **Example:** `Router# show interface gigabitethernet 0/1/1 switchport`	(Optional) Displays the switchport blocking configuration.

Example

The following example shows how to block multicast and unicast flooding on GigabitEthernet interface 0/1/1 and how to verify the configuration:

```
Router# configure terminal
Router(config)# interface GigabitEthernet0/1/1
Router(config-if)# switchport access vlan 20
Router(config-if)# switchport mode access
Router(config-if)# switchport block multicast
Router(config-if)# switchport block unicast
Router(config-if)# exit
Router(config)# end
Router#
```

Following command shows the blocking state of unknown unicast and multicast on the interface:

```
Router#show interfaces gigabitEthernet 0/1/1 switchport
Name: Gi0/1/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 20 (VLAN0020)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: disabled
Voice VLAN: none
```

```
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: enabled
Unknown multicast blocked: enabled
Appliance trust: none
Router#
```

Configuring Switchport Blocking