Control Plane Policing

This chapter describes Control Plane Policing and procedures to configure Control Plane Policing.

- Control Plane Policing, page 1
- Finding Feature Information, page 1
- Restrictions for Control Plane Policing, page 2
- Benefits of Control Plane Policing, page 3
- Defining Control Plane Services, page 3
- Verifying Control Plane Services, page 4
- Configuration Examples for Control Plane Policing, page 6
- Technical Assistance, page 6

Control Plane Policing

The Control Plane Policing feature allows you to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS devices and switches against reconnaissance and denial-of-service (DoS) attacks. In this way, the control plane (CP) can help maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.

Finding Feature Information

For the latest feature information and caveats, see the release notes for your platform and software release. Use Cisco Feature Navigator to find information about platform support and Cisco IOS XE Software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.
Restrictions for Control Plane Policing

Output Rate-Limiting Support

Output rate-limiting is performed in the silent (packet discard) mode. Silent mode enables a device to silently discard packets using policy maps applied to output control plane traffic with the `service-policy output` command.

MQC Restrictions

The Control Plane Policing feature requires the MQC to configure packet classification, packet marking, and traffic policing. All restrictions that apply when you use the MQC to configure traffic policing also apply when you configure control plane policing. Only two MQC actions are supported in policy maps—`police` and `set`.

Only `permit any any` is supported.

The Control Plane Policing feature supports IP, IGMP, OSPF and ARP.

OSPF Restrictions

- Hardware based layer 3 forwarding is not supported.
- The maximum layer 3 traffic line rate supported is 3 Mbps. When the traffic line rate exceeds 3 Mbps, all layer 3 protocols fail.

Policer Support

- Only 3Mbps policer is supported.
- More than 3Mbps policer cannot be attached to the control plane.
- Only input policer is supported.
- If any control packet is configured for 3Mbps rate limit, all the remaining control packets are dropped.
- There is no priority method for control-packets.

We recommend that you configure support control packets within 2Mbps and spare 1Mbps for class-default.

Match Criteria Support and Restrictions

The following classification (match) criteria are supported:

- Standard and extended IP access control lists (ACLs).

  **Note**  
  In extended IP access control list only IGMP and ospf is supported.

- In class-map configuration mode, match criteria specified by the following commands:
  
  * match protocol ip
match protocol arp

**Note**
The `match input-interface` command is not supported.

**Note**
Features that require Network-Based Application Recognition (NBAR) classification may not work well at the control plane level.

### Benefits of Control Plane Policing

Configuring the Control Plane Policing feature on your Cisco router or switch provides the following benefits:

- Protection against DoS attacks at infrastructure routers and switches
- QoS control for packets that are destined to the control plane of Cisco routers or switches
- Ease of configuration for control plane policies
- Better platform reliability and availability

### Defining Control Plane Services

**Restrictions for Control Plane Services**

- Platform-specific restrictions, if any, are checked when the service policy is applied to the control plane interface.
- Output policing does not provide any performance benefits. It simply controls the information that is leaving the device.

**Before You Begin**

Before you enter control-plane configuration mode to attach an existing QoS policy to the control plane, you must first create the policy using MQC to define a class map and policy map for control plane traffic.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `control-plane`
4. `service-policy {input} policy-map-name`
5. `end`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch&gt; <code>enable</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters control-plane configuration mode (a prerequisite for Step 4)</td>
</tr>
<tr>
<td><code>control-plane</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>control-plane</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Attaches a QoS service policy to the control plane. Note the following points:</td>
</tr>
<tr>
<td><code>service-policy {input} policy-map-name</code></td>
<td>- <code>input</code>—Applies the specified service policy to packets received on the control plane.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-cp)# <code>service-policy input control-plane-policy</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-cp)# <code>end</code></td>
</tr>
</tbody>
</table>

### Verifying Control Plane Services

### SUMMARY STEPS

1. enable
2. `show policy-map control-plane`
3. `exit`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Displays information about the control plane.</td>
</tr>
<tr>
<td><code>show policy-map control-plane</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# show policy-map control-plane all</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>(Optional) Exits privileged EXEC mode.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# exit</code></td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

The following example shows that the policy map TEST is associated with the control plane. This policy map polices traffic that matches the class map TEST, while allowing all other traffic (that matches the class map "class-default") to go through as is.

```
Switch# sh policy-map control-plane
```

Limited counter support. Refer documentation for details.

**Control Plane**

```
Service-policy input: pigmp

Class-map: igmp (match-all)
  108210 packets, 6925376 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: access-group 100
  police:
    cir 2000000 bps, bc 62500 bytes
    conformed 98551 packets, 6307200 bytes; actions:
      transmit
    exceeded 9659 packets, 618176 bytes; actions:
      drop
    conformed 0000 bps, exceeded 0000 bps

Class-map: class-default (match-any)
  17 packets, 5959 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: any
  police:
    cir 1000000 bps, bc 31250 bytes
    conformed 17 packets, 5959 bytes; actions:
      transmit
    exceeded 0 packets, 0 bytes; actions:
      drop
    conformed 0000 bps, exceeded 0000 bps
```
The following example shows how to configure control plane policing:

```
Switch(config)# access-list 101 permit ospf any any
Switch(config)# class-map ospf
Switch(config-cmap)# match access-group 101
Switch(config)# policy-map pospf
Switch(config-pmap)# class ospf
Switch(config-pmap-c)# police cir 2m
Switch(config-pmap-c-police)# control-plane
Switch(config-cp)# service-policy input pospf
```

**Technical Assistance**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
<tr>
<td>download documentation, software, and tools. Use these resources to install</td>
<td></td>
</tr>
<tr>
<td>and configure the software and to troubleshoot and resolve technical</td>
<td></td>
</tr>
<tr>
<td>issues with Cisco products and technologies. Access to most tools on the</td>
<td></td>
</tr>
<tr>
<td>Cisco Support and Documentation website requires a Cisco.com user ID and</td>
<td></td>
</tr>
<tr>
<td>password.</td>
<td></td>
</tr>
</tbody>
</table>