34 HRE-X Filtering

Overview

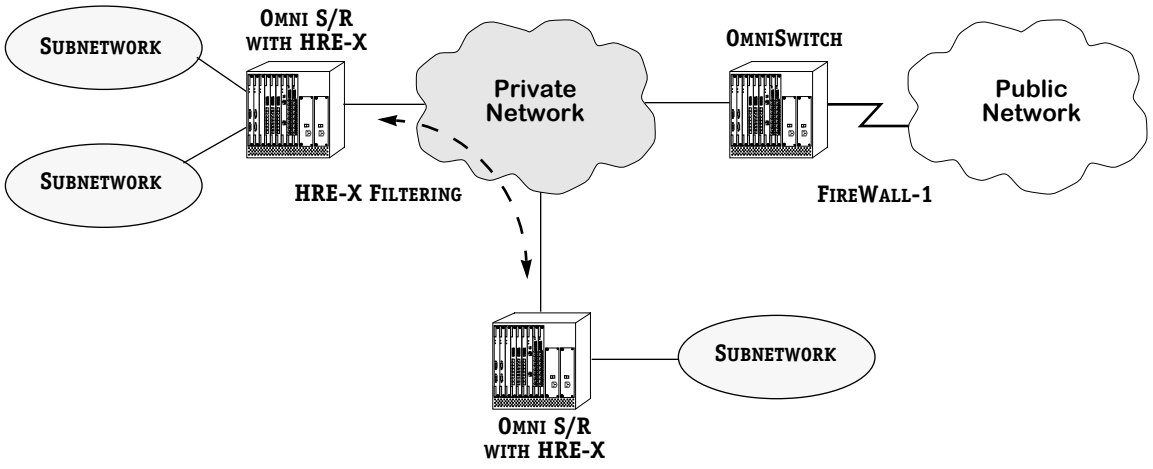
HRE-X filtering is a way of filtering network traffic by controlling whether or not routed packets are forwarded or blocked at the router interface. (This type of filtering is sometimes referred to as *access control lists.*) The feature requires an Omni Switch/Router (OmniS/R) with an HRE-X installed.

When a packet arrives on the switch, the switch examines layer 3 or layer 4 information in the protocol header to determine whether or not to forward the packet. Traffic is forwarded based on:

- IP source or destination address (layer 3)
- IPX destination network and node (layer 3)
- TCP destination port number (layer 4)

The switch checks its filtering database to match this information to a filtering rule. If a rule exists for the packet, then the rule is cached on the HRE-X and applied to the packet. Any additional traffic that comes into the switch with the same layer 3 or layer 4 information goes directly through the HRE-X. Because the feature is controlled largely by the HRE-X, filtering is done at wire speed; adding filtering lists or rules has minimal impact on performance.

HRE-X filtering lists provide moderate security inside internal networks, functioning like an internal firewall for LANs. The filtering lists complement the switch's IP Firewall feature, which provides a high level of protection from external networks over the WAN (see illustration below). For more details about the Firewall feature, see the *Switched Network Services User Manual.*



HRE-X Filtering Between Private Subnetworks

♦ Note ♦

The HRE-X filtering feature and the IP Firewall feature should not be configured on the same switch.

A list or group of filters (also called *rules*) may be created to be applied to an IP flow, an IPX flow, or flows with a particular TCP port number. If more than one rule exists for a packet, the most specific rule takes precedence. When no filtering rule exists for a packet, the HRE-X either allows or denies the packet based on a global configuration setting for the type of traffic (IP or IPX). The default is to allow both IP and IPX traffic; unlike the IP Firewall feature, HRE-X filtering allows by default all traffic that would normally pass through the switch. You must configure it explicitly if you want to deny particular traffic. The next section describes precedence in more detail.

Filtering Precedence

When multiple filters exist for the source/destination pair, the *most specific rule* will take precedence and be applied to the packet.

IP Rule Precedence

For IP traffic, precedence is determined by whether or not a TCP port number exists for the rule and what the granularity is of the IP source or destination address/mask.

- **TCP port number**—If a TCP port number exists for the rule, the rule will take precedence. The first rule in the examples below is the most specific rule because it contains a port number. TCP port numbers are well-known port numbers defined by the Internet Assigned Numbers Authority (IANA) for services like Telnet or FTP and various other services and applications.
- **IP address/mask combination**—The most specific address takes precedence. To calculate the most specific address, the switch uses an index based on the number of contiguous bits in the address mask that are set to zero. This index is called the *precision index*, and the calculation is made starting with the most significant bit in the mask (the leftmost bit). The lower the index value the more specific the address.

  In the example below, using the destination address, the masks of the first two entries have no bits set to zero so their index is 0, which is the most specific index. The first entry is more specific than the second entry because it also includes a port number. The less specific destination addresses both have an index of 8 because the first 8 bits of each mask are zero. The last entry is the least specific because its source address has an index of 32.

	Destination	Dest Mask	Source	Source Mask	Port
more specific	193.201.184.130	0xffffffff	193.201.181.0	0xffffff00	20
	193.201.184.130	0xffffffff	193.201.181.0	0xffffff00	
less specific	193.201.184.0	0xffffff00	193.201.181.0	0xffffff00	
	193.201.184.0	0xffffff00	0.0.0.0	0x00000000	

If the most specific rule for the destination address and the most specific rule for the source address have equal "specificity," by default the rule that applies to the *destination* address will be applied. You can configure the system so that the source address rule will take precedence instead.

IPX Rule Precedence

IPX packets are filtered only on destination address, from most specific to least specific as follows:

- **Full address**—Both the network and node values are specified in the rule
- **Node address**—Only the node value is specified in the rule
- **Network address**—Only the network value is specified in the rule
- **Global address**—Neither the network nor the node value is specified in the rule.

In the example here, the first address is a full address—it includes both the network and the node addresses. The node alone is a less specific address; the least specific is the network address without the node address.

	Network	Node
most specific	12345678	00:5A:4D:CC:22:11
	—	00:5A:4D:CC:22:11
least specific	12345678	—

Hardware/Software Requirements

HRE-X filtering is supported on the OmniS/R. An HRE-X must be installed on the MPX or on all network interface (NI) cards in order for HRE-X filtering to be executed on the switch. The HRE-X is a later-generation submodule that enables high-speed layer 3 IP and IPX routing; the filtering feature will not work with the HRE or HRE Plus. For more information about the HRE-X, see Chapter 1, "Omni Switch/Router Chassis and Power Supplies."

