12

Traffic/Security Filters and Monitors

Contents

Overview

Applicable Switch Models. As of June 2007, Traffic/Security filters are available on these current ProCurve switch models:

Switch Models	Source-Port Filters	Protocol Filters	Multicast Filters
Switch 8212zl	Yes	Yes	Yes
Series 6400cl	Yes	*No*	*No*
Series 5400zl	Yes	Yes	Yes
Series 4200vl	Yes	*No*	*No*
Series 3500yl	Yes	*Yes*	*Yes*
Series 3400cl	Yes	*No*	*No*
Series 2800	Yes	*No*	*No*
Series 2500	Yes	Yes	Yes
Switch 4000m and 8000m	Yes	Yes	Yes

This chapter describes Traffic/Security filters on the switches covered in this guide. For information on filters for other switches in the above table, refer to the documentation provided for those switches.

Introduction

Feature	Default	Menu	CLI	Web
configure source-port filters	none	n/a	page 12-21	n/a
configure protocol filters	none	n/a	page 12-21	n/a
configure multicast filters	none	n/a	page 12-21	n/a
display filter data	n/a	n/a	page 12-23	n/a

You can enhance in-band security and improve control over access to network resources by configuring static filters to forward (the default action) or drop unwanted traffic. That is, you can configure a traffic filter to either forward or drop all network traffic moving to outbound (destination) ports and trunks (if any) on the switch.

Filter Limits

The switch accepts up to 101 static filters. These limitations apply:

- Source-port filters: up to 78
- Multicast filters: up to 16 with 1024 or fewer VLANs configured. Up to 8 with more than 1024 VLANs configured.
- Protocol filters: up to 7

Using Port Trunks with Filters

The switch manages a port trunk as a single source or destination for source-port filtering. If you configure a port for filtering before adding it to a port trunk, the port retains the filter configuration, but suspends the filtering action while a member of the trunk. If you want a trunk to perform filtering, first configure the trunk, then configure the trunk for filtering. Refer to "Configuring a Filter on a Port Trunk" on page 12-19.

Filter Types and Operation

Table 12-1. Filter Types and Criteria

Static Filter Type	Selection Criteria
Source-Port	Inbound traffic from a designated, physical source-port will be forwarded or dropped on a per-port (destination) basis.
Multicast	Inbound traffic having a specified multicast MAC address will be forwarded to outbound ports (the default) or dropped on a per-port (destination) basis.
Protocol	Inbound traffic having the selected frame (protocol) type will be forwarded or dropped on a per-port (destination) basis.

Source-Port Filters

This filter type enables the switch to forward or drop traffic from *all* end nodes on the indicated source-port to specific destination ports.
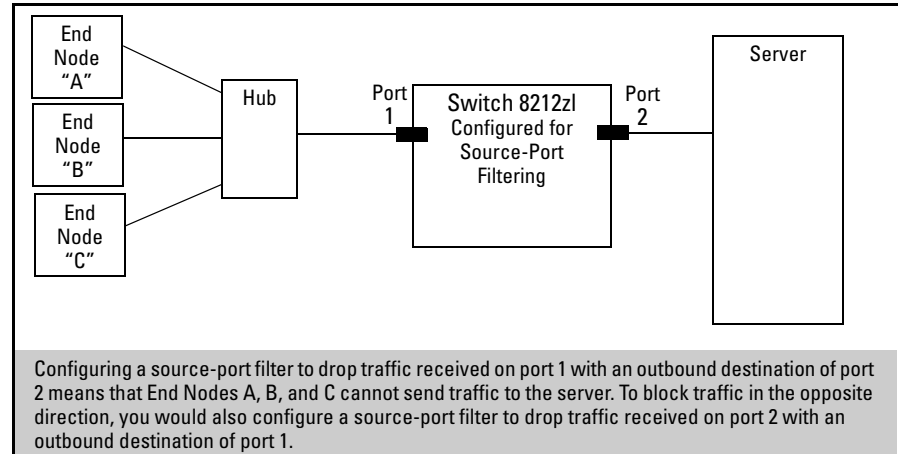

Configuring a source-port filter to drop traffic received on port 1 with an outbound destination of port 2 means that End Nodes A, B, and C cannot send traffic to the server. To block traffic in the opposite direction, you would also configure a source-port filter to drop traffic received on port 2 with an outbound destination of port 1.

Figure 12-1. Example of a Source-Port Filter Application

Operating Rules for Source-Port Filters

■ You can configure one source-port filter for each physical port and port trunk on the switch. (Refer to the **filter** command on page 12-18.)

■ You can include all destination ports and trunks in the switch on a single source-port filter.

