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 XE routers 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.

Restrictions for Control Plane Policing

Output Rate-Limiting Support

Output rate-limiting is performed in silent (packet discard) mode. Silent mode enables a router to silently discard packets using policy maps applied to output control plane traffic with the **service-policy output** command. For more information, see the “Output Rate-Limiting and Silent Mode Operation” section.

MQC Restrictions

The Control Plane Policing feature requires the Modular QoS CLI (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 commands are supported in policy maps—**police** and **set**.

Match Criteria Support and Restrictions

The following classification (match) criteria are supported:

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

- In class-map configuration mode, match criteria specified by the following commands:
  - **match dscp**
  - **match ip dscp**
  - **match ip precedence**
  - **match precedence**
  - **match protocol arp**
  - **match protocol ipv6**
  - **match protocol pppoe**

Note The **match protocol pppoe** command matches all PPPoE data packets that are sent to the control plane.

- **match protocol pppoe-discovery**

Note The **match protocol pppoe-discovery** command matches all PPPoE control packets that are sent to the control plane.

- **match qos-group**

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.

Information About Control Plane Policing

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

Control Plane Terms to Understand

The following terms are used for the Control Plane Policing feature:

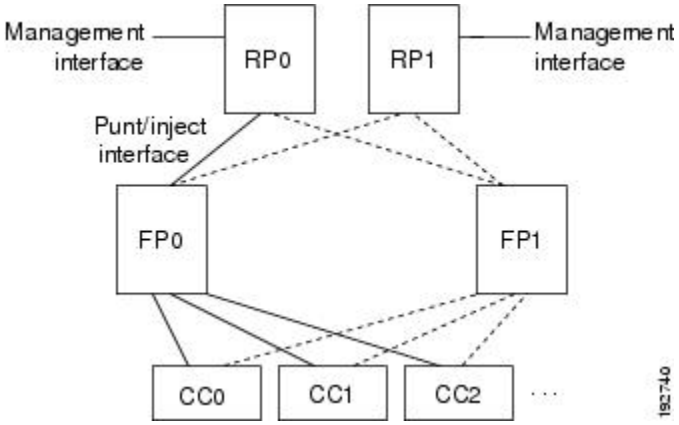
- Control plane—A collection of processes that run at the process level on the Route Processor (RP). These processes collectively provide high-level control for most Cisco IOS XE functions. The traffic sent to or sent by the control plane is called control traffic.
- Forwarding plane—A device that is responsible for high-speed forwarding of IP packets. Its logic is kept simple so that it can be implemented by hardware to do fast packet-forwarding. It punts packets that require complex processing (for example, packets with IP options) to the RP for the control plane to process them.

Control Plane Policing Overview

To protect the control plane on a router from DoS attacks and to provide fine-control over the traffic to or from the control plane, the Control Plane Policing feature treats the control plane as a separate entity with its own interface for ingress (input) and egress (output) traffic. This interface is called the punt/inject interface, and it is similar to a physical interface on the router. Along this interface, packets are punted from the forwarding plane to the RP (in the input direction) and injected from the RP to the forwarding plane (in the output direction). A set of quality of service (QoS) rules can be applied on this interface in order to achieve CoPP.

These QoS rules are applied only after the packet has been determined to have the control plane as its destination or when a packet exits from the control plane. You can configure a service policy (QoS policy map) to prevent unwanted packets from progressing after a specified rate limit has been reached; for example, a system administrator can limit all TCP/SYN packets that are destined for the control plane to a maximum rate of 1 megabit per second.

Figure 1: Abstract Illustration of a Device with Dual RPs and Dual Forwarding Panes



The figure above provides an abstract illustration of a device with dual RPs and dual forwarding planes. Only one RP and one forwarding plane are active at any time. The other RP and forwarding plane are in stand-by mode and do not receive traffic from the carrier card (CC). Packets destined to the control plane come in through the carrier card and then go through the active forwarding plane before being punted to the active RP. When an input QoS policy map is configured on the control plane, the active forwarding plane performs the QoS action (for example, a transmit, drop, or set action) before punting packets to the active RP in order to achieve the best protection of the control plane in the active RP.

On the other hand, packets exiting the control plane are injected to the active forwarding plane, and then go out through the carrier card. When an output QoS policy map is configured on the control plane, the active forwarding plane performs the QoS action after receiving the injected packets from the RP. This process saves the valuable CPU resource in the RP.

Note As shown in "Control Plane Policing Overview" section, the management interface is directly connected to the RP, so all traffic through the management interface to or from the control-plane is not subject to the CoPP function performed by the forwarding plane.