IP and/or IPX routing must be enabled on the switch. IP or IPX routing may be enabled when you create a group or VLAN and configure a virtual router port. For information about configuring groups and VLANs, see Chapter 25, "Managing Groups and Ports." For information about IP routing, see Chapter 31, "IP Routing." For information about IPX routing, see Chapter 33, "IPX Routing."

♦ Important Note♦

HRE-X filtering is compatible with routing protocols in the switch, including RIP, OSPF, and BGP4. If VRRP is loaded and running in the switch, all VRRP routers on the LAN must be configured with the same HRE-X rules; otherwise the security of the network will be compromised. For more information about VRRP, see the *Advanced Routing User Manual.*

HRE-X Filtering Configuration Overview

This section describes the broad steps necessary to set up filtering groups on the switch. The referenced commands are part of the User Interface (see *HRE-X Filtering UI* on page 34-5). HRE-X filtering may also be configured using the switch's Command Line Interface (CLI) or a Text-based Configuration file. See the *CLI Reference Manual* for more information about the CLI.

Step 1. Create Global Filtering Groups

Create global groups for IP and IPX flows by using the **fltipmod** command and the **ftipxmod** command respectively. Multiple groups may be created for each protocol. These commands are also used to add filtering rules to groups. Information about these commands is given in *IP Filtering Groups* on page 34-6 and *IPX Filtering Groups* on page 34-10.

The filtering configuration is set up so that you can configure filtering groups and rules and save them before actually committing the configuration to the HRE-X. Use the **fltd** command to review all saved groups and filters before activating them with the **fltcommit** command.

Step 2. Create Service Filtering Groups

A service filtering group is a group of configured IP groups that are applied to a particular TCP service such as Telnet or FTP. Use the **fltservice** command to configure a service filtering group and associate IP groups with it. See *Service Filtering Groups* on page 34-12 for more information about this command.

Step 3. Specify Groups and Services to be Active

Any group or service that you want to make active on the switch must be listed on the Modify Filtering Globals screen using the **fltcfg** command. See *Configuring Global Parameters* on page 34-15 for more information about this command.

Step 4. Activate Groups and Filters

Any configuration for groups and filters that you have configured may be activated by using the **fltcommit** command. Entering this command forces the switch to upload the current changes to the HRE-X. See *Activating Configuration Changes* on page 34-5 for more information about this command. Current saved changes may also be activated by rebooting the switch.

A list of currently active groups/filters may be displayed using the **fltactd** command. A list of all saved groups/filters may be displayed using the **fltd** command. See *Displaying Active Filters* on page 34-17 and *Displaying All Filters* on page 34-24 for information about these commands.

HRE-X Filtering UI

When filtering is loaded on the switch, it adds a submenu to the Networking menu of the User Interface (UI).

♦ Note ♦

For general information about the UI, see Chapter 8, "The User Interface."

To display the Filtering submenu, enter **filtering** at the system prompt.

If the UI is configured for terse mode, enter a **?** to display the submenu. In verbose mode the submenu automatically displays.

```
Command          Filtering Menu
---------------- ------------------------------------------------------------
fltactd          Display all active filters
fltactipd        Display active IP filters
fltactipxd       Display active IPX filters
fltactipq        Query disposition for an IP flow
fltactipxq       Query disposition for an IPX flow
fltcfg           Modify filtering globals
fltcommit        Commits configuration to HRE-X
fltd             Display all filtering groups
fltipd           Display IP filtering groups
fltipxd          Display IPX filtering groups
fltipchk         Find all filters that affect an IP address
fltipxchk        Find all filters that affect an IPX address
fltipmod         Add/modify IP filtering groups
fltipxmod        Add/modify IPX filtering groups
fltreadcfg       Read filtering configuration from a file
fltrm            Remove a filtering group from the configuration
fltrmall         Remove all filtering groups
fltrstcntrs      Reset the active filter utilization counters
fltservice       Add/modify filtering service groups

    Main      File      Summary  VLAN      Networking
    Interface Security  System   Services  Help
```

Commands are executed by typing the command and pressing **<Enter>**. On configuration screens, parameters may be changed by entering the number next to the relevant parameter, an equal sign, and the desired value at the prompt (for example, **1=ipgroup1**). After changes are made, enter **s** to save your changes or **q** to quit the screen.

Activating Configuration Changes

You can configure groups and filtering rules and edit them before actually activating them on the switch. Activating the changes means that the cache in the HRE-X is cleared and rules in the configuration file are rebuilt in the filtering database to include any changes saved through the **fltcfg**, **fltipmod**, **fltipxmod**, **fltrm**, **fltrmall**, or **fltservice** commands. *All traffic is dropped, and no learning takes place until the database is rebuilt.*

To activate the configuration changes, you can reboot the switch or use the **fltcommit** command. When you enter this command, a message similar to the following displays:

```
Are you sure you want to stop filtering
and restart the filtering configuration?: (n) :
```

Enter **y** to rebuild the filtering database with currently saved changes.

Creating Filtering Groups and Rules

This section describes how to set up HRE-X filtering groups and rules. IP groups and IPX groups are configured separately. Service filtering groups may be configured for any IP groups that are created. The filtering feature is set up so that groups may be created and edited before they are activated on the switch.

IP Filtering Groups

The **fltipmod** command is used to create IP filtering groups and to add address entries to those groups. When you create a new filtering group, you include at least one address rule for the group. To display the Modify IP Filtering Group screen, enter the following command:

```
fltipmod
```

The screen displays similar to the following:

```
Modify IP Filtering Group

1) Group                :
2) Primary Address:     Destination
    21) Destination Address: ALL
        211) Source Address   : ALL
        212) Allow or Deny    : Allow

Command {Item=Value/?/A/D/F/H/N/Q/-/+/R/S} (Redraw) :
```

To change any of these settings, enter the relevant item number, an equal sign, and the desired value. Any changes you save on this screen are not activated until the group is listed on the Modify Filtering Globals screen using the **fltcfg** command and the changes are uploaded to the HRE-X using the **fltcommit** command.

