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 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.

Information About Control Plane Policing

Control Plane Policing Overview

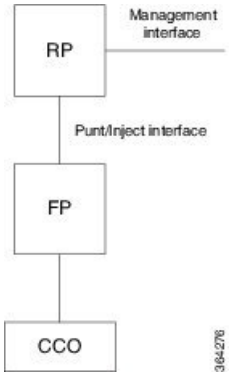
To protect the control plane on a router from DoS attacks and to provide fine-control over the traffic to the control plane, the Control Plane Policing feature treats the control plane as a separate entity with its own interface for ingress (input) and egress (output) traffic. This interface is called the punt or 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 the input direction) 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. 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/TELNET packets that are destined for the control plane.

You can use the **platform qos-feature copp-mpls enable** command to enable the Control Plane Policing feature on the device for MPLS explicit null scenario, control packets destined to the device is punted to proper control CPU Q. If CoPP-MPLS remains disabled, then self destined control packets like BGP, LDP, telnet and so on, that are MPLS explicit null tagged are not classified by CoPP and is punted to HOST_Q instead of CFM_Q/CONTROL_Q.

Note The command **platform qos-feature copp-mpls enable** is supported only on Cisco ASR 920 platform.

Figure 1: Abstract Illustration of a Router with a Single RP and Forwarding Plane



The figure provides an abstract illustration of the router with a single RP and forwarding plane. Packets that are destined to the control plane come in through the carrier card and then go through the forwarding plane before being punted to the RP. When an input QoS policy map is configured on the control plane, the forwarding plane performs the QoS action (for example, a transmit or drop action) before punting packets to the RP in order to achieve the best protection of the control plane in the RP.

Note The figure is not applicable to the RSP3 module.

Note As mentioned in this section, the control plane interface is directly connected to the RP, so all traffic through the control plane interface to or from the control-plane is not subject to the CoPP function performed by the forwarding plane.

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 router, 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.

Supported Protocols

The following table lists the protocols supported on Control Plane Policing feature. It is mandatory that the IP address should match the source or destination IP address.

Supported Protocols	Criteria	Match	Queue#
TFTP - Trivial FTP	IP/Port Match	permit udp 64.202.160.0 0.0.1.255 eq 69 any permit udp 64.202.160.0 0.0.1.255 any eq 69	NQ_CPU_HOST_Q
TELNET	IP/Port Match	permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq telnet permit tcp 169.223.252.0 0.0.3.255 eq telnet host 169.223.253.1	NQ_CPU_CONTROL_Q
NTP - Network Time Protocol	IP/Port Match	permit udp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq ntp permit udp 169.223.252.0 0.0.3.255 eq ntp host 169.223.253.1	NQ_CPU_HOST_Q
FTP - File Transfer Protocol	IP/Port Match	permit tcp host <FTP server> eq ftp <loopback block> permit tcp host <FTP server> <loopback block> eq ftp	NQ_CPU_HOST_Q
SNMP - Simple Network Management Protocol	IP/Port Match	permit udp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq snmp permit udp 169.223.252.0 0.0.3.255 eq snmp host 169.223.253.1	NQ_CPU_HOST_Q

Supported Protocols	Criteria	Match	Queue#
TACACS - Terminal Access Controller Access-Control System	IP/Port Match	permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq tacacs permit tcp 169.223.252.0 0.0.3.255 eq tacacs host 169.223.253.1 permit udp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq tacacs permit udp 169.223.252.0 0.0.3.255 eq tacacs host 169.223.253.1	NQ_CPU_HOST_Q
FTP-DATA	IP/Port Match	permit tcp any any eq 20 permit tcp any eq 20 any permit udp any any eq 20 permit udp any eq 20 any	NQ_CPU_HOST_Q
HTTP - Hypertext Transfer Protocol	IP/Port Match	permit tcp any any eq www permit tcp any eq www any	NQ_CPU_HOST_Q
WCCP - Web Cache Communication Protocol	IP/Port Match	IP access list copp-system-acl-wccp 10 permit udp any eq 2048 any eq 2048	NQ_CPU_HOST_Q
BGP - Border Gateway Protocol	IP/Port Match	permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq bgp permit tcp 169.223.252.0 0.0.3.255 eq bgp host 169.223.253.1	NQ_CPU_CFM_Q

Supported Protocols	Criteria	Match	Queue#
SSH - Secure Shell	IP/Port Match	permit udp [remote vty mgmt subnet] 0.0.0.255 any eq 22 permit udp [remote vty mgmt subnet] 0.0.0.255 eq 22 any permit tcp [remote vty mgmt subnet] 0.0.0.255 any eq 22 permit tcp [remote vty mgmt subnet] 0.0.0.255 eq 22 any	NQ_CPU_HOST_Q
ICMP - Internet Control Message Protocol	Protocol Match	access-list 110 permit icmp any 169.223.253.1	NQ_CPU_HOST_Q
ISAKMP - Internet Security Association and Key Management Protocol	IP/Port Match	permit udp any host x.x.x.x eq isakmp permit udp any eq isakmp host x.x.x.x permit udp any host x.x.x.x eq non500-isakmp permit udp any eq non500-isakmp host x.x.x.x	NQ_CPU_HOST_Q
SAA - Service Assurance Agent	IP/Port Match	permit icmp host 10.2.2.4 host 10.1.1.1	NQ_CPU_HOST_Q
DHCP - Dynamic Host Configuration Protocol	IP/Port Match	permit udp host 0.0.0.0 host 255.255.255.255 eq bootps permit udp any eq bootps any eq bootps permit udp host 0.0.0.0 host 255.255.255.255 eq bootpc permit udp any eq bootpc any eq bootpc	NQ_CPU_HOST_Q