■ Each source-port filter includes:

   • One source port or port trunk (**trk1**, **trk2**, …**trk***n*)
   • A set of destination ports and/or port trunks that includes all untrunked LAN ports and port trunks on the switch
   • An action (forward or drop) for each destination port or port trunk

When you create a source-port filter, the switch automatically sets the filter to forward traffic from the designated source to all destinations for which you do not specifically configure a "drop" action. Thus, it is not necessary to configure a source-port filter for traffic you want the switch to forward unless the filter was previously configured to drop the desired traffic.

■ When you create a source port filter, all ports and port trunks (if any) on the switch appear as destinations on the list for that filter, even if routing is disabled and separate VLANs and/or subnets exist. Where traffic would normally be allowed between ports and/or trunks, the switch automatically forwards traffic to the outbound ports and/or trunks you do not specifically configure to drop traffic. (Destination ports that comprise a trunk are listed collectively by the trunk name— such as **Trk1**— instead of by individual port name.)

■ Packets allowed for forwarding by a source-port filter are subject to the same operation as inbound packets on a port that is not configured for source-port filtering.

■ With multiple IP addresses configured on a VLAN, and routing enabled on the switch, a single port or trunk can be both the source and destination of packets moving between subnets in that same VLAN. In this case, you can prevent the traffic of one subnet from being routed to another subnet of the same port by configuring the port or trunk as both the source and destination for traffic to drop.

Example

If you wanted to prevent server "A" from receiving traffic sent by workstation "X", but do not want to prevent any other servers or end nodes from receiving traffic from workstation "X", you would configure a filter to drop traffic from port 5 to port 7. The resulting filter would drop traffic from port 5 to port 7, but would forward all other traffic from any source port to any destination port. (Refer to figures 12-2 and 12-3.
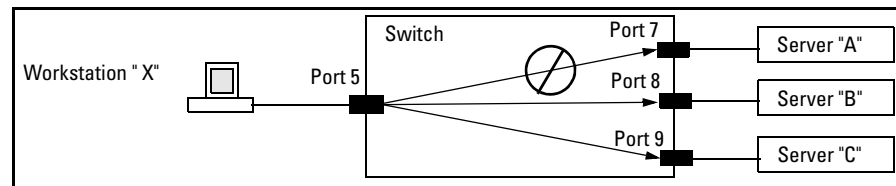

Figure 12-2. Example of a Filter Blocking Traffic only from Port 5 to Server "A"

```
Traffic/Security Filters

 Filter Type : Source Port
 Source Port : 5

 Dest Port  Type      | Action
 --------- --------- + -------
 1          100/1000T | Forward
 2          100/1000T | Forward
 3          100/1000T | Forward
 4          100/1000T | Forward
 5          100/1000T | Forward
 6          100/1000T | Forward
 7          100/1000T | Drop
 8          100/1000T | Forward
 9          100/1000T | Forward
 10         100/1000T | Forward
 .              .         .
 .              .         .
 .              .         .
 22         100/1000T | Forward
 23         100/1000T | Forward
 24         100/1000T | Forward
```

This list shows the filter created to block (drop) traffic from source port 5 (workstation "X") to destination port 7 (server "A"). Notice that the filter allows traffic to move from source port 5 to all other destination ports.

Figure 12-3. The Filter for the Actions Shown in Figure 12-2

Named Source-Port Filters

You can specify named source-port filters that may be used on multiple ports and port trunks. A port or port trunk can only have one source-port filter, but by using this capability you can define a source-port filter once and apply it to multiple ports and port trunks. This can make it easier to configure and manage source-port filters on your switch. The commands to define, configure, apply, and display the status of named source-port filters are described below.

Operating Rules for Named Source-Port Filters

■   A port or port trunk may only have one source-port filter, named or not named.

■   A named source-port filter can be applied to multiple ports or port trunks.

■   Once a named source-port filter is defined, subsequent changes only modify its action, they don't replace it.

■   To change the named source-port filter used on a port or port trunk, the current filter must first be removed, using the **no filter source-port named-filter <filter-name >** command.

■   A named source-port filter can only be deleted when it is not applied to any ports.

Defining and Configuring Named Source-Port Filters

The named source-port filter command operates from the global configuration level.

Syntax: [no] filter source-port named-filter <*filter-name*>

> *Defines or deletes a named source-port filter. The <filter-name> may contain a maximum of 20 alpha-numeric characters (longer names may be specified, but they are not displayed.) A filter-name cannot be a valid port or port trunk name.*
>
> *The maximum number of named source-port filters that can be used is equal to the number of ports on a switch.*
>
> *A named source-port filter can only be removed if it is not in use (use the* **show filter source-port** *command to check the status). Named source-port filters are not automatically deleted when they are no longer used.*
>
> *Use the* **no** *option to delete an unused named source-port filter.*

Syntax: filter source-port named-filter <*filter-name* > drop < *destination-port-list* >