Fields on the screen are defined as follows:

Group

The name of the IP filtering group. Displays blank for a new group. An IP group consists of IP destination and source addresses. Each destination address may have multiple source addresses associated with it; each source address may have multiple destination addresses associated with it.

Primary Address

The type of address to which you want to add filtering rules. The default is **Destination**.

Destination (Source) Address

If the Primary Address is **Destination**, this field name is Destination Address. If the Specific Address is **Source**, this field name is Source Address. The default value is **ALL**. This field defines the specific address to which you may add source or destination addresses. The address mask is optional.

Source (Destination) Address

If the Primary Address is **Destination**, this field name is Source Address. If the Specific Address is **Source**, this field name is Destination Address. This field is used to add source or destination addresses to the specific address. The address mask is optional.

Allow or Deny

The disposition of the rule, to allow traffic that matches the rule or to deny it. The default is **Allow**.

Commands on this screen are not case-sensitive. They are defined as follows:

A	Adds a new address to the primary address
D	Deletes an address from the primary address
F	Finds the first rule for the indicated group. To use this command, enter an existing group name, for example **1=ip_group1**. Enter the **F** command, and the screen redisplays with the first rule in the group.
H	Displays help for the screen.
Q	Quits the screen and return to the system prompt.
–	Displays previous rule for this address.
+	Displays next rule for this address.
R	Redraws the screen.
S	Saves the changes; changes are not active until the next reboot or after the **fltcommit** command is entered.

Creating IP Filtering Groups

To create a new IP filtering group:

1. At the command prompt for the Modify IP Filtering Group screen, enter a unique group name. For example:

   1=group4

   The Primary Address is the type of address to which the rules will apply (there may be just one rule for the address). You can change the default (**Destination**) to **Source** by entering **2=s** at the command prompt. If you change the default, when the screen redisplays the field names change to correspond to the primary address.

2. Enter the relevant Destination Address (or Source Address) The address mask is optional. For example:

   21=193.201.184.39 ffffffff

   If you did not enter a mask, the system will include the natural mask of the address for you.

3. Enter the relevant Source Address (or Destination Address). The address mask is optional. For example:

   211=193.201.181.0

   If you did not enter a mask, the system will include the natural mask of the address for you.

4. Change the disposition for the rule, if desired, using **a** for allow or **d** for deny. For example:

```
212=d
```

Enter **s** at the command prompt to save the group and the address rule. To create another new group, enter **n** at the command prompt to return screen values to their defaults and start creating another IP group. To add more address rules to the group, see *Modifying IP Filtering Groups* on page 34-8.

Modifying IP Filtering Groups

To add rules to an IP filtering group, enter the **fltipmod** command with the group name. For example:

```
fltipmod group4
```

Or, if the Modify IP Filtering Group screen is already displayed, you can bring up the information for the group by entering **1=*<group name>***. For example:

```
1=group4
```

The screen redisplays with that group name, but other fields are not updated with the group's current information. To see current information for the group, enter **f** at the command line. The screen redisplays.

♦ Important Note ♦

If you do not display the group's current information, any information you enter and save for the existing group will overwrite the current information.

The screen display is similar to the following:

```
Modify IP Filtering Group

1) Group                 : group4
2) Primary Address:    Destination
   21) Destination Address: 193.201.184.39      ff.ff.ff.ff
      211) Source Address   :193.201.181.0       ff.ff.ff.00
      212) Allow or Deny      : Deny

Command {Item=Value/?/A/D/F/H/Q/-/+/R/S} (Redraw) :
```

Make any changes to the group and enter **s** to save your changes. Enter **q** to quit the screen. To activate a group, use the **fltcfg** command to list the group name on the Modify Filtering Globals screen and the **fltcommit** command to activate the configuration.

Adding Rules to IP Filtering Groups

To add another address to this group:

1. Enter **a** at the prompt of the Modify IP Filtering Group screen. The following message displays:

```
Add Destination or Source:
```

2. Enter **d** for destination or **s** for source. The screen redisplays with the appropriate field set to the default value (**All**).

3. Enter the address. Repeat these two steps to add more addresses to the filtering group.

4. Enter **s** at the command prompt to save the change(s).
5. Enter **q** to quit the screen. Use the **fltcommit** command to activate the new configuration.

IPX Filtering Groups

The **fltipxmod** command is used to create IPX filtering groups and to add address entries to those groups. When you create a new filtering group, you must include at least one address rule for the group. To display the Modify IPX Filtering Group screen, enter the following command:

```
fltipxmod
```

The screen displays similar to the following:

```
Modify IPX Filtering Group

1) Group                    :
2) Destination Network      : ALL
    21) Destination Node    : ALL
    22) Allow or Deny       : Allow

Command {Item=Value/?/A/D/F/H/Q/-/+/R/S} (Redraw) :
```

Fields are defined here:

Group. The group name is required to add a group. The name may be any alphanumeric string up to 30 characters.

Destination Network. By default this field is set to **ALL**, meaning that the group includes all IPX destination networks. Specify a particular destination network address by entering a valid 8-character address.

Destination Node. By default this field is set to **ALL**, meaning that the filtering rule applies to all nodes on the destination network. Specify a particular destination node by entering a valid 12-character address.

Allow or Deny. The disposition of the current rule. By default this field is set to **Allow**.

Commands on this screen are not case-sensitive. They are defined as follows:

A	Adds a new address to the specific address
D	Deletes an address from the specific address
F	Finds the first rule for the indicated group. To use this command, enter an existing group name, for example **1=ipx_group1**. Enter the **F** command, and the screen redisplays with the first rule in the group.
H	Displays help for the screen.
Q	Quits the screen and return to the system prompt.
–	Displays previous rule for this specific address.
+	Displays next rule for this specific address.
R	Redraws the screen.
S	Saves the changes; changes are not active until the next reboot or after the **fltcommit** command is entered.

Creating IPX Filtering Groups

To create a new IPX filtering group:

1. At the command prompt for the Modify IPX Filtering Group screen, enter a unique group name. For example:

   ```
   1=ipx_group1
   ```

   The screen redisplays with the group name you entered. By default, the destination network and destination node addresses are set to **ALL**.