In high-availability (HA) mode, when an RP switchover happens, the active forwarding plane forwards traffic to the new active RP along the new punt/inject interface. The active forwarding plane continues to perform the CoPP function before punting traffic to the new active RP. When a forwarding plane switchover happens, the new active forwarding plane receives traffic from the carrier card and performs the CoPP function before punting traffic to the active RP.

Note The handles some traditional control traffic in the forwarding plane directly to reduce the load on the control plane. One example is the IP Internet Control Message Protocol (ICMP) echo-request packet sent to this router. When a router receives such packets, the packets are handled directly in the forwarding plane without being punted to the RP. In order to be consistent with other Cisco routers and to provide the same capability to control such packets using CoPP, the router extends the CoPP function on such packets, even though the packets are not punted to the RP. Customers can still use the CoPP function to rate-limit or to mark such packets.

Output Rate-Limiting and Silent Mode Operation

A router is automatically enabled to silently discard packets when you configure output policing on control plane traffic using the **service-policy output** *policy-map-name* command.

Rate-limiting (policing) of output traffic from the control plane is performed in silent mode. In silent mode, a router that is running Cisco IOS XE software operates without sending any system messages. If a packet that is exiting the control plane is discarded for output policing, you do not receive an error message.

How to Use Control Plane Policing

Defining Control Plane Services

Perform this task to define control plane services, such as packet rate control and silent packet discard for the active RP.

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.

Note

- 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **control-plane**
4. **service-policy** {**input** | **output** *policy-map-name*}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**control-plane** **Example:** `Device(config)# control-plane`	Enters control-plane configuration mode (which is a prerequisite for defining control plane services).
Step 4	**service-policy** {**input** | **output** *policy-map-name*} **Example:** `Device(config-cp)# service-policy input control-plane-policy`	Attaches a QoS service policy to the control plane. • **input**—Applies the specified service policy to packets received on the control plane. • **output**—Applies the specified service policy to packets transmitted from the control plane and enables the device to silently discard packets. • *policy-map-name*—Name of a service policy map (created using the **policy-map** command) to be attached.
Step 5	**end** **Example:** `Device(config-cp)# end`	(Optional) Returns to privileged EXEC mode.

Verifying Control Plane Services

SUMMARY STEPS

1. **enable**
2. **show policy-map control-plane** [**all**] [**input** [**class** *class-name*] | **output** [*class class-name*]]
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show policy-map control-plane** [**all**] [**input** [**class** *class-name*]	**output** [*class class-name*]] **Example:** `Device# show policy-map control-plane all`	Displays information about the control plane. • **all**—(Optional) Displays service policy information about all QoS policies used on the CP. • **input**—(Optional) Displays statistics for the attached input policy. • **output**—(Optional) Displays statistics for the attached output policy. • **class** *class-name*—(Optional) Specifies the name of the traffic class whose configuration and statistics are displayed.
Step 3	**exit** **Example:** `Device# exit`	(Optional) Exits privileged EXEC mode.

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.

```
Device# show policy-map control-plane

Control Plane
Service-policy input:TEST
Class-map:TEST (match-all)
      20 packets, 11280 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:access-group 101
      police:
        8000 bps, 1500 limit, 1500 extended limit
        conformed 15 packets, 6210 bytes; action:transmit
```

```
        exceeded 5 packets, 5070 bytes; action:drop
        violated 0 packets, 0 bytes; action:drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
Class-map:class-default (match-any)
      105325 packets, 11415151 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:any
```