> *Configures the named source-port filter to drop traffic having a destination on the ports and/or port trunks in the < destination-port-list >. Can be followed by the* **forward** *option if you have other destination ports or port trunks previously set to* **drop** *that you want to change to* **forward***. For example:*
>
> *filter source-port named-filter <filter-name > drop < destina-tion-port-list > forward < destination-port-list>*
>
> *The* **destination-port-list** *may contain ports, port trunks, and ranges (for example 3-7 or trk4-trk9) separated by commas.*

Syntax: filter source-port named-filter <*filter-name* > forward
< *destination-port-list* >

> *Configures the named source-port filter to forward traffic having a destination on the ports and/or port trunks in the* <**destination-port-list**>*. Since "forward" is the default state for destinations in a filter, this command is useful when destinations in an existing filter are configured for "drop" and you want to change them to "forward". Can be followed by the* **drop** *option if you have other destination ports set to* **forward** *that you want to change to* **drop***. For example:*
>
> filter source-port named-filter <*filter-name* > forward < *destination-port-list* > drop < *destination-port-list* >

A named source-port filter must first be defined and configured before it can
be applied. In the following example two named source-port filters are
defined, **web-only** and **accounting**.

```
ProCurve(config)# filter source-port named-filter web-
only
```

```
ProCurve(config)# filter source-port named-filter
accounting
```

By default, these two named source-port filters forward traffic to all ports and
port trunks.

To configure a named source-port filter to prevent inbound traffic from being
forwarded to specific destination switch ports or port trunks, the **drop** option
is used. For example, on a 26-port switch, to configure the named source-
port filter **web-only** to drop any traffic except that for destination ports 1 and 2, the
following command would be used:

```
ProCurve(config)# filter source-port named-filter web-
only drop 3-26
```

A named source-port filter can be defined and configured in a single command
by adding the **drop** option, followed by the required destination-port-list.

Viewing a Named Source-Port Filter

You can list all source-port filters configured in the switch, both named and
unnamed, and their action using the **show** command below.

Syntax: show filter source-port

> *Displays a listing of configured source-port filters, where
> each filter entry includes a Filter Name, Port List, and
> Action:*
>
> > ***Filter Name***: *The filter-name used when a named
> > source-port filter is defined. Non-named source-port
> > filters are automatically assigned the port or port trunk
> > number of the source port.*
> >
> > ***Port List***: *Lists the port and port trunk destinations
> > using the filter. Named source-port filters that are not in
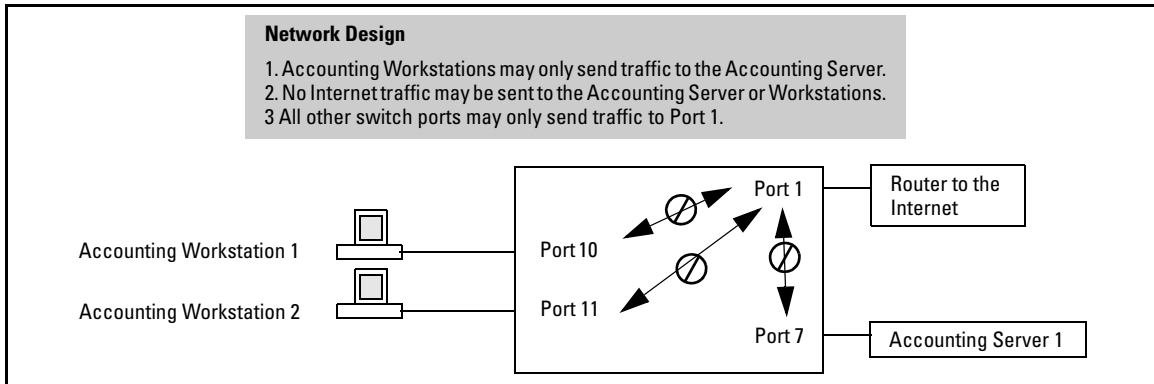> > use display* ***NOT USED***.
> >
> > ***Action***: *Lists the ports and port trunks dropped by the
> > filter. If a named source-port filter has been defined but
> > not configured, this field is blank.*

> [index] *For the supplied index (IDX) displays the action taken
> (Drop or Forward) for each destination port on the switch.*

Using Named Source-Port Filters

A company wants to manage traffic to the Internet and its accounting server on a 26-port switch. Their network is pictured in Figure 12-4. Switch port 1 connects to a router that provides connectivity to a WAN and the Internet. Switch port 7 connects to the accounting server. Two workstations in accounting are connected to switch ports 10 and 11.

Network Design

1. Accounting Workstations may only send traffic to the Accounting Server.
2. No Internet traffic may be sent to the Accounting Server or Workstations.
3 All other switch ports may only send traffic to Port 1.