2. To set the destination network address, enter any valid 8-character IPX destination address. For example:

   ```
   2=00001000
   ```

3. To set the destination node address, enter any valid node address (without the colons). For example:

   ```
   21=234567890000
   ```

   The screen redisplays as follows:

   ```
   Modify IPX Filtering Group

   1) Group                  : ipx_group
   2) Destination Network    : 00001000
      21) Destination Node     : 23:45:67:89:00:00
      22) Allow or Deny        : Allow

   Command {Item=Value/?/A/D/F/H/Q/-/+/R/S} (Redraw) :
   ```

4. To save the group, enter **s** at the command prompt. The group is saved to the configuration (but the rule or rules you enter are not yet active on the HRE-X).

5. To create another group, enter **n** at the command prompt. The screen redisplays with parameter defaults.

To activate a group, use the **fltcfg** command to list the group name on the Modify Filtering Globals screen and the **fltcommit** command to activate the configuration. See *Configuring Global Parameters* on page 34-15.

Modifying an IPX Filtering Group

To modify an existing IPX filtering group, enter the **fltipxd** command with the IPX group name. For example:

```
fltipxmod ipx_group
```

The screen displays similar to the following:

```
Modify IPX Filtering Group

1) Group                  : ipx_group
2) Destination Network    : 00001000
   21) Destination Node     : 23:45:67:89:00:00
   22) Allow or Deny        : Allow

Command {Item=Value/?/A/D/F/H/Q/-/+/R/S} (Redraw) :
```

Make any desired changes and then enter **s** at the command prompt to save your changes.

Adding a Rule to an IPX Group

To add another address to this group, enter **a** at the command prompt of the Modify IPX Filtering Group screen. The following message displays:

```
Add Network(T) or Node(D) :
```

Enter **t** to add a rule for a new network destination address or **d** to enter a rule for a new destination node. The screen redisplays with the appropriate field set to its default.

Enter the new address(es). Enter **s** at the command prompt to save the change.

Service Filtering Groups

Service groups are supersets of IP groups associated with a TCP destination port number. To configure a service filtering group, you create a name for the service, enter the relevant port number (as defined by the IANA), and associate the service with one or more IP groups.

To display the Configure Service Filtering Group screen, enter the **fltservice** command.

A screen similar to the following displays:

```
                Configure Service Filtering Group

1) Name        :
2) Number(s)   :
3) Groups      :

Command {Item=Value/?/F/H/N/Q/R/S} (Redraw) :
```

Fields on the screen are described here:

Name

The name of the service associated with the groups numbers to which you want to apply filters, for example FTP or Telnet.

Number(s)

The TCP port numbers that apply to the service. TCP port numbers are defined by the IANA. For example, port numbers for FTP are 20 and 21, and Telnet is 23.

Groups

The names of filtering groups that should be applied to any traffic with the specified destination port numbers. Groups are configured using the **fltipmod** command and must already be created to be listed here.

Commands on the screen are defined here:

F	Finds the current information for the specified service. To use this command, enter an existing service group name, for example **1=ftp**. Enter the **F** command, and the screen redisplays with the information configured for that service.
H	Displays help for the screen.
N	Returns screen values to their defaults (blank); use this command to configure a new service.
Q	Quits the screen and returns to the system prompt.
R	Redraws the screen.
S	Saves the changes; changes are not active until the next reboot or after the **fltcommit** command is entered.

Creating a Service Filtering Group

To create a service filtering group:

1. On the Configure Service Filtering Group screen, enter the service group name. For example:

   1=ftp_group

2. Enter the relevant TCP service number(s). When entering multiple numbers, include a space between them. For example:

   2=20 21

3. Enter the name of the existing IP filtering group(s) that the service group will be a part of. (IP filtering groups are created using the **fltipmod** command.) For example:

   3=ipgroup1 ipgroup2

4. Enter **s** to save the change. To create another service filtering group, enter **n** to return all fields to the defaults (blank) and follow steps 1 through 3 again. The group or groups are saved to the configuration but are not yet active on the HRE-X.

5. Enter **q** to quit the screen.

To activate a service filtering group, use the **fltcfg** command to list the group name on the Modify Filtering Globals screen and the **fltcommit** command to activate the configuration. See *Configuring Global Parameters* on page 34-15.

Modifying a Service Filtering Group

Enter the **fltservice** command with the name of the service group. For example:

```
fltservice ftp_group
```

Or, if the Configure Service Filtering Group screen is already displayed and you want to modify a different group, enter **1=<service group name>**. For example:

```
1=ftp_group
```

The screen displays with the group name, but the other fields are not updated with current information for the group. To display current information for the group, enter **f** at the command prompt.

♦ Important Note ♦

If you do not display the group's current information, any information you enter and save for the existing group will overwrite the current information.

The Configure Service Filtering Group screen displays for the relevant service.

```
Configure Service Filtering Group

1) Name         : ftp_group
2) Number(s)    : 20 21
3) Groups       : group1

Command {Item=Value/?/F/H/N/Q/R/S} (Redraw) :
```

If you want to delete numbers or groups from the service filtering group, enter the number of the relevant parameter, an equal sign, and the numbers or groups that should be included. To remove all numbers or groups, leave the value blank. In the example screen above, to remove port number 20, enter the following:

```
2=21
```

After making changes, enter **s** at the command prompt to save your changes. Use the **fltcommit** command to activate the change(s).

Configuring Global Parameters

Global HRE-X filtering settings are configured on the Modify Filtering Globals screen. Any changes you make on this screen will be active after the next reboot or when you enter the **fltcommit** command. Any filtering groups that you want to activate must be listed on this screen.

To modify global filtering parameters, enter the following command:

```
fltcfg
```

A screen similar to the following displays:

```
                    Modify Filtering Globals

1) Administrative Enable (Enable or Disable)   : Enabled
2) Default IP Rule (Allow or Deny)             : Allow
3) Default IPX Rule (Allow or Deny)            : Allow
4) Precedence (Source or Destination)          : Destination
5) Global Groups                               :
6) Services                                    :

Command {Item=Value/?/Quit/Redraw/Save} (Redraw) :
```

To change any of these settings, enter the relevant item number, an equal sign, and the desired value. When you are finished, enter **s** to save the changes. Enter **q** to quit the screen and return to the system prompt. Use the **fltcommit** command to activate the changes.