Configuring Control Plane Policing to Mitigate Denial-of-Service Attacks

Apply control plane policing (CoPP) to RSVP packets to mitigate denial of service (DoS) attacks.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **permit** *protocol* {**any | host** {*address* | *name*}} {**any | host** {*address* | *name*}}
4. **access-list** *access-list-number* **permit** *protocol* {**tcd | udp**} {**any | host** {*source-addr* | *name*}} **eq** *port number* {**any | host** {*source-addr* | *name*}} **eq** *port number*
5. **class-map** *class-map-name*
6. **match access-group** *access-list-index*
7. **exit**
8. **policy-map** *policy-map-name*
9. **class** *class-map-name*
10. **police rate** *units* **pps**
11. **conform-action** *action*
12. **exit**
13. **exit**
14. **control plane** [**host | transit | cef-exception**]
15. **service-policy** {**input** | **output**} *policy-map-name*
16. **exit**
17. **exit**
18. **show control-plane** {**aggregate** | **cef-exception** | **counters** | **features** | **host** | **transit**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**access-list** *access-list-number* **permit** *protocol* {**any** | **host** {*address* | *name*}} {**any** | **host** {*address* | *name*}} **Example:** `Device(config)# access-list 140 permit 46 any any`	Configures an access list for filtering frames by protocol type.
Step 4	**access-list** *access-list-number* **permit** *protocol* {**tcd** | **udp**} {**any** | **host** {*source-addr* | *name*}} **eq** *port number* {**any** | **host** {*source-addr* | *name*}} **eq** *port number* **Example:** `Device(config)# access-list 141 permit udp any eq 1699 any eq 1698`	Configures an access list for filtering frames by UDP protocol and matches only packets with a given port number.
Step 5	**class-map** *class-map-name* **Example:** `Device(config)# class-map match-any MyClassMap`	Creates a class-map and enters QoS class-map configuration mode.
Step 6	**match access-group** *access-list-index* **Example:** `Device(config-cmap)# match access-group 140`	Specifies access groups to apply to an identity policy. The range of valid values is 1-2799.
Step 7	**exit** **Example:** `Device(config-cmap)# exit`	Exits QoS class-map configuration mode and returns to global configuration mode.
Step 8	**policy-map** *policy-map-name* **Example:** `Device(config)# policy-map Policy1`	Specifies a service policy and enters QoS policy-map configuration mode.
Step 9	**class** *class-map-name* **Example:** `Device(config-pmap-)# class MyClassMap`	Enters QoS policy-map class configuration more
Step 10	**police rate** *units* **pps** **Example:** `Device(config-pmap-c)# police rate 10 pps`	Polices traffic destined for the control plane at a specified rate.
Step 11	**conform-action** *action* **Example:** `Device(config-pmap-c-police)# conform-action transmit`	(Optional) Specifies the action to take on packets that conform to the police rate limit and enters policy-map class police configuration mode.
Step 12	**exit** **Example:** `Device(config-pmap-c-police)# exit`	Exits policy-map class police configuration mode

	Command or Action	Purpose
Step 13	**exit** **Example:** `Device(config-pmap-)# exit`	Exits policy-map class configuration mode
Step 14	**control plane** [**host** | **transit** | **cef-exception**] **Example:** `Device(config)# control-plane`	Associates or modifies attributes (such as a service policy) that are associated with the control plane of the device and enters control plane configuration mode.
Step 15	**service-policy** {**input** | **output**} *policy-map-name* **Example:** `Device(config-cp)# service-policy input Policy1`	Attaches a policy map to a control plane.
Step 16	**exit** **Example:** `Device(config-cp)# exit`	Exits control plane configuration mode and returns to global configuration mode.
Step 17	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode returns to privileged EXEC mode.
Step 18	**show control-plane** {**aggregate** | **cef-exception** | **counters** | **features** | **host** | **transit**} **Example:** `Device# show control-plane features`	Displays the configured control plane features

Configuration Examples for Control Plane Policing

Example: Configuring Control Plane Policing on Input Telnet Traffic

The following example shows how to apply a QoS policy for aggregate control plane services to Telnet traffic that is received on the control plane. Trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 forward Telnet packets to the control plane without constraint while allowing all remaining Telnet packets to be policed at the specified rate.

```
! Allow 10.1.1.1 trusted host traffic.
Device(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet

! Allow 10.1.1.2 trusted host traffic.
Device(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet

! Rate-limit all other Telnet traffic.
Device(config)# access-list 140 permit tcp any any eq telnet
! Define class-map "telnet-class."
Device(config)# class-map telnet-class

Device(config-cmap)# match access-group 140
```

```
Device(config-cmap)# exit
Device(config)# policy-map control-plane-in
Device(config-pmap)# class telnet-class
Device(config-pmap-c)# police 80000 conform transmit exceed drop
Device(config-pmap-c)# exit
Device(config-pmap)# exit
! Define aggregate control plane service for the active route processor.
Device(config)# control-plane
Device(config-cp)# service-policy input control-plane-in
Device(config-cp)# end
```

Example: Configuring Control Plane Policing on Output ICMP Traffic

The following example shows how to apply a QoS policy for aggregate control plane services to Telnet traffic transmitted from the control plane. Trusted networks with source addresses 10.0.0.0 and 10.0.0.1 receive Internet Control Management Protocol (ICMP) port-unreachable responses without constraint while allowing all remaining ICMP port-unreachable responses to be dropped.

```
! Allow 10.0.0.0 trusted network traffic.
Device(config)# access-list 141 deny icmp 10.0.0.0 0.0.0.255 any port-unreachable

! Allow
10.0.0.1
 trusted network traffic.
Device(config)# access-list 141 deny icmp 10.0.0.1 0.0.0.255 any port-unreachable

! Rate-limit all other ICMP traffic.
Device(config)# access-list 141 permit icmp any any port-unreachable
Device(config)# class-map icmp-class

Device(config-cmap)# match access-group 141
Device(config-cmap)# exit
Device(config)# policy-map control-plane-out
! Drop all traffic that matches the class "icmp-class."
Device(config-pmap)# class icmp-class
Device(config-pmap-c)# drop
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# control-plane
! Define aggregate control plane service for the active route processor.
Device(config-cp)# service-policy output control-plane-out
Device(config-cp)# end
```