Accounting Workstation 1

Accounting Workstation 2

Port 10

Port 11

Port 1

Port 7

Router to the Internet

Accounting Server 1

Figure 12-4. Network Configuration for Named Source-Port Filters Example

Defining and Configuring Example Named Source-Port Filters. While named source-port filters may be defined and configured in two steps, this is not necessary. Here we define and configure each of the named source-port filters for our example network in a single step.

```
ProCurve(config)# filter source-port named-filter web-only drop 2-26
ProCurve(config)# filter source-port named-filter accounting drop 1-6,8,9,12-26
ProCurve(config)# filter source-port named-filter no-incoming-web drop 7,10,11

ProCurve(config)# show filter source-port

Traffic/Security Filters

Filter Name           | Port List           | Action
 ------------------- + ------------------- + -------------------
web-only              | NOT USED            | drop 2-26
accounting            | NOT USED            | drop 1-6,8-9,12-26
no-incoming-web       | NOT USED            | drop 7,10-11

ProCurve Switch 2626(config)#
```

Ports and port trunks using the filter. When **NOT USED** is displayed the named source-port filter may be deleted.

Lists the ports and port trunks dropped by the filter. Ports and port trunks not shown are forwarded by the filter.

To remove a port or port trunk from the list, update the named source-port filter definition using the **forward** option.

Figure 12-5. Applying Example Named Source-Port Filters

Once the named source-port filters have been defined and configured we now apply them to the switch ports.

```
ProCurve(config)# filter source-port 2-6,8,9,12-26 named-filter web-only
ProCurve(config)# filter source-port 7,10,11 named-filter accounting
ProCurve(config)# filter source-port 1 named-filter no-incoming-web
ProCurve(config)#
```

Figure 12-6. Source Port Filters Applied to Switch Ports

The **show filter** command shows what ports have filters applied.

```
ProCurve(config)# show filter

Traffic/Security Filters

 IDX Filter Type   | Value
 --- ------------- + -------------------
  1   Source Port  | 2
  2   Source Port  | 3
  3   Source Port  | 4
  4   Source Port  | 5
  5   Source Port  | 6
  6   Source Port  | 8
  7   Source Port  | 9
  8   Source Port  | 12

  20  Source Port  | 24
  21  Source Port  | 25
  22  Source Port  | 26
  23  Source Port  | 7
  24  Source Port  | 10
  25  Source Port  | 11
  26  Source Port  | 1
```

Indicates the port number or port-trunk name of the source port or trunk assigned to the filter.

An automatically assigned index number used to identify the filter for a detailed information listing. A filter retains its assigned IDX number for as long as the filter exists in the switch. The switch assigns the lowest available IDX number to a new filter. This can result in a newer filter having a lower IDX number than an older filter if a previous (source-port or named source-port) filter deletion created a gap in the filter listing.

Figure 12-7. Example of the show filter Command

Using the **IDX** value in the **show filter** command, we can see how traffic is filtered on a specific port (**Value**).The two outputs below show a non-accounting and an accounting switch port.

```
ProCurve(config)# show filter 4        ProCurve(config)# show filter 24

 Traffic/Security Filters               Traffic/Security Filters

  Filter Type : Source Port              Filter Type : Source Port
  Source Port : 5                        Source Port : 10

  Dest   Port Type     | Action          Dest   Port Type     | Action
  --------- --------- + -------          --------- --------- + -----------
  1       10/100TX    | Forward          1         10/100TX    | Drop
  2       10/100TX    | Drop             2         10/100TX    | Drop
  3       10/100TX    | Drop             3         10/100TX    | Drop
  4       10/100TX    | Drop             4         10/100TX    | Drop
  5       10/100TX    | Drop             5         10/100TX    | Drop
  6       10/100TX    | Drop             6         10/100TX    | Drop
  7       10/100TX    | Drop             7         10/100TX    | Forward
  8       10/100TX    | Drop             8         10/100TX    | Drop
  9       10/100TX    | Drop             9         10/100TX    | Drop
  10      10/100TX    | Drop             10        10/100TX    | Drop
  11      10/100TX    | Drop             11        10/100TX    | Drop
  12      10/100TX    | Drop             12        10/100TX    | Drop
   .         .          .                 .          .            .
```

Figure 12-8. Example Showing Traffic Filtered on Specific Ports

The same command, using IDX 26, shows how traffic from the Internet is
handled.

```
ProCurve(config)# show filter 26

 Traffic/Security Filters

  Filter Type : Source Port
  Source Port : 1

  Dest    Port Type    | Action
  --------- --------- + -----------------------
  1         10/100TX    | Forward
  2         10/100TX    | Forward
  3         10/100TX    | Forward
  4         10/100TX    | Forward
  5         10/100TX    | Forward
  6         10/100TX    | Forward
  7         10/100TX    | Drop
  8         10/100TX    | Forward
  9         10/100TX    | Forward
  10        10/100TX    | Drop
  11        10/100TX    | Drop
  12        10/100TX    | Forward
    .           .          .
```