Fields on this screen are defined as follows:

Administrative Enable (Enable or Disable)

Determines whether or not HRE-X filtering will be enabled at the next reboot or when the **fltcommit** command is entered. The default is **Enabled**. To change this value, enter **1=d** for disabled or **1=e** for enabled.

Default IP Rule (Allow or Deny)

Determines the disposition for IP traffic when no filtering rules are configured for the flow. The default is **Allow**. If you set this parameter to **Deny**, any IP packets without filtering rules are discarded. To change this value, enter **2=d** for deny or **2=a** for allow.

Default IPX Rule (Allow or Deny)

Determines the disposition for IPX traffic when no filtering rules are configured for the flow. The default is **Allow**. If you set this parameter to **Deny**, any IPX packets without filtering rules are discarded. To change this value, enter **3=d** for deny or **3=a** for allow

Precedence (Source or Destination)

If there is a conflict between a rule for an IP source address and a rule for an IP destination address, this parameter determines which rule will be applied. The default is **Destination**. To change this value, enter **4=s** for source or **4=d** for destination. (IPX traffic is always filtered on destination address. The setting of this parameter does not apply to IPX traffic.)

Global Groups

Determines which IP or IPX groups will be active at the next reboot or when the **fltcommit** command is entered. Global groups must first be configured using the **fltipmod** or the **fltipx-mod** commands for IP or IPX traffic respectively before you can enter the group names here. These groups do not include service filtering groups.

Services

Determines which IP service filtering groups will be active at the next reboot or when the **fltcommit** command is entered. Service filtering groups apply to a particular TCP port for IP traffic and are configured using the **fltservice** command. The groups must be configured first before you can enter them here.

Activating Filtering Groups

To activate filtering groups on the switch:

1. At the command line on the Modify Filtering Globals screen, enter the relevant item number for global groups or service groups, an equal sign, and valid group name(s). For multiple groups, separate group names with a space. For example:

   ```
   5=ip_group1 ip_group2
   ```

2. The Modify Filtering Globals screen redisplays with the group name(s).
3. Enter **s** to save the configuration.
4. Enter **q** to quit the screen and return to the system prompt.
5. Enter the **fltcommit** command to make the groups active.

Deactivating Filtering Groups

To deactivate filtering groups on the switch:

1. At the command line on the Modify Filtering Globals screen, enter the relevant item number, an equal sign, and any group name(s) you want to keep active. For multiple groups, separate group names with a space. To remove all global groups or all service groups, leave the value blank. For example:

   ```
   6=
   ```

2. The Modify Filtering Globals screen redisplays with the group name(s) removed.
3. Enter **s** to save the configuration.
4. Enter **q** to quit the screen and return to the system prompt.
5. Enter the **fltcommit** command to deactivate the group(s).

Displaying Filters

All currently saved and active filters on the switch may be displayed. The displays may be sorted by protocol type (IP or IPX). You can also display the disposition of any active rule (allow or deny) for a particular flow. The counters for active rules may also be reset.

Displaying Active Filters

All active filters may be displayed for both global IP and IPX groups and service IP groups. Active filters are those that have been configured using the **fltipmod**, **fltipxmod**, and **fltservice** commands and activated using the **fltcommit** command. You can also display active filters for IP addresses only or active filters for IPX addresses only as described in the next sections. See *Displaying All Filters* on page 34-24 to display all filters, including filters that have been saved but not activated yet.

To display all active filters, enter the following command:

```
fltactd
```

A screen similar to the following displays:

```
Active Filtering Rules
======================
Filter Admin State: ENABLED
Filter Init State: ACTIVE

Active IP Filters
==============
Default: ALLOW, Precedence: DESTINATION

GLOBAL
-------------
IP Group Name
ID#    Destination      Dest Mask       Source              Src Mask       A/D      Count
-------------------------------------------------------------------------------------------------------------------
group1
   0   193.201.184.0    ff.ff.ff.0    ******ALL******     ***********    ALLOW        0
   1       199.0.0.0     ff.0.0.0     ******ALL******     ***********    DENY         0
group2
   2       129.3.4.5    ff.ff.ff.ff       129.6.0.0         ff.ff.0.0    DENY         0
   3       129.4.0.0     ff.ff.0.0        129.3.0.0         ff.ff.0.0    DENY         0


SERVICE: ftp PORTS: 20, 21
------------------------------------------
IP Group Name
ID#    Destination      Dest Mask       Source              Src Mask       A/D      Count
-------------------------------------------------------------------------------------------------------------------
group3
   4   193.201.185.0    ff.ff.ff.0    193.201.184.0         ff.ff.ff.0    ALLOW        0
```

(continued)

```
Active IPX Filters
==================
Default: DENY

Full Address Rules
------------------------------
IPX Group Name
    ID#       Network          Node                  A/D       Count
-------------------------------------------------------------------------------------------
ipxgroup1
        0     00001000     23:45:67:89:00:00     ALLOW          0
        1     00001000     09:87:65:43:21:09     DENY           0
ipxgroup2
        2     22220000     67:89:01:AA:BB:CC     DENY           0


Network Rules
---------------------
IPX Group Name
    ID#       Network          Node                  A/D       Count
-------------------------------------------------------------------------------------------
ipxgroup2
        0     22220000     *******ALL*******     DENY           0


Global Rule
--------------------
IPX Group Name
-------------------------------------------------------------------------------------------
ipxgroup2
        0     **ALL**      *******ALL*******     ALLOW          2
```

General fields at the top of the screen for Active Filtering Rules are defined here. Fields for the IP display and the IPX display are explained in the next sections respectively.

Filter Admin State. Displays the current administrative filtering state (**ENABLED** or **DISABLED**), which was activated at the last reboot or when the **fltcommit** command was entered. Filtering is enabled or disabled through the **fltcfg** command.

Filter Init State. Displays the current operational state of the filtering database (**ACTIVE** or **INACTIVE**).

