

Traffic/Security Filters

(HP ProCurve Series 2600/2600-PWR and 2800 Switches)

Contents

Overview	10-2
Using Source-Port Filters	10-4
Operating Rules for Source-Port Filters	10-4
Configuring a Source-Port Filter	10-5
Viewing a Source-Port Filter	10-7
Filter Indexing	10-8
Editing a Source-Port Filter	10-9

Overview

Applicable Switch Models. Traffic/Security filters are available on these current HP ProCurve switch models:

- HP ProCurve Series 2600/2600-PWR Switches (source-port filters)
- HP ProCurve Switch 2800 Series (source-port filters)
- HP ProCurve Switch 2512 and 2524 (source-port, multicast, and protocol filters)

This chapter describes Traffic/Security filters on the Switch 2800 Series devices. For information on filters for the Switch 2512 and 2524, refer to the *Management and Configuration Guide* provided for these devices.

General Operation. You can enhance in-band security and improve control over access to network resources by configuring static per-port 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 between an inbound (source) port or trunk and any outbound (destination) ports and trunks (if any) on the switch.

- With routing disabled on the switch (the default), source-port filtering can operate on traffic moving within the same VLAN.
- With routing enabled on the switch, source-port filtering can operate on traffic moving between VLANs as well as within the same VLAN. (If you configure multinetting within a VLAN and enable routing on the switch, you can use source-port filtering to filter traffic between subnets within the same VLAN.)

Note

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 10-6.

When you create a source port filter, all ports or port trunks on the switch appear as destinations on the list for that filter. The switch automatically forwards traffic to the 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.) For example, if you want 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 10-1 and 10-2.

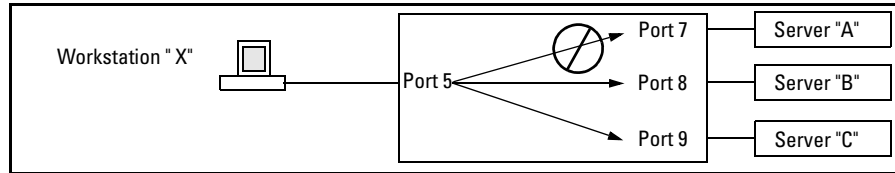


Figure 10-1. Example of a Filter Blocking Traffic only from Port 5 to Server "A"

```

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 10-2. The Filter for the Actions Shown in Figure 10-1

Applying a Source Port Filter in a Multinetted VLAN. If you have multiple IP addresses configured on the same VLAN (multinetting), and routing is enabled on the switch, then 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 on the same port by configuring the port or trunk as both the source and destination for traffic to drop.

Using Source-Port Filters

This feature is available only on the Series 2600, 2600-PWR, 2500, and 2800 Switches.

Operating Rules for Source-Port Filters

- You can configure one source-port filter for each physical port or port trunk on the switch.
- Each source-port filter you configure is composed of:
 - One source port or port trunk (**trk1**, **trk2**, ...**trk6**)
 - A set of destination ports and/or port trunks that includes all LAN ports and port trunks on the switch
 - An action 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.

Configuring a Source-Port Filter

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

Syntax: [no] filter source-port [e] < source-port-number > [drop [forward] | forward [drop]]

Creates or deletes the source port filter assigned to < source-port-number >. If you create a source-port filter without specifying a drop or forward action, the switch automatically creates a filter with a forward action from the designated source to all destinations on the switch.

[drop [e] < destination-port-list >]

Configures the filter for the designated source-port (or source-trunk) (< source-port-number >) to drop traffic for the ports and/or port trunks in the < destination-port-list >. Can be followed by the **forward** option if you have other destination ports set to **drop** that you want to change to **forward**. For example:

```
filter source-port <source-port-number > drop < destination-port-list > forward  
< destination-port-list >
```

[forward [e] < destination-port-list >]

Configures the filter for the designated source (< source-port-number >) to forward traffic for the destinations 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 <source-port-number > forward < destination-port-list >  
drop < destination-port-list >
```

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:

```
HPswitch(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:

```
HPswitch(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 that 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:

```
HPswitch(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:

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

IDX	Filter Type	Value
1	Source Port	*5*

```
HPswitch(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 10-3. Example of Switch Response to Adding a Filtered Source Port to a Trunk

Viewing a Source-Port Filter

You can list all source-port filters configured in the switch and, optionally, the detailed information on a specific filter.

Syntax: show filter

Displays a listing of configured filters, where each filter entry includes an IDX (index) number, Filter Type, and Value :

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 (source-port) filter deletion created a gap in the filter listing.

Filter Type: Indicates the type of filter assigned to the IDX number.

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

Use **show filter** to learn the index number of a specific filter you want to examine in more detail.

[*index*]

Displays detailed data on the filter designated by the index number. For source-port filters, the display includes the source-port number, a listing of all ports and/or trunks on the switch (with their port types), and the filter action configured on each port or trunk (**Forward**—the default—or **Drop**).

For example, assume that these three filters exist on the switch:

Source Port	Destination Port(s)	Action
1	6-7	Drop; Forward on all other ports/trunks
2	8-9	Drop; Forward on all other ports/trunks
3	1-2	Drop; Forward on all other ports/trunks

If you wanted to determine the index number for the filter on source port 3 and then view a listing the filter details on source port 3, you would use the **show filter** and **show filter [INDEX]** commands, as shown in figure 10-4.

The screenshot shows two CLI sessions. The first session shows the output of the `show filter` command, which lists three filters with indices 1, 2, and 4. A callout box points to index 4, stating: "The show filter command lists the index number for source-port 3." The second session shows the output of the `show filter 4` command, which displays the details for filter 4, including its source port (3) and a table of destination ports and actions. A callout box points to the command, stating: "The show filter 4 command lists the details for the filter at source-port 3."

```
HPswitch(config)# show filter
Traffic/Security Filters
  IDX Filter Type | Value
-----+-----
  1 Source Port   | 1
  2 Source Port   | 2
  4 Source Port   | 3

HPswitch(config)# show filter 4
Traffic/Security Filters
Filter Type : Source Port
Source Port : 3
Dest Port Type | Action
-----+-----
  1      100/1000T | Drop
  2      100/1000T | Drop
  3      100/1000T | Forward
  4      100/1000T | Forward
  .
  .
  .
 23      100/1000T | Forward
 24      100/1000T | Forward
```

Figure 10-4. Example of Listing Filters and the Details of a Specific Filter

Filter Indexing

The switch automatically assigns each new source-port filter to the lowest-available index (IDX) number. 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.

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. 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 10-5. 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 10-5:

HPswitch(config)# show filter 1			HPswitch(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 10-5. Assigning Additional Destination Ports to an Existing Filter

— This page is intentionally unused. —