Figure 12-9. Example of Source Port Filtering with Internet Traffic

As the company grows, more resources are required in accounting. Two additional accounting workstations are added and attached to ports 12 and 13. A second server is added attached to port8.
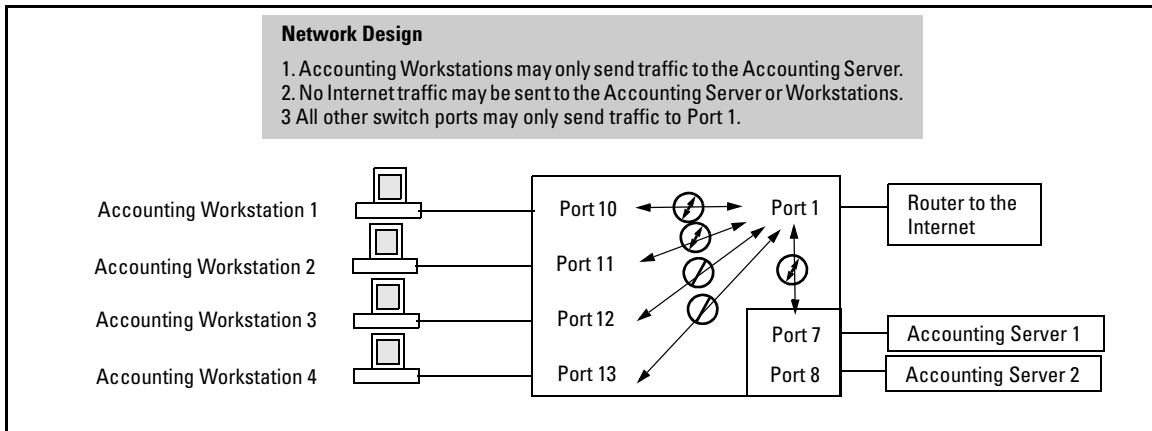

Network Design

1. Accounting Workstations may only send traffic to the Accounting Server.
2. No Internet traffic may be sent to the Accounting Server or Workstations.
3 All other switch ports may only send traffic to Port 1.

Accounting Workstation 1 — Port 10
Accounting Workstation 2 — Port 11
Accounting Workstation 3 — Port 12
Accounting Workstation 4 — Port 13
Port 1 — Router to the Internet
Port 7 — Accounting Server 1
Port 8 — Accounting Server 2

Figure 12-10. Expanded Network Configuration for Named Source-Port Filters Example

The following revisions to the named source-port filter definitions maintain the desired network traffic management, as shown in the **Action** column of the **show** command.

```
ProCurve(config)# filter source-port named-filter accounting forward 8,12,13
ProCurve(config)# filter source-port named-filter no-incoming-web drop 8,12,13
ProCurve(config)#
ProCurve(config)# show filter source-port

 Traffic/Security Filters

 Filter Name            | Port List               | Action
 ------------------- + ------------------- + ------------------------
 web-only               | 2-6,8-9,12-26           | drop 2-26
 accounting             | 7,10-11                 | drop 1-6,9,14-26
 no-incoming-web        | 1                       | drop 7-8,10-13

ProCurve(config)#
```

Figure 12-11. Example Showing Network Traffic Management with Source Port Filters

We next apply the updated named source-port filters to the appropriate switch ports. As a port can only have one source-port filter (named or not named), before applying the new named source-port filters we first remove the existing source-port filters on the port.

```
ProCurve(config)# no filter source-port 8,12,13
ProCurve(config)# filter source-port 8,12,13 named-filter accounting
ProCurve(config)#
```

The named source-port filters now manage traffic on the switch ports as shown below, using the **show filter source-port** command.

```
ProCurve(config)# show filter source-port

 Traffic/Security Filters

 Filter Name          | Port List           | Action
 -------------------- + -------------------- + -------------------------
 web-only             | 2-6,9,14-26         | drop 2-26
 accounting           | 7-8,10-13           | drop 1-6,9,14-26
 no-incoming-web      | 1                   | drop 7-8,10-13

ProCurve(config)#
```

Figure 12-12. Named Source-Port Filters Managing Traffic

Static Multicast Filters

This filter type enables the switch to forward or drop multicast traffic to a specific set of destination ports. This helps to preserve bandwidth by reducing multicast traffic on ports where it is unnecessary, and to isolate multicast traffic to enhance security.

You can configure up to 16 static multicast filters (defined by the **filter** command—page 12-21). However, if an IGMP-controlled filter for a joined multicast group has the same multicast address as a static multicast filter configured on a given port, the IGMP-controlled filter overrides the static multicast filter configured on that port. Note that in the default configuration, IGMP is disabled on VLANs configured in the switch. To enable IGMP on a specific VLAN, use the **vlan < *vid* > ip igmp** command. (For more on this command, refer to the chapter titled "Multimedia Traffic Control with IP Multicast (IGMP)" in the *Multicast and Routing Guide* for your switch.)

