



Configuring Protocol Filtering

This chapter describes how to configure protocol filtering on Ethernet, Fast Ethernet, and Gigabit Ethernet ports on the Catalyst enterprise LAN switches. The configuration tasks in this chapter apply to Ethernet, Fast Ethernet, and Gigabit Ethernet switch ports on switching modules and fixed-configuration switches, as well as to supervisor engine Fast and Gigabit Ethernet uplink ports.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Command Reference—Catalyst 4000 Family, Catalyst 2948G, and Catalyst 2980G Switches*.

This chapter consists of these sections:

- [Understanding How Protocol Filtering Works, page 18-1](#)
- [Default Protocol Filtering Configuration, page 18-2](#)
- [Configuring Protocol Filtering, page 18-2](#)

Understanding How Protocol Filtering Works

Protocol filtering prevents certain protocol traffic from being forwarded out switch ports. Broadcast and unicast flood traffic is filtered based on the membership of ports in different protocol groups. This filtering is in addition to the filtering provided by port-VLAN membership.

With protocol filtering enabled, ports are identified on a protocol basis. A port can be a member of one or more of the protocol groups. Flood traffic for each protocol group is forwarded out a port only if that port belongs to the appropriate protocol group.

Layer 2 protocols, such as Spanning Tree Protocol (STP) and Cisco Discovery Protocol (CDP), are not affected by protocol filtering. Dynamic VLAN ports and ports that have port security enabled are members of all protocol groups.

You can configure a port with any one of these modes for each protocol group: **on**, **off**, or **auto**. If the configuration is set to **on**, the port receives all the flood traffic for that protocol. If the configuration is set to **off**, the port does not receive any flood traffic for that protocol.

If the configuration is set to **auto**, a port becomes a member of the protocol group only after the device connected to the port transmits packets of the specific protocol group. The switch detects the traffic, adds the port to the protocol group, and begins forwarding flood traffic for that protocol group to that port. Autoconfigured ports are removed from the protocol group if the attached device does not transmit packets for that protocol within 60 minutes. Ports are also removed from the protocol group when the supervisor engine detects that the link is down on the port.

For example, if a host that supports both IP and Internetwork Packet Exchange (IPX) is connected to a switch port configured as **auto** for IPX, and the host is transmitting only IP traffic, the port to which the host is connected will not forward any IPX flood traffic to the host.

However, if the host transmits an IPX packet, the supervisor engine software detects the protocol traffic and the port is added to the IPX group, allowing the port to receive IPX flood traffic. If the host does not send any IPX traffic for more than 60 minutes, the port is removed from the IPX protocol group.

By default, ports are configured to **on** for the IP protocol group. Typically, you should only configure a port to **auto** for IP if there is a directly connected end station connected to the port. The default port configuration for IPX and Group is **auto**.

Packets are classified into these protocol groups:

- IP (**ip**)
- IPX (**ipx**)
- AppleTalk and DECnet (**group**)
- Packets not belonging to any of these protocols

Default Protocol Filtering Configuration

Table 18-1 shows the default protocol filtering configuration.

Table 18-1 Protocol Filtering Default Configuration

Feature	Default Value
Protocol filtering	Disabled
ip mode	on
ipx mode	auto
group mode	auto

Configuring Protocol Filtering

These sections describe how to configure protocol filtering on Ethernet, Fast Ethernet, and Gigabit Ethernet ports:

- [Configuring Protocol Filtering, page 18-3](#)
- [Disabling Protocol Filtering, page 18-3](#)

Configuring Protocol Filtering

To configure protocol filtering on Ethernet, Fast Ethernet, and Gigabit Ethernet ports, perform this task in privileged mode:

	Task	Command
Step 1	Enable protocol filtering on the switch.	set protocolfilter enable
Step 2	Set the protocol membership of the desired ports.	set port protocol <i>mod_num/port_num</i> {ip ipx group} {on off auto}
Step 3	Verify the port filtering configuration.	show port protocol [<i>mod_num[/port_num]</i>]

This example shows how to enable protocol filtering, set the protocol membership of ports, and verify the configuration:

```

Console> (enable) set protocolfilter enable
Protocol filtering enabled on this switch.
Console> (enable) set port protocol 3/1-4 ip on
IP protocol set to on mode on ports 3/1-4.
Console> (enable) set port protocol 3/1-4 ipx off
IPX protocol disabled on ports 3/1-4.
Console> (enable) set port protocol 3/1-4 group auto
Group protocol set to auto mode on ports 3/1-4.
Console> (enable) show port protocol 3/1-4
Port      Vlan      IP        IP Hosts IPX        IPX Hosts Group      Group Hosts
-----
3/1       4         on        1          off        0          auto-off  0
3/2       5         on        1          off        0          auto-on   1
3/3       2         on        1          off        0          auto-off  0
3/4       4         on        1          off        0          auto-on   1
Console> (enable)

```

Disabling Protocol Filtering

To disable protocol filtering, perform this task in privileged mode:

	Task	Command
	Disable protocol filtering on the switch.	set protocolfilter disable

This example shows how to disable protocol filtering:

```

Console> (enable) set protocolfilter disable
Protocol filtering disabled on this switch.
Console> (enable)

```

