Overview

The CPU protection feature enhances the efficiency of an HP device's CPU and Content Addressable Memory (CAM).

Some denial of service attacks make use of spoofed IP addresses. If the device must create CAM entries for a large number of spoofed IP addresses over a short period of time, it requires excessive CAM utilization. Similarly, if an improperly configured host on the network sends out a large number of packets that are normally processed by the CPU (for example, DNS requests), it requires excessive CPU utilization.

The CPU protection feature allows you to configure the HP device to automatically take actions when thresholds related to high CPU or CAM usage are exceeded.

NOTE: The CPU protection feature is supported on the following devices, starting with software release 07.7.00:
- 9300 series Routing Switches with Standard or EP management modules

The CPU protection feature is disabled by default.

How the CPU Protection Feature Works

The CPU protection feature uses the concepts of normal mode and exhausted mode. The device transitions from normal mode to exhausted mode when specified thresholds for conditions related to high CPU usage and CAM usage are exceeded. When the device enters exhausted mode, actions can be taken to reduce the strain on system resources. You can define the conditions that cause the device to enter exhausted mode, the actions to take while the device is in exhausted mode, and the conditions that enable the device to go back to normal mode.

For example, you can specify that a CPU usage percentage of 90% is a condition that will cause the device to go from normal mode to exhausted mode. When the device enters exhausted mode, you can specify that the action to take is to forward unknown unicast traffic in hardware instead of sending it to the CPU. You can further specify that a CPU usage percentage of 80% will cause the device to go back to normal mode.

Conditions

You can define thresholds for the following conditions:
- CPU utilization percentage
- Layer 2, Layer 3, and Layer 4 CAM usage percentage

For each of these conditions, you can define two threshold values, a declaring watermark and a clearing watermark. When the device is in normal mode, and a condition surpasses its declaring watermark, the device...
enters exhausted mode. When the device is in exhausted mode, and the condition drops below the clearing watermark, the device goes back into normal mode.

**Actions**

When the declaring watermark defined for a condition has been exceeded, the device enters exhausted mode. When the device is in exhausted mode, the following actions can be taken:

- **Dynamic aging adjustment control** – If dynamic aging adjustment control is specified as an action, when the system enters exhausted mode, the age limit value for CAM entries is dynamically changed to a smaller value, decreasing from 70 seconds to 35 seconds. When the system re-enters normal mode, the age limit value for CAM entries goes back to 70 seconds. Dynamic aging adjustment control is supported on both Standard or Standard (non-EP) and EP devices.

- **Unknown unicast flooding/dropping** – You can configure the device to perform hardware flooding or dropping of unknown unicast packets when it enters exhausted mode. Packets with unknown unicast destination addresses can be either dropped or flooded by hardware to all ports in the VLAN. The unknown unicast flooding/dropping action is supported on EP devices only.

- **Multicast/broadcast flooding/dropping** – You can configure the system to drop or perform hardware flooding for multicast or broadcast packets, instead of sending them to the CPU. The multicast/broadcast flooding/dropping action is supported on EP devices only.

The hardware flooding actions are not applicable in every configuration, since under certain circumstances the device needs to send packets to the CPU for processing. For example, if a port on a Routing Switch has an IP address configured, hardware flooding will not be enabled, so that ARP packets can be sent to the CPU.

Hardware flooding will not be applied on the following kinds of VLANs:

- Layer 2 control VLAN (VLAN ID 4094)
- Management VLAN
- Protocol VLAN
- Private VLAN

On a Routing Switch, hardware flooding will not be enabled on a physical port that has a Layer 3 address configured. For virtual routing (VE) interfaces, packets are processed by the CPU by default, but hardware flooding can be enabled. See “Enabling Hardware Flooding on Virtual Routing Interfaces” on page 8-3 for more information.

**Configuring CPU Protection**

Configuring CPU protection consists of enabling CPU protection, specifying conditions that place the system into exhausted mode, and specifying actions to take when the system is in exhausted mode. The following sections instruct how to enable CPU protection and describe the default conditions and actions on the device, and how to modify the default conditions and actions.

**Enabling CPU Protection**

The CPU protection feature is disabled by default. To enable it, enter one or both of the following commands, depending on whether you want the device to protect the CPU, the CAM, or both.

- The following command enables the HP device to automatically take actions when thresholds related to high CAM usage are exceeded:

  ProCurveRS(config)# cpupro-action hardware-flooding enable

  **NOTE:** Hardware flooding actions are supported on EP devices only.
To enable hardware flooding on virtual interfaces, see "Enabling Hardware Flooding on Virtual Routing Interfaces" on page 8-3.