The total of static multicast filters and IGMP multicast filters together can range from 389 to 420, depending on the current **max-vlans** setting in the switch. If multiple VLANs are configured, then each filter is counted once per VLAN in which it is used.

Table 12-2.   Multicast Filter Limits

Max-VLANs Setting	Maximum # of Multicast Filters (Static and IGMP Combined)
1 (the minimum)	420
8 (the default)	413
32 or higher	389

N o t e s

Per-Port IP Multicast Filters. The static multicast filters described in this section filter traffic having a multicast address you specify. To filter all multicast traffic on a per-VLAN basis, refer to the section titled "Configuring and Displaying IGMP" in the chapter titled "Multimedia Traffic Control with IP Multicast (IGMP)" in the *Multicast and Routing Guide* for your switch.

IP Multicast Filters. Multicast filters are configured using the Ethernet format for the multicast address. IP multicast addresses occur in the range of 224.0.0.0 through 239.255.255.255 (which corresponds to the Ethernet multi-cast address range of 01005e-000000 through 01005e-7fffff). Any static Traffic/ Security filters configured with a **multicast** filter type and a multicast address in this range will continue to be in effect unless IGMP learns of a multicast group destination in this range. In this case, IGMP takes over the filtering function for the multicast destination address(es) for as long as the IGMP group is active. If the IGMP group subsequently deactivates, the static filter resumes control over traffic to the multicast address.

C a u t i o n

If Spanning Tree is enabled, then the MSTP multicast MAC address (0180c2-000000) should not be filtered. (STP will not operate properly if the MSTP multicast MAC address is filtered.)

Protocol Filters

This filter type enables the switch to forward or drop, on the basis of protocol type, traffic to a specific set of destination ports on the switch. Filtered protocol types include:

- AppleTalk
- ARP
- IPX

- NetBEUI
- SNA

Only one filter for a particular protocol type can be configured at any one time. For example, a separate protocol filter can be configured for each of the protocol types listed above, but only one of those can be an IP filter. Also, the destination ports for a protocol filter can be on different VLANs.

You can configure up to seven protocol filters.

Configuring Traffic/Security Filters

Use this procedure to specify the type of filters to use on the switch and whether to forward or drop filtered packets for each filter you specify.

1. Select the static filter type(s).

2. For inbound traffic matching the filter type, determine the filter action you want for each outbound (destination) port on the switch (forward or drop). The default action for a new filter is to forward traffic of the specified type to all outbound ports.

3. Configure the filter.

4. Use **show filter** (page 12-23) to check the filter listing to verify that you have configured correct action for the desired outbound ports.

Configuring a Source-Port Traffic Filter

Syntax: [no] filter

[source-port < *port-number* | *trunk-name*>]

Specifies one inbound port or trunk. Traffic received inbound on this interface from other devices will be filtered. The **no** *form of the command deletes the source-port filter for* < port-number > *and returns the destination ports for that filter to the* **Forward** *action. (Default: Forward on all ports.)*

Note: *If multiple VLANs are configured, the source-port and the destination port(s) must be in the same VLAN unless routing is enabled. Similarly, if a VLAN containing both the source and destination is multi-netted, the source and destination ports and/or trunks must be in the same subnet unless routing is enabled.*

[drop] < *destination-port-list* > [forward < *port-list* >]

Configures the filter to drop traffic for the ports and/or trunks in the designated **< destination-port-list >**. *Can be followed by* **forward < destination-port-list >** *if you have other destination ports set to* **drop** *that you want to change to* **forward**. *If no drop or forward action is specified, the switch automatically creates a filter with a* **forward** *action from the designated source port (or trunk) to all destination ports (or trunks) on the switch.*

[forward] < *port-list* >

Configures the filter to forward traffic for the ports and/ or trunks in the designated **< destination-port-list >**. *Because* **forward** *is the default state for destinations in a filter, this command is useful when destinations in an existing filter are configured for* **drop** *and you want to change them to* **forward**. *Can be followed by* **drop < destination-port-list >** *if you have other destination ports set to* **forward** *that you want to change to* **drop**. *If no drop or forward action is specified, the switch automatically creates a filter with a forward action from the designated source port (or trunk) to all desti-nation ports (or trunks) on the switch.*

Example of Creating a Source-Port Filter

For example, assume that you want to create a source-port filter that drops all traffic received on port 5 with a destination of port trunk 1 (**Trk1**) and any port in the range of port 10 to port 15. To create this filter you would execute this command:

```
ProCurve(config)# filter source-port 5 drop trk1,10-15
```