Example: Marking Output Control Plane Packets

The following example shows how to apply a QoS policy on the control plane to mark all egress IPv6 echo-request packets with IPv6 precedence 6.

```
! Match all IPv6 Echo Requests
Device(config)# ipv6 access-list coppacl-ipv6-icmp-request
Device(config-ipv6-acl)# permit icmp any any echo-request
Device(config-ipv6-acl)# exit
Device(config)# class-map match-all coppclass-ipv6-icmp-request
Device(config-cmap)# match access-group name coppacl-ipv6-icmp-request
Device(config-cmap)# exit
! Set all egress IPv6 Echo Requests with precedence 6
Device(config)# policy-map copp-policy
```

```
Device(config-pmap)# class coppclass-ipv6-icmp-request
Device(config-pmap-c)# set precedence 6
Device(config-pmap-c)# exit
Device(config-pmap)# exit
! Define control plane service for the active route processor.
Device(config)# control-plane
Device(config-cp)# service-policy output copp-policy
Device(config-cp)# end
```

Example: Configuring Control Plane Policing to Mitigate Denial-of-Service Attacks

The following example shows how to configure control plane policing (CoPP) to police RSVP packets at a specified rate and displays configured CoPP features.

```
Device> enable
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# access-list 140 permit 46 any any
Device(config)# access-list 141 permit adp any eq 1699 any eq 1698
Device(config)# class-map match-any MyClassMap
Device(config-cmap)# match access-group 140
Device(config-cmap)# match access-group 141
Device(config-cmap)# exit
Device(config)# policy-map Policy1
Device(config-pmap)# class MyClassMap
Device(config-pmap-c)# police rate 10 pps
Device(config-pmap-c-police)# conform-action transmit
Device(config-pmap-c-police)# exceed-action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# control-plane
Device(config-cp)# service-policy input Policy1
Device(config-cp)#
*Sep 14 08:07:39.898: %CP-5-FEATURE: Control-plane Policing feature enabled on Control plane
 aggregate path
Device(config-cp)#
Device(config-c p)# exit
Device(config)# exit
Device#
*Sep 14 08:09:04.154: %SYS-5-CONFIG_I: Configured from console by console
Device# show control-plane features
Total 1 features configured

Control plane aggregate path features :

-------------------------------------------------------
Control-plane Policing activated Sep 14 2012 08:0

-------------------------------------------------------
```

Enabling QoS Policing and Matching for PPPoE Traffic on the Input Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **platform qos punt-path-matching**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**platform qos punt-path-matching** **Example:** `Device(config)# platform qos punt-path-matching`	Enables QoS policing and matching for PPPoE traffic on the input interface.
Step 4	**end** **Example:** `Device(config)# end`	(Optional) Returns to privileged EXEC mode.

Disabling QoS Policing and Matching for PPPoE Traffic on the Input Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no platform qos punt-path-matching**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**no platform qos punt-path-matching** **Example:** `Device(config)# no platform qos punt-path-matching`	Disables QoS policing and matching for PPPoE traffic on the input interface.
Step 4	**end** **Example:** `Device(config)# end`	(Optional) Returns to privileged EXEC mode.

Example: Configuring PPPoE and PPPoE Discovery Packets on the Input Interface and Control Plane

The following example shows how to configure PPPoE and PPPoE discovery packets on the input interface and control plane:

```
Device#configure terminal
Device(config)#class-map pppoed
Device(config-cmap)#match protocol pppoe-discovery
Device(config-cmap)#class-map pppoe
Device(config-cmap)#match protocol pppoe
Device(config-cmap)#policy-map pppoe-input
Device(config-pmap)#class pppoed

Device(config-pmap-c)#police 10000
Device(config-pmap-c-police)#class pppoe
Device(config-pmap-c)#police 10000
Device(config-pmap-c-police)#int g0/0/0.100
Device(config-subif)#service-p input pppoe-input

Device(config-subif)#end

Device#show platform hardware qfp active feature qos config global

Punt-Path-Matching are: enabled
```

Additional References for Control Plane Policing

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	Cisco IOS Quality of Service Solutions Command Reference
QoS features overview	"Quality of Service Overview" module
MQC	"Applying QoS Features Using the MQC" module
Security features overview	"Security Overview" module

MIBs

MIB	MIBs Link
CISCO-CLASS-BASED-QOS-MIB	To locate and download MIBs for selected platforms, Cisco IOS XE Software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

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

Feature Information for Control Plane Policing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Control Plane Policing