Displaying Active IP Filters

Active global IP groups and service IP groups may be displayed using the **fltactipd** command. The screen display is similar to the following:

```
Active IP Filters
==========
Default: ALLOW, Precedence: DESTINATION

GLOBAL
----------
IP Group Name
ID#    Destination      Dest Mask       Source            Src Mask       A/D      Count
-------------------------------------------------------------------------------------------------------------------
group1
   0   193.201.184.0    ff.ff.ff.0    ******ALL******     **********     ALLOW      0
   1       199.0.0.0     ff.0.0.0     ******ALL******     **********     DENY       0
   2       200.0.0.0     ff.0.0.0     ******ALL******     **********     DENY       0
group2
   3       129.3.4.5    ff.ff.ff.ff       129.6.0.0        ff.ff.0.0     DENY       0
   4       129.4.0.0     ff.ff.0.0        129.3.0.0        ff.ff.0.0     DENY       0
   5       129.4.0.0     ff.ff.0.0        129.3.4.6       ff.ff.ff.ff    ALLOW      0
group3
   6   193.201.185.0    ff.ff.ff.0    193.201.184.0       ff.ff.ff.0     ALLOW      0
   7   193.201.181.0    ff.ff.ff.0    193.201.184.0       ff.ff.ff.0     DENY       0
   8   193.201.185.0    ff.ff.ff.0        198.0.0.0        ff.0.0.0      ALLOW      0

SERVICE: ftp PORTS: 20, 21
----------------------------------------
IP Group Name
ID#    Destination      Dest Mask       Source            Src Mask       A/D      Count
-------------------------------------------------------------------------------------------------------------------
group1
   0   193.201.184.0    ff.ff.ff.0    ******ALL******     **********     ALLOW      0
   1       199.0.0.0     ff.0.0.0     ******ALL******     **********     DENY       0
   2       200.0.0.0     ff.0.0.0     ******ALL******     **********     DENY       0
group2
   3       129.3.4.5    ff.ff.ff.ff       129.6.0.0        ff.ff.0.0     DENY       0
   4       129.4.0.0     ff.ff.0.0        129.3.0.0        ff.ff.0.0     DENY       0
   5       129.4.0.0     ff.ff.0.0        129.3.4.6       ff.ff.ff.ff    ALLOW      0
```

Fields are defined as follows:

IP Group Name. The name of a group with IP rules.

ID#. The unique rule ID assigned by the switch for each active filtering rule configured for the protocol.

Destination. The destination IP address.

Dest Mask. The mask identifying which bits in the destination IP address are significant.

Source. The source IP address.

Src Mask. The mask identifying which bits in the source IP address are significant.

A/D. The disposition of packets matching this rule (**ALLOW** or **DENY**).

Count. The number of packets that have arrived on the switch and matched this rule.

Displaying Active IPX Filters

To display all active filters for IPX addresses only, enter the following command:

```
fltactipxd
```

The screen displays similar to the following:

```
Active IPX Filters
==================
Default: DENY

Full Address Rules
--------------------------
IPX Group Name
    ID#       Network          Node                  A/D       Count
-------------------------------------------------------------------------------------------
ipxgroup1
        0     00001000     23:45:67:89:00:00     ALLOW          0
        1     00001000     09:87:65:43:21:09     DENY           0
ipxgroup2
        2     22220000     67:89:01:AA:BB:CC     DENY           0

Network Rules
---------------------
IPX Group Name
    ID#       Network          Node                  A/D       Count
-------------------------------------------------------------------------------------------
ipxgroup2
        0     22220000     *******ALL*******     DENY           0

Global Rule
------------------
IPX Group Name
-------------------------------------------------------------------------------------------
ipxgroup2
        0     **ALL**      *******ALL*******     ALLOW          2
```

Fields are defined as follows:

IPX Group Name. The name of a group of IPX rules.

ID#. A unique ID assigned by the switch for each active rule configured for the protocol.

Network. The destination IPX network number.

Node. The destination IPX node.

A/D. The disposition of packets matching this rule (**ALLOW** or **DENY**).

Count. The number of packets that have arrived on the switch and matched this rule.

Displaying the Disposition for Particular Flows

The disposition of a filtering rule is whether to deny or allow the flow it specifies. You can display the disposition for a particular IP source/destination address pair or an IPX destination address. You can also display more details about the address. For IP, these details include the rule ID and the precision index for each rule for both the source and the destination addresses. For IPX, these details include the rules and their disposition for the node address and the network address.

Disposition for IP Flows

Using the **fltactipq** command you can display whether or not a particular IP source and destination address pair is accepted on the switch, and what filtering rule, if any, applies to the flow. (The filtering rule must be active on the switch.) The display may be more detailed to include the rules that apply to the source address and destination address respectively.

The command syntax is as follows:

fltactipq [v] ***destination-address source-address [port number]***

where

- v — (optional) indicates verbose output for the command
- *destination-address*—the destination IP address in dotted decimal notation
- *source-address*—the source IP address in dotted decimal notation
- *port number*—(optional) indicates the TCP port number. If no number is supplied, or you specify zero, only global rules are checked; if a port number is specified, all rules for the port number and all global rules are checked.

For example, if you enter

```
fltactipq 193.201.184.33  193.201.185.12 0
```

A message similar to the follow displays, depending on the rules you have configured:

```
IP flow (dest 193.201.184.23, src 193.201.185.12) is DENIED; GLOBAL rule #4.
```

To display more information about the destination and source addresses, enter the **v** option with the command. For example:

```
fltactipq v 193.201.184.33  193.201.185.12 0
```

A screen similar to the following displays, depending on the rules you have configured:

```
IP Filter Check
=============

GLOBAL
------------
   Destination: 193.201.184.23
   -----------------------------------
   precision 32, rules 4
   precision 8, rules 0

   Source: 193.201.185.12
   -----------------------------------
   precision 32, rules 0,1, 2, 3,7
   precision 24, rules 15, 16, 17
   precision 8, rules 4, 5, 6

IP flow (dest 193.201.184.23, src 193.201.185.12) is DENIED; GLOBAL rule #4.
```

The **precision** value corresponds to the precision index calculated by the switch (see *IP Rule Precedence* on page 34-2). The lower the value the more precise the rule. The rule values correspond to the rule index numbers on the Active Filtering Rules screen displayed using the **fltactd** or **fltactipd** command.

Disposition for IPX Flows

Use the **fltactipxq** command to display the disposition for a particular IPX address and what filtering rule, if any, applies to the flow. (The filtering rule must be active on the switch.) The screen may be more detailed to display the full address, node address, or network address rules.