Later, suppose you wanted to shift the destination port range for this filter up by two ports; that is, to have the filter drop all traffic received on port 5 with a destination of any port in the range of port 12 to port 17. (The **Trk1** destination is already configured in the filter and can remain as-is.)With one command you can restore forwarding to ports 10 and 11 while adding ports 16 and 17 to the "drop" list:

```
ProCurve(config)# filter source-port 5 forward 10-11 drop
16-17
```

Configuring a Filter on a Port Trunk

This operation uses the same command as is used for configuring a filter on an individual port. However, the configuration process requires two steps:

1. Configure the port trunk.

2. Configure a filter on the port trunk by using the trunk name (**trk1**, **trk2**, ...**trk6**) instead of a port name.

For example, to create a filter on port trunk 1 to drop traffic received inbound for trunk 2 and ports 10-15:

```
ProCurve(config)# filter source-port trk1 drop trk2,10-15
```

Note that if you first configure a filter on a port and then later add the port to a trunk, the port remains configured for filtering *but the filtering action will be suspended while the port is a member of the trunk.* That is, the trunk does not adopt filtering from the port configuration. You must still explicitly configure the filter on the port trunk. If you use the **show filter < *index* >** command for a filter created before the related source port was added to a trunk, the port number appears between asterisks (*), indicating that the filter action has been suspended for that filter. For example, if you create a

filter on port 5, then create a trunk with ports 5 and 6, and display the results, you would see the following:

```
ProCurve(config)# filter source-port 5 drop 2
ProCurve(config)# trunk 5-6 trk1
ProCurve(config)# show filter

 Traffic/Security Filters

  IDX Filter Type  | Value
  --- ------------ + ------------------
  1   Source Port  | *5*

ProCurve(config)# show filter 1

 Traffic/Security Filters

  Filter Type : Source Port
  Source Port : *5*

  Dest Port Type      | Action
  --------- --------- + -------
  1         100/1000T | Forward
  2         100/1000T | Drop
  3         100/1000T | Forward
  4         100/1000T | Forward
  .         .           .
  .         .           .
  .         .           .
```

The *5* shows that port 5 is configured for filtering, but the filtering action has been suspended while the port is a member of a trunk.

If you want the trunk to which port 5 belongs to filter traffic, then you must explicitly configure filtering on the trunk.

Note: If you configure an existing trunk for filtering and later add another port to the trunk, the switch will apply the filter to all traffic moving on any link in the trunk. If you remove a port from the trunk it returns to the configuration it had before it was added to the trunk

Figure 12-13. Example of Switch Response to Adding a Filtered Source Port to a Trunk

Editing a Source-Port Filter

The switch includes in one filter the action(s) for all destination ports and/or trunks configured for a given source port or trunk. Thus, if a source-port filter already exists and you want to change the currently configured action for some destination ports or trunks, use the **filter source-port** command to update the existing filter. For example, suppose you configure a filter to drop traffic received on port 8 and destined for ports 1 and 2. The resulting filter is shown on the left in figure 12-14. Later, you update the filter to drop traffic received on port 8 and destined for ports 3 through 5. Since only one filter exists for a given source port, the filter on traffic from port 8 appears as shown on the right in figure 12-14:

```
ProCurve(config)# show filter 1          ProCurve(config)# show filter 1

 Traffic/Security Filters                 Traffic/Security Filters

  Filter Type : Source Port                Filter Type : Source Port
  Source Port : 8                          Source Port : 8

  Dest Port Type      | Action            Dest Port Type      | Action
  --------- --------- + ------            --------- --------- + ------
  1         100/1000T | Drop              1         100/1000T | Drop
  2         100/1000T | Drop              2         100/1000T | Drop
  3         100/1000T | Forward           3         100/1000T | Drop
  4         100/1000T | Forward           4         100/1000T | Drop
  5         100/1000T | Forward           5         100/1000T | Drop
  6         100/1000T | Forward           6         100/1000T | Forward
  7         100/1000T | Forward           7         100/1000T | Forward
  8         100/1000T | Forward           8         100/1000T | Forward
  9         100/1000T | Forward           9         100/1000T | Forward
  10        100/1000T | Forward           10        100/1000T | Forward
```

Figure 12-14. Assigning Additional Destination Ports to an Existing Filter

Configuring a Multicast or Protocol Traffic Filter

Syntax: [no] filter

[multicast < *mac- address* >]

Specifies a multicast address. Inbound traffic received (on any port) with this multicast address will be filtered. (Default: Forward on all ports.)

The **no** *form of the command deletes the multicast filter for the < mac-address > multicast address and returns the destination ports for that filter to the* **Forward** *action.*

[< forward | drop > < *port-list* >]

Specifies whether the designated destination port(s) should forward or drop the filtered traffic.

