

Configuring Protocol Filtering

This chapter describes how to configure protocol filtering on Ethernet, Fast Ethernet, and Gigabit Ethernet ports on the Catalyst 5000, 4000, 2948G, 2926G, and 2926 series 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* for your switch.

This chapter consists of these sections:

- Understanding How Protocol Filtering Works on page 26-1
- Protocol Filtering Hardware and Software Requirements on page 26-2
- Default Protocol Filtering Configuration on page 26-3
- Configuring Protocol Filtering on page 26-3

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. Protocol filtering is supported only on nontrunking Ethernet, Fast Ethernet, and Gigabit Ethernet ports.

Trunking ports are always members of all protocol groups. Filtering is not performed on trunk ports; therefore, there are no interoperability issues with switches without an NFFC. Layer 2 protocols, such as Spanning-Tree Protocol (STP) and Cisco Discovery Protocol (CDP), are not affected by protocol filtering. Dynamic 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**, the port is added to the group only after packets of the specific protocol are received on that port. With autolearning, ports become members of the protocol group only after receiving packets of the corresponding protocol from the device attached to that port.

Autoconfigured ports are removed from the protocol group if no packets are received 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, but 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 sends 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 stops sending 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 out the port. The default port configuration for IPX and Group is **auto**.

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.

On the Catalyst 5000, 2926G, and 2926 series switches, packets are classified into the following protocol groups:

- IP
- IPX
- AppleTalk, DECnet, and Banyan VINES (“group”)
- Packets not belonging to any of these protocols

On the Catalyst 4000 and 2948G series switches, packets are classified into the following protocol groups:

- IP
- IPX
- AppleTalk and DECnet (“group”)
- Packets not belonging to any of these protocols

Protocol Filtering Hardware and Software Requirements

Protocol filtering requires the following hardware and software:

- Catalyst 4000, 2948G, or 2926G series switch, or a Catalyst 5000 series switch with a Supervisor Engine III module and a NetFlow Feature Card (NFFC) or NFFC II.
- Supervisor engine software release 4.1 or later. Certain hardware requires a later version of software (for example, the NFFC II requires software release 4.3 or later).

Default Protocol Filtering Configuration

Table 26-1 shows the default protocol filtering configuration.

Table 26-1 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 Catalyst 5000 series Ethernet-type VLANs and on Ethernet and Fast Ethernet ports:

- Configuring Protocol Filtering on page 26-3
- Disabling Protocol Filtering on page 26-4

Configuring Protocol Filtering

To configure protocol filtering on Ethernet and Fast 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</i>[/<i>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 7/1-4 ip on
IP protocol set to on mode on ports 7/1-4.
Console> (enable) set port protocol 7/1-4 ipx off
IPX protocol disabled on ports 7/1-4.
Console> (enable) set port protocol 7/1-4 group auto
Group protocol set to auto mode on ports 7/1-4.
Console> (enable) show port protocol 7/1-4
Port      Vlan      IP        IP Hosts  IPX       IPX Hosts  Group    Group Hosts
-----
7/1       4         on        1         off        0          auto-off 0
7/2       5         on        1         off        0          auto-on  1
7/3       2         on        1         off        0          auto-off 0
7/4       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