- The following command enables the HP device to automatically take actions when thresholds related to high CPU usage are exceeded:

  ProCurveRS(config)# cpupro-action quick-aging enable

**Syntax:** [no] cpupro-action hardware-flooding enable

**Syntax:** [no] cpupro-action quick-aging enable

Use the **no** form of the command to disable CPU protection.

**Enabling Hardware Flooding on Virtual Routing Interfaces**

By default, hardware flooding on virtual routing interfaces causes the device to copy packets to the CPU. You can optionally configure the device to allow hardware flooding without copying packets to the CPU.

To globally allow hardware flooding on virtual routing interfaces and disable the device from copying packets to the CPU, enter the following command:

  ProCurveRS(config)# cpupro-action hardware ve-not-to-cpu

**Syntax:** [no] cpupro-action hardware ve-not-to-cpu

To allow hardware flooding on a virtual routing interface for VLAN 10 and disable the device from copying packets to the CPU, enter the following command:

  ProCurveRS(config)# vlan 10
  ProCurveRS(config-vlan-10)# ve-flooding-not-to-cpu

**Syntax:** [no] ve-flooding-not-to-cpu

The setting for an individual VLAN overrides the global setting.

**Default CPU Protection Conditions and Actions**

By default, there are three CPU protection conditions defined on the device:

- Condition 1 is related to CPU usage. The declaring watermark is CPU usage at 90%, and the clearing watermark is CPU usage at 60%.
- Condition 2 is related to Layer 2, Layer 3, or Layer 4 CAM usage. The declaring watermark is Layer 2 CAM usage at 90%, and the clearing watermark is Layer 2 CAM usage at 60%.
- Condition 3 is a composite condition that is true if either Condition 1 or Condition 2 are true.

Condition 3 is associated with the quick aging, unknown-unicast flooding, multicast flooding, and broadcast flooding actions. This means that when condition 3 is true, these actions will take place.

**Modifying Default Conditions**

You can modify the default CPU protection conditions listed above.

For example, to modify the default condition for CPU utilization percentage, enter a command such as the following:

  ProCurveRS(config)# cpupro-condition sys cpu declaring 95 clearing 60

**Syntax:** [no] cpupro-condition sys cpu declaring <percent> clearing <percent>

To modify the default condition for Layer 2, Layer 3, or Layer 4 CAM usage percentage, enter a command such as the following:

  ProCurveRS(config)# cpupro-condition sys cam declaring 95 clearing 60

**Syntax:** [no] cpupro-condition sys cam declaring <percent> clearing <percent>

For each condition, the declaring watermark percentage must be higher than the clearing watermark percentage.
Specifying Actions
For the hardware flooding actions, you can specify the number of CAM entries that can be allocated to each kind of traffic, as well as whether to flood or drop the traffic.

Allocating CAM Entries for Hardware Flooding
To accommodate the hardware flooding/dropping actions, the device allocates Layer 2 CAM entries to match broadcast traffic, multicast traffic, and unknown unicast traffic. These Layer 2 CAM entries exist in three sections of Layer 2 CAM space, one section for each type of traffic. By default, each of these sections consist of 256 CAM entries. You can optionally configure the number of CAM entries allocated for each type of traffic.

For example, to allocate 128 CAM entries for unknown-unicast flooding, enter the following command:

```
ProCurveRS(config)# cpupro-action hardware unknown-unicast-flooding max-entries 128
```

**Syntax:** [no] cpupro-action hardware broadcast-flooding | multicast-flooding | unknown-unicast-flooding
max-entries <entries>

Specifying Whether to Flood or Drop Traffic
When the unknown-unicast, broadcast, or multicast traffic actions are enabled, by default the device forwards the traffic in hardware, flooding it to all ports in the VLAN. You can optionally configure the device to drop the traffic instead.

For example, to cause unknown-unicast traffic to be dropped when the device enters exhausted mode, enter the following command:

```
ProCurveRS(config)# cpupro-action hardware unknown-unicast-flooding mode drop
```

**Syntax:** [no] cpupro-action hardware broadcast-flooding | multicast-flooding | unknown-unicast-flooding
mode flood | drop

Displaying CPU Protection Information
You can display information about the conditions and actions configured on the device.