The command syntax is as follows:

```
fltactipxq [v] destination-network destination-node
```

where

- v—(optional) indicates verbose output for the command
- *destination-network*—the network address in hexadecimal
- *destination-node*—the node address in hexadecimal

For example, if you enter:

```
fltactipxq 12345678   aa:bb:cc:dd:ee:11
```

A message similar to the following displays:

```
IPX flow (12345678, AA:BB:CC:DD:EE:11) is DENIED; FULL ADDR ruleid #4.
```

To display more information about this flow, include the **v** option with the command. For example:

```
fltactipxq v 12345678 aa:bb:cc:dd:ee:11
```

The screen display is similar to the following:

```
IPX Filter Check
===============
   Full Address Rules
   ------------------------------
   rule #4 applies; DENIED

   Node Rules
   -----------------
   no rule applies

   Network Rules
   ----------------------
   rule #0 applies; ALLOWED

   Global Rule
   -----------------
   no rule applies

IPX flow (12345678, AA:BB:CC:DD:EE:11) is DENIED; FULL ADDR ruleid #4.
```

Resetting the Counters

To reset the counters for all active filters, use the **fltrstcntrs** command. The Count field on all active displays (from the **fltactd**, **fltactipd**, and **fltactipxd** commands) is set to zero.

Displaying All Filters

You can display filtering rules for all IP and IPX filtering groups, regardless of whether they are active (cached on the HRE-X) or not. You can also display rules for a particular IP or IPX address as described in the next sections.

To display all filters (active and not-yet-active), enter the following command.

```
fltd
```

The screen display is similar to the one shown here.

```
Default IP rule: ALLOW
IP Group Name
     Destination     Dest Mask          Source             Source Mask          A/D
-------------------------------------------------------------------------------------------------------------------
group 3
  193.201.185.0   - ff.ff.ff.0       193.201.184.0      - ff.ff.ff.0         ALLOW
  193.201.181.0   - ff.ff.ff.ff                                              DENY

group 2
  129.3.4.5       -ff.ff.ff.ff       ***ALL***          - ******************  ALLOW
                                     129.4.0.0          - ff.ff.0.0          DENY
                                     129.5.0.0          - ff.ff.0.0          DENY
                                     129.6.0.0          - ff.ff.0.0.         DENY

  129.4.0.0       - ff.ff.0.0        129.3.0.0          - ff.ff.0.0          DENY
                                     129.3.4.6          - ff.ff.ff.ff        ALLOW
group 1
  193.201.184.0.  - ff.ff.ff.0       ***ALL***          - ******************  ALLOW
  199.0.0.0       - ff.0.0.0                                                 DENY
  200.0.0.0       - ff.0.0.0                                                 DENY

  ***ALL***       - ****************  193.201.185.0      - ff.ff.ff.0         DENY
  193.201.181.0   - ff.ff.ff.0                                               ALLOW


Default IPX rule: ALLOW
IPX Group Name
          Network       Node                  A/D
-----------------------------------------------------------------------
group4
          000001000     23:45:67:89:00:00     ALLOW
                        09:87:65:43:21:09     DENY

          22220000      67:89:01:23:45:67     DENY
                        34:56:65:43:34:56     DENY
                        34:56:55:44:55:56     DENY
                        34:56:65:43:34:56     ALLOW

          ***ALL***     67:89:01:23:45:67     DENY
                        34:56:65:43:34:56     ALLOW
```

Fields in this display are configured using the **fltipmod** and **fltipxmod** commands described in *IP Filtering Groups* on page 34-6 and *IPX Filtering Groups* on page 34-10. They are defined as follows:

IP Group Name. The name of a group with IP rules.

Destination. The destination IP address.

Dest Mask. The mask identifying which bits in the destination IP address are significant.

Source. The source IP address.

Source Mask. The mask identifying which bits in the source IP address are significant.

A/D. The disposition of packets matching this rule (**ALLOW** or **DENY**).

IPX Group Name. The name of a group of IPX rules.

Network. The destination IPX network number.

Node. The destination IPX node.

A/D. The disposition of packets matching this rule (**ALLOW** or **DENY**).

Displaying IP Filtering Groups

To display filtering rules for *all* IP filtering groups, enter the following command:

```
fltipd
```

A screen similar to the following displays:

```
Default IP rule: ALLOW
IP Group Name
     Destination     Dest Mask          Source            Source Mask          A/D
-------------------------------------------------------------------------------------------------------
group 3
  193.201.185.0   - ff.ff.ff.0       193.201.184.0     - ff.ff.ff.0         ALLOW
  193.201.181.0   - ff.ff.ff.ff                                             DENY

  193.201.184.0   - ff.ff.ff.0       198.0.0.0         - ff.0.0.0           DENY
  193.201.185.0   - ff.ff.ff.0                                              ALLOW
  193.201.186.0   - ff.ff.ff.0                                              DENY
  193.201.187.0   - ff.ff.ff.0                                              ALLOW

group 2
  129.3.4.5       -ff.ff.ff.ff       ***ALL***         - ******************  ALLOW
                                     129.4.0.0         - ff.ff.0.0          DENY
                                     129.5.0.0         - ff.ff.0.0          DENY
                                     129.6.0.0         - ff.ff.0.0.         DENY

  129.4.0.0       - ff.ff.0.0        129.3.0.0         - ff.ff.0.0          DENY
                                     129.3.4.6         - ff.ff.ff.ff        ALLOW
group 1
  193.201.184.0.  - ff.ff.ff.0       ***ALL***         - ******************  ALLOW
  199.0.0.0       - ff.0.0.0                                                DENY
  200.0.0.0       - ff.0.0.0                                                DENY
  201.0.0.0       - ff.0.0.0                                                DENY

  ***ALL***       - ****************  193.201.185.0     - ff.ff.ff.0         DENY
  193.201.181.0   - ff.ff.ff.0                                              ALLOW
```

To display filtering rules for *a particular IP address*, enter the **fltipchk** command with the relevant IP address. For example:

```
fltipchk 193.201.184.0
```

A screen similar to the following displays:

```
Name
Destination      Destination Mask          Source          Source Mask       A/D
-------------------------------------------------------------------------------------------------------------------
group3                IP    Primary Address
  193.201.184.0    ff.ff.ff.0
group3                IP    Primary Address
       198.0.0.0     ff.00.00.00
group2                IP    Secondary Address
       129.3.4.5     ff.ff.ff.ff          ****ALL****      **********       ALLOW
group1                IP    Primary Address
     ****ALL****    **********
group1                IP    Secondary Address
     ****ALL****    **********          193.201.185.0    ff.ff.ff.00       DENY
```

All the rules that apply to the address are displayed. *Primary* indicates that the address was used to add rules to; *secondary* indicates that the address was added as a rule to the displayed address. Fields are described in *Displaying All Filters* on page 34-24.

