



CHAPTER 36

Configuring Layer 3 Protocol Filtering

This chapter describes how to configure Layer 3 protocol filtering on Ethernet, Fast Ethernet, and Gigabit Ethernet ports on the Catalyst 6500 series switches.



Note

For complete syntax and usage information for the commands that are used in this chapter, refer to the *Catalyst 6500 Series Switch Command Reference* publication.

This chapter consists of these sections:

- [Understanding How Layer 3 Protocol Filtering Works, page 36-1](#)
- [Default Layer 3 Protocol Filtering Configuration, page 36-2](#)
- [Configuring Layer 3 Protocol Filtering on the Switch, page 36-2](#)

Understanding How Layer 3 Protocol Filtering Works

Layer 3 protocol filtering prevents certain protocol traffic from being forwarded out the switch ports. Layer 3 protocol filtering is implemented on the supervisor engine and does not require a Policy Feature Card (PFC) or Multilayer Switch Feature Card (MSFC). The broadcast and unicast flood traffic is filtered based on the membership of the ports in the different protocol groups. This filtering is in addition to the filtering that is provided by the port-VLAN membership. Layer 3 protocol filtering is supported only on the nontrunking Ethernet, Fast Ethernet, and Gigabit Ethernet ports.

The trunking ports are always members of all protocol groups. To avoid compatibility issues with the other networking devices, Layer 3 protocol filtering is not performed on the trunk ports. Layer 2 protocols, such as Spanning Tree Protocol (STP) and Cisco Discovery Protocol (CDP), are not affected by Layer 3 protocol filtering. The 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 the packets of the specific protocol are received on that port. With autolearning, the ports become members of the protocol group only after receiving the packets of the corresponding protocol from the device that is attached to that port. The autoconfigured ports are removed from the protocol group if no packets are received for that protocol within 60 minutes. The 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 that is configured as **auto** for IPX, but the host is transmitting only the IP traffic, the port to which the host is connected does 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 the IPX flood traffic. If the host stops sending the IPX traffic for more than 60 minutes, the port is removed from the IPX protocol group.

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

With Layer 3 protocol filtering enabled, the ports are identified on a protocol basis. A port can be a member of one or more protocol groups. The flood traffic for each protocol group is forwarded out a port only if that port belongs to the appropriate protocol group.

The packets are classified into these protocol groups:

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

Default Layer 3 Protocol Filtering Configuration

Table 36-1 shows the default Layer 3 protocol filtering configuration.

Table 36-1 Layer 3 Protocol Filtering Default Configuration

Feature	Default Value
Layer 3 protocol filtering	Disabled
ip mode	on
ipx mode	auto
group mode	auto

Configuring Layer 3 Protocol Filtering on the Switch

These sections describe how to configure Layer 3 protocol filtering on the Ethernet-type VLANs and on any type of Ethernet port:

- [Enabling Layer 3 Protocol Filtering, page 36-3](#)
- [Disabling Layer 3 Protocol Filtering, page 36-3](#)

Enabling Layer 3 Protocol Filtering



Note Protocol filtering is supported only on the Ethernet VLANs and on the nontrunking EtherChannel ports. The **set protocolfilter** command is not supported on the Network Analysis Module (NAM), the Supervisor Engine 720, or the Supervisor Engine 32.

To enable Layer 3 protocol filtering on the Ethernet ports, perform this task in privileged mode:

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

This example shows how to enable Layer 3 protocol filtering, set the protocol membership of the 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 Layer 3 Protocol Filtering

To disable Layer 3 protocol filtering, perform this task in privileged mode:

	Task	Command
	Disable Layer 3 protocol filtering on the switch.	set protocolfilter disable

This example shows how to disable Layer 3 protocol filtering:

```

Console> (enable) set protocolfilter disable

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

```