Displaying Condition Information
To display the CPU protection conditions configured on the device, enter the following command:

```
ProCurveRS# show l2-cpupro conditions
```

**Syntax:** show l2-cpupro conditions

Table 8.1 lists the output of the show l2-cpupro condition command.
Table 8.1: Output of the show l2-cpupro condition command

<table>
<thead>
<tr>
<th>This field</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition Configuration:</td>
<td>The conditions configured on the device. These include the three pre-configured conditions, as well as any user-configured conditions.</td>
</tr>
<tr>
<td>Condition Monitoring:</td>
<td>Whether any of the conditions has surpassed its declaring watermark.</td>
</tr>
<tr>
<td>CPU Condition:</td>
<td>Whether the condition defined for CPU usage percentage has surpassed its declaring watermark, as well as the condition's declaring watermark, clearing watermark, and the number of times the declaring watermark has been exceeded.</td>
</tr>
<tr>
<td>Layer 2 CAM Condition:</td>
<td>Whether the condition defined for Layer 2 CAM usage percentage has surpassed its declaring watermark, as well as the condition's declaring watermark, clearing watermark, and the number of times the declaring watermark has been exceeded.</td>
</tr>
</tbody>
</table>

Displaying Action Information

To display information about actions configured on the device, enter the following command:

ProCurveRS# show l2-cpupro actions

Action Configuration:
1: action(03) q-aging(Ena) Deactivated
2: action(03) hw-flood(Ena) Deactivated

Action Execution:
Quick Aging: enabled
   Not in Quick Aging mode
   Normal age limit: 126
   Quick age limit: 63

HW Flooding:
unknown-unicast: installed not activated
   max entries: 256, current entries: 5
   action mode:flooding
multicast: installed not activated
   max entries: 256, current entries: 5
   action mode:flooding
broadcast: installed not activated
   max entries: 256, current entries: 5
   action mode:flooding

Syntax: show l2-cpupro actions

Table 8.2 lists the output of the show l2-cpupro actions command.
### Table 8.2: Output of the `show l2-cpupro actions` command

<table>
<thead>
<tr>
<th>This field</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action Configuration:</td>
<td>The actions configured on the device.</td>
</tr>
<tr>
<td>Action Execution:</td>
<td>Which actions have been enabled.</td>
</tr>
<tr>
<td>Quick Aging:</td>
<td>Whether the quick aging action has been enabled for a condition.</td>
</tr>
<tr>
<td>Not in Quick Aging mode</td>
<td>Whether the device is in exhausted mode and the quick aging action is in effect.</td>
</tr>
<tr>
<td>Normal age limit:</td>
<td>The age limit for CAM entries when the device is in normal mode.</td>
</tr>
<tr>
<td>Quick age limit:</td>
<td>The age limit for CAM entries when the device is in exhausted mode and the quick aging action is in effect.</td>
</tr>
<tr>
<td>HW Flooding:</td>
<td>Information about the three kinds of hardware-flooding actions.</td>
</tr>
<tr>
<td>unknown-unicast:</td>
<td>Whether CAM entries for the unknown-unicast action have been installed and whether the unknown-unicast action has been enabled:</td>
</tr>
<tr>
<td></td>
<td>max entries: – The maximum number of Layer 2 CAM entries that can be allocated for hardware flooding of unknown-unicast traffic.</td>
</tr>
<tr>
<td></td>
<td>current entries: – The number of Layer 2 CAM entries currently in use for hardware flooding of unknown-unicast traffic.</td>
</tr>
<tr>
<td></td>
<td>action mode: – Whether the device floods or drops unknown-unicast traffic when this action takes place.</td>
</tr>
<tr>
<td>broadcast:</td>
<td>Whether CAM entries for the broadcast action have been installed and whether the broadcast action has been enabled:</td>
</tr>
<tr>
<td></td>
<td>max entries: – The maximum number of Layer 2 CAM entries that can be allocated for hardware flooding of broadcast traffic.</td>
</tr>
<tr>
<td></td>
<td>current entries: – The number of Layer 2 CAM entries currently in use for hardware flooding of broadcast traffic.</td>
</tr>
<tr>
<td></td>
<td>action mode: – Whether the device floods or drops broadcast traffic when this action takes place.</td>
</tr>
<tr>
<td>multicast:</td>
<td>Whether CAM entries for the multicast action have been installed and whether the multicast action has been enabled:</td>
</tr>
<tr>
<td></td>
<td>max entries: – The maximum number of Layer 2 CAM entries that can be allocated for hardware flooding of multicast traffic.</td>
</tr>
<tr>
<td></td>
<td>current entries: – The number of Layer 2 CAM entries currently in use for hardware flooding of multicast traffic.</td>
</tr>
<tr>
<td></td>
<td>action mode: – Whether the device floods or drops multicast traffic when this action takes place.</td>
</tr>
</tbody>
</table>