[protocol < ip | ipx | arp | appletalk | sna | netbeui >]

Specifies a protocol type. Traffic received (on any port) with this protocol type will be filtered. (Default: Forward on all ports.)

The **no** *form of the command deletes the protocol filter for the specified protocol and returns the destination ports for that filter to the* **Forward** *action.*

[< forward | drop > < *port-list* >]

Specifies whether the designated destination port(s) should forward or drop the filtered traffic.

For example, suppose you wanted to configure the filters in table 12-3 on a switch. (For more on source-port filters, refer to "Configuring a Source-Port Traffic Filter" on page 12-18.)

Table 12-3.   Filter Example

Filter Type	Filter Value	Action	Destination Ports
Source-Port	Inbound ports: A1, A2*	Drop	D1-D4
Multicast	010000-123456	Drop	C1-C24, D5-D10
Multicast	010000-224466	Drop	B1-B4
Protocol	Appletalk	Drop	C12-C18, D1
Protocol	ARP	Drop	D17, D21-D24

*Because the switch allows one inbound port in a source-port filter, the requirement to filter ports A1 and A2 means you will configure two separate source-port filters.

The following commands configure the filters listed above:

```
ProCurve(config)# filter source-port a1 drop e d1-d4
ProCurve(config)# filter source-port a2 drop d1-d4
ProCurve(config)# filter multicast 010000-123456 drop e c1-c24,d5-d10
ProCurve(config)# filter multicast 010000-224466 drop e b1-b4
ProCurve(config)# filter protocol appletalk drop e c12-c18,d1
ProCurve(config)# filter protocol arp drop e d17,d21-d24
```

Figure 12-15. Configuring Various Traffic/Security Filters

Filter Indexing

The switch automatically assigns each new filter to the lowest-available index (IDX) number. The index numbers are included in the **show filter** command described in the next section and are used with the **show filter < *index* >** command to display detailed information about a specific filter.

If there are no filters currently configured, and you create three filters in succession, they will have index numbers 1 - 3. However, if you then delete the filter using index number "2" and then configure two new filters, the first new filter will receive the index number "2" and the second new filter will receive the index number "4". This is because the index number "2" was made vacant by the earlier deletion, and was therefore the lowest index number available for the next new filter.

Displaying Traffic/Security Filters

This command displays a listing of all filters by index number and also enables you to use the index number to display the details of individual filters.

Syntax: show filter

> *Lists the filters configured in the switch, with corresponding filter index (**IDX**) numbers.*
> **IDX**: *An automatically assigned index number used to identify the filter for a detailed information listing. A filter retains its assigned IDX number for as long as the filter exists in the switch. The switch assigns the lowest available IDX number to a new filter. This can result in a newer filter having a lower IDX number than an older filter if a previous filter deletion created a gap in the filter listing.*
> **Filter Type**: *Indicates the type of filter assigned to the **IDX** number (source-port, multicast, or protocol).*
> **Value**: *Indicates the port number or port-trunk name of the source port or trunk assigned to the filter*

[*index*]

> Lists the filter type and other data for the filter corresponding to the index number in the **show filter** output. Also lists, for each outbound destination port in the switch, the port number, port type, and filter action (forward or drop). The switch assigns the lowest available index number to a new filter. If you delete a filter, the index number for that filter becomes available for the next filter you create.

For example, to display the filters created in figure 12-15 on page 12-22 and then list the details of the multicast filter for multicast address **010000-224466**:

```
ProCurve(config)# show filter

   Traffic/Security Filters

   IDX Filter Type  | Value
   --- ------------ + ----------------
   1   Source Port  | A1
   2   Source Port  | A2
   3   Multicast    | 010000-123456
   4   Multicast    | 010000-224466
   5   Protocol     | AppleTalk
   6   Protocol     | ARP

ProCurve(config)# show filter 4

   Traffic/Security Filters

   Filter Type : Multicast
   Multi-cast Address : 010000-224466

   Dest Port Type       | Action
   --------- ---------- + -------
   A1        1000LX     | Forward
   A2                   | Forward
   A3                   | Forward
   A4        1000SX     | Forward
   B1        100/1000T  | Drop
   B2        100/1000T  | Drop
   B3        100/1000T  | Drop
   B4        100/1000T  | Drop
   C1        10/100TX   | Forward
   C2        10/100TX   | Forward
   C3        10/100TX   | Forward
   C4        10/100TX   | Forward
   C5        10/100TX   | Forward
   C6        10/100TX   | Forward
   C7        10/100TX   | Forward
-- MORE --, next page: Space, next line: Enter,
```

Lists all filters configured in the switch.

Filter Index Numbers (Automatically Assigned)

Criteria for Individual Filters

Uses the index number (IDX) for a specific filter to list the details for that filter only.

Figure 12-16. Example of Displaying Filter Data