Control Plane Policing

Last Updated: December 9, 2011

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.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

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, page 4.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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**.

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

On the Cisco ASR 1000 series router, the following terms are used for the Control Plane Policing feature.

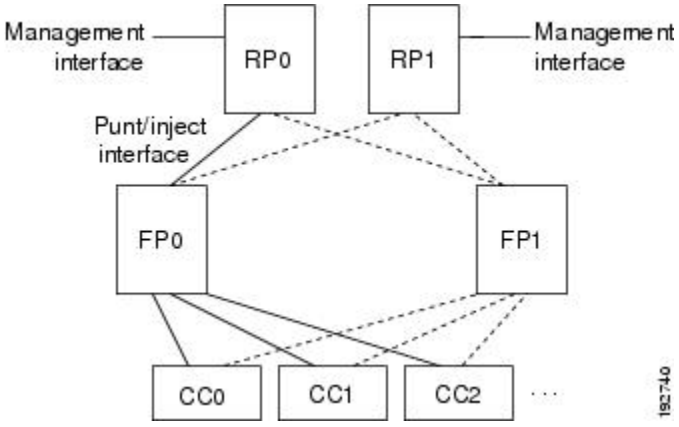
- Control plane (CP)--A collection of processes that run at the process level on the Route Processor (RP). These processes collectively provide high-level control for most Cisco IOS XE functions. The traffic sent to or sent by the control plane is called control traffic.
- Forwarding plane (FP)--A device 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 CP on a router from DoS attacks and to provide fine-control over the traffic to or from the CP, the Control Plane Policing feature treats the CP 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 FP to the RP (in the input direction) and injected from the RP to the FP (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 CP as its destination or when a packet exits from the CP. 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 CP to a maximum rate of 1 megabit per second.

Figure 1 Abstract Illustration of a Cisco ASR 1000 Series Router with Dual RPs and Dual FPs



The figure below provides an abstract illustration of a Cisco ASR 1000 series router with dual RPs and dual FPs. Only one RP and one FP are active at any time. The other RP and FP are in stand-by mode and do not receive traffic from the carrier card (CC). Packets destined to the CP come in through the carrier card, and then go through the active FP before being punted to the active RP. When an input QoS policy map is configured on the CP, the active FP 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 CP are injected to the active FP, and then go out through the carrier card. When an output QoS policy map is configured on the CP, the active FP performs the QoS action after receiving the injected packets from the RP. Again this saves the valuable CPU resource in the RP.

Note As shown in Control Plane Policing Overview, page 3, 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 FP.

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

Note The Cisco ASR 1000 series router handles some traditional control traffic in the FP directly to reduce the load on the CP. One example is the IP Internet Control Message Protocol (ICMP) echo-request packet sent to this router. When a Cisco ASR1000 series router receives such packets, the packets are handled directly in the FP 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 Cisco ASR 1000 series 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 CP 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 CP services, such as packet rate control and silent packet discard, for the active RP.

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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**control-plane** **Example:** `Router(config)# control-plane`	Enters control-plane configuration mode (a prerequisite for Defining Control Plane Services, page 4).

	Command or Action	Purpose
Step 4	**service-policy** {**input**| **output** *policy-map-name* **Example:** `Router(config-cp)# service-policy input control-plane-policy`	Attaches a QoS service policy to the control plane. Note the following points: • **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 router 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:** `Router(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:** `Router> 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:** `Router# show policy-map control-plane all`	Displays information about the control plane. Note the following points: • **all** --(Optional) Service policy information about all QoS policies used on the CP. • **input** --(Optional) Statistics for the attached input policy. • **output** --(Optional) Statistics for the attached output policy. • **class** *class-name* --(Optional) Name of the traffic class whose configuration and statistics are displayed.

	Command or Action	Purpose
Step 3	**exit** **Example:** `Router# 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.

```
Router# 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
```

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 on the CP for input Telnet traffic. 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.
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet

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

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

```
Router(config)# class-map telnet-class

Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-in
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police 80000 conform transmit exceed drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Define control plane service for the active route processor.
Router(config)# control-plane
Router(config-cp)# service-policy input control-plane-in
Router(config-cp)# end
```

Example Configuring Control Plane Policing on Output ICMP Traffic

The following example shows how to apply a QoS policy on the CP for egress ICMP port-unreachable packets. Trusted networks with source addresses 10.0.0.0 and 10.0.1.0 receive 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.
Router(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.
Router(config)# access-list 141 deny icmp 10.0.1.0 0.0.0.255 any port-unreachable

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

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

Example Marking Output Control Plane Packets

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

```
! Match all IPv6 Echo Requests
Router(config)# ipv6 access-list coppacl-ipv6-icmp-request
Router(config-ipv6-acl)# permit icmp any any echo-request
Router(config-ipv6-acl)# exit
Router(config)# class-map match-all coppclass-ipv6-icmp-request
Router(config-cmap)# match access-group name coppacl-ipv6-icmp-request
Router(config-cmap)# exit
! Set all egress IPv6 Echo Requests with precedence 6
Router(config)# policy-map copp-policy
Router(config-pmap)# class coppclass-ipv6-icmp-request
Router(config-pmap-c)# set precedence 6
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Define control plane service for the active route processor.
```

```
Router(config)# control-plane
Router(config-cp)# service-policy output copp-policy
Router(config-cp)# end
```

Additional References

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

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

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

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

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

Feature Name	Releases	Feature Information
Control Plane Policing	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.2	The Control Plane Policing feature allows users 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 routers and switches against reconnaissance and denial-of-service (DoS) attacks. For Cisco IOS XE Release 2.1, this feature was implemented on Cisco ASR 1000 series routers. For Cisco IOS XE Release 2.2, this feature was modified to include support for packet marking, output rate-limiting, and additional match criteria. The following commands were introduced or modified: **match protocol pppoe**, **match protocol pppoe-discovery**.