Displaying IPX Filtering Groups

To display filtering rules for *all* IPX groups, enter the following command:

```
fltipxd
```

A screen similar to the following displays:

```
Default IPX rule: ALLOW
IPX Group Name
          Network      Node                  A/D
-------------------------------------------------------------------
group4
          000001000    23:45:67:89:00:00     ALLOW
                       09:87:65:43:21:09     DENY

          22220000     67:89:01:23:45:67     DENY
                       34:56:65:43:34:56     DENY
                       34:56:55:44:55:56     DENY
                       34:56:65:43:34:56     ALLOW

          ***ALL***    67:89:01:23:45:67     DENY
                       34:56:65:43:34:56     ALLOW
```

To display filtering rules for *a particular IPX address*, enter the **fltipxchk** command with the relevant IPX address. For example:

```
fltipxchk 00001000
```

The screen displays similar to the following:

```
Name     Network      Node Number          A/D
-----------------------------------------------------------------------------------------------
group4   00001000     23:45:89:00:00       ALLOW
```

Fields are described in *Displaying All Filters* on page 34-24.

Displaying Service Groups

The **fltd** command may also be used to display all saved service groups (active and not-yet-active) only.

To display filters for TCP ports, enter the following command:

```
fltd services
```

A screen similar to the following displays:

```
Name            Port        Group
-------------------------------------------------------------------------------
port3            623        group4
                 634
                 645

port2            423        group12
                 434        group22
                 445        group32
                 456

port1             23        group1
                  34        group2
                  45        group3
                  56
```

Fields in this display are configured using the **fltservice** command described in *Service Filtering Groups* on page 34-12. They are defined as follows:

Name. The name of the service associated with the group numbers to which filters apply.

Port. The TCP port numbers that apply to the service.

Group. The names of the filtering groups that should be applied to any traffic with the specified destination port numbers.

Configuring a List of Filtering Rules

Instead of configuring filtering rules individually, you may want to create a file that contains all the rules and then load that file into switch memory. The file may be created using UI commands in the Edit menu (see Chapter 11, "Managing Files") or offline using any ASCII editor.

To read a list of filtering rules into the switch through the UI, use the **fltreadcfg** command. This command is useful if you *are not* using the Text-Based Configuration Command Line Interface (CLI) feature in the switch. The Text-Based Configuration CLI may be used for uploading files that contain commands for filtering rules as well commands for many other functions in the switch. For more information about text-based configuration, see the *Text-Based Configuration CLI Reference Guide*.

♦ Note ♦

Only filtering commands should be used in the text file that will be read into the switch using the **fltreadcfg** command. Other CLI commands should not be included in the file.

The syntax of commands in the file is the same as for HRE-X filtering commands used in the Text-Based Configuration CLI. For more information about the construction of the syntax, see the *Text-Based Configuration CLI Reference Guide*. Part of a sample file is shown here:

```
filter group group1 source ip
filter rule group1 all 199.206.184.1/255.0.0.0 deny
filter rule group1 all 199.206.184.1/255.255.0.0 deny
filter rule group1 all 199.206.184.1/255.255.255.0 deny
filter rule group1 all 199.206.184.1/255.255.255.255 allow
filter rule group1 all 199.206.184.1 allow
filter rule group1 all 199.206.184.0 allow
filter rule group1 all 10.206.184.1/255.0.0.0 deny
filter rule group1 all 10.206.184.1/255.255.0.0 deny
filter rule group1 all 10.206.184.1/255.255.255.0 deny
filter rule group1 all 10.206.184.1/255.255.255.255 allow
.
.
.
.
```

To read the file into the switch, enter the **fltreadcfg** command with the filename. For example:

```
fltreadcfg fltlist2
```

A message displays similar to the following:

```
Reading filter file: fltlist2 ......Complete
```

Removing Filtering Groups and Services

To remove groups or services from the configuration, use the **fltrm** command. Removing a group or service deletes it from the configuration. You can also use this command to remove groups from a service or to delete all groups and services from the configuration. The following sections describe how to use the command.

After removing groups and/or services, use the **fltcommit** command to activate the changes. See *Activating Configuration Changes* on page 34-5 for more information about the **fltcommit** command.

To deactivate groups or services, rather than delete them, use the **fltcfg** command. See *Configuring Global Parameters* on page 34-15.

Deleting an IP or IPX Group

To delete an IP or IPX group, enter the **fltrm** command with the group name. For example:

```
fltrm group4
```

A message displays similar to the following:

```
Do you want to remove group4 (n):
```

Enter **y** to remove the group from the configuration. The group will be deleted at the next reboot or when the **fltcommit** command is entered.

Deleting a Service

To delete a service from the configuration, enter the **fltrm** command with the service name. For example:

```
fltrm ftp
```

A message displays similar to the following:

```
Do you want to remove service ftp? (n):
```

Enter **y** to remove the service from the configuration. The service will be deleted at the next reboot or when the **fltcommit** command is entered. Note that the associated IP groups are not deleted from the configuration; only the service is deleted.

Removing a Group From a Service

To remove an IP group from a service, enter the service name and the relevant group name. For example:

```
fltrm ftp group1
```

The group will be removed at the next reboot or when the **fltcommit** command is entered. Note that the IP group is removed from the service, but the group is not deleted from the configuration.

Deleting All Group, Service, and Global Configuration

To remove all filtering groups at once, enter the following command:

```
fltrmall
```

A message displays similar to the following:

```
Remove all Filters? (n):
```

Enter **y** to remove all filters from the configuration. All groups and services will be deleted at the next reboot or when the **fltcommit** command is entered.