Packet Processing Thresholds

Packet Processing Thresholds

Threshold monitoring can be enabled for the packet processing values described in the following table.

Value	Description
Packets filtered/dropped	Enables the generation of alerts or alarms based on the total number of packets that were filtered or dropped based on ACL rules during the polling interval.
Packets forwarded	Enables the generation of alerts or alarms based on the total number of packets that were forwarded to the CPU during the polling interval.

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Filtered/Dropped Packet Thresholds

Filtered/dropped packet thresholds generate alerts or alarms based on the total number of packets that were filtered or dropped by the system as a result of ACL rules during the specified polling interval.

Alerts or alarms are triggered for filtered/dropped packets based on the following rules:

- **Enter condition:** Actual number of filtered/dropped packets > or = High Threshold

- **Clear condition:** Actual number of filtered/dropped packets < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Note These instructions assume that ACLs have been previously configured.

Configuring Filtered/Dropped Packet Thresholds

Use the following example to configure the filtered/dropped packet thresholds:

```
configure
 threshold packets-filtered-dropped  <high_thresh> [ clear <low_thresh>]
 threshold poll packets-filtered-dropped interval <time>
 threshold monitoring packets-filtered-dropped
      end
```

Forwarded Packet Thresholds

Forwarded packet thresholds generate alerts or alarms based on the total number of packets that were forwarded to active system CPU(s) during the specified polling interval. Packets are forwarded to active system CPUs when the NPUs do not have adequate information to properly route them.

Note Ping and/or traceroute packets are intentionally forwarded to system CPUs for processing. These packet types are included in the packet count for this threshold.

Alerts or alarms are triggered for forwarded packets based on the following rules:

- **Enter condition:** Actual number of forwarded packets > or = High Threshold
- **Clear condition:** Actual number of forwarded packets < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Configuring Forwarded Packet Thresholds

Use the following example to configure the forwarded packet thresholds:

```
configure
 threshold packets-forwarded-to-cpu  <high_thresh> [ clear <low_thresh> ]
 threshold poll packets-forwarded-to-cpu interval <time>
 threshold monitoring packets-forwarded-to-cpu
      end
```