Supported Protocols	Criteria	Match	Queue#
DNS - Domain Name System	IP/Port Match	permit udp host <DNS server> eq domain any permit udp host <DNS server> any eq domain permit tcp host <DNS server> eq domain any permit tcp host <DNS server> any eq domain	NQ_CPU_HOST_Q
DLSw - Data-Link Switching	IP/Port Match	permit any any eq 2065 permit any eq 2065 any	NQ_CPU_HOST_Q
LDP - Label Distribution Protocol	IP/Port Match	permit tcp any any eq 646 permit tcp any eq 646 any permit udp any any eq 646 permit udp any eq 646 any	NQ_CPU_CFM_Q

Supported Protocols	Criteria	Match	Queue#
RADIUS - Remote Authentication Dial In User Service	IP/Port Match	permit udp 64.202.160.0 0.0.1.255 eq 1645 any permit udp 64.202.160.0 0.0.1.255 any eq 1645 permit udp 64.202.160.0 0.0.1.255 eq 1646 any permit udp 64.202.160.0 0.0.1.255 any eq 1646 permit udp 64.202.160.0 0.0.1.255 eq 1812 any permit udp 64.202.160.0 0.0.1.255 any eq 1812 permit udp 64.202.160.0 0.0.1.255 eq 1813 any permit udp 64.202.160.0 0.0.1.255 any eq 1813 permit tcp 64.202.160.0 0.0.1.255 eq 1645 any permit tcp 64.202.160.0 0.0.1.255 any eq 1645 permit tcp 64.202.160.0 0.0.1.255 eq 1646 any permit tcp 64.202.160.0 0.0.1.255 any eq 1646 permit tcp 64.202.160.0 0.0.1.255 eq 1812 any permit tcp 64.202.160.0 0.0.1.255 any eq 1812 permit tcp 64.202.160.0 0.0.1.255 eq 1813 any permit tcp 64.202.160.0 0.0.1.255 any eq 1813	NQ_CPU_HOST_Q
HSRP - Hot Standby Router Protocol	IP/Port Match	permit udp any 224.0.0.0/24 eq 1985 permit udp any eq 1985 224.0.0.0/24	NQ_CPU_HOST_Q

Supported Protocols	Criteria	Match	Queue#
Network Configuration Protocol (NETCONF)	IP/Port Match	IP access list ext copp-system-acl-telnet permit tcp any any eq 830 - NETCONF	NQ_CPU_HOST_Q
PostgreSQL Support	IP/Port Match	IP access list ext copp-system-acl-telnet PostgreSQL IP/Port Match permit tcp 169.223.252.0.0 0.0.3.255 host 169.223.253.1 eq 5432	NQ_CPU_HOST_Q
Source IP or Destination IP	IP Match only	Permit IP host 10.1.1.1 or 10.1.1.2 **Note** The **`permit ip any any`** command is not supported.	NQ_CPU_HOST_Q

Input Rate-Limiting and Silent Mode Operation

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

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

Restrictions for Control Plane Policing

Input Rate-Limiting Support

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

MQC Restrictions

The Control Plane Policing feature requires the Modular QoS CLI (MQC) to configure packet classification and traffic policing. All restrictions that apply when you use the MQC to configure traffic policing also apply when you configure control plane policing.

Match Criteria Support

Only the extended IP access control lists (ACLs) classification (match) criteria is supported.

Restrictions for CoPP

- IPv6 is not supported.
- Port range ACL is not supported.
- To filter MPLS labeled packets, use the **platform qos-feature copp-mpls enable** command.
- Due to hardware limitation, to match the control plane packets against CoPP, ACL rules that match with IP addresses should be added, since adding generic ACL rules with any any matches both the data plane and control plane traffic.

IP Access List Overview

Access control lists (ACLs) perform packet filtering to control which packets move through the network and where. Such control provides security by helping to limit network traffic, restrict the access of users and devices to the network, and prevent traffic from leaving a network. IP access lists can reduce the chance of spoofing and denial-of-service attacks and allow dynamic, temporary user access through a firewall.

IP access lists can also be used for purposes other than security, such as bandwidth control, restricting the content of routing updates, redistributing routes, triggering dial-on-demand (DDR) calls, limiting debug output, and identifying or classifying traffic for quality of service (QoS) features. This module provides an overview of IP access lists.

Benefits

Improved Traffic Flow

This feature improves the Turbo ACL processing process in PXF by more expediently removing older entries. As a result, more Turbo ACL processing can be done in the PXF processing path, thereby allowing more router traffic to be accelerated using the PXF processing path.

Configuration of Route Processor Memory Limits for ACL Processing

This feature allows users to set the amount of memory reserved for ACL processes (such as compilation, storage, and classification) in the RP path. Users who need more memory for ACL processes now have the ability to set aside additional memory resources in the RP path for ACL processes. Users who need more more memory for other processes in the RP path now can set aside less memory for ACL processes.

Benefits of IP Access Lists

Access control lists (ACLs) perform packet filtering to control the flow of packets through a network. Packet filtering can restrict the access of users and devices to a network, providing a measure of security. Access lists can save network resources by reducing traffic. The benefits of using access lists are as follows:

- Authenticate incoming rsh and rcp requests—Access lists can simplify the identification of local users, remote hosts, and remote users in an authentication database that is configured to control access to a device. The authentication database enables Cisco software to receive incoming remote shell (rsh) and remote copy (rcp) protocol requests.
- Block unwanted traffic or users—Access lists can filter incoming or outgoing packets on an interface, thereby controlling access to a network based on source addresses, destination addresses, or user authentication. You can also use access lists to determine the types of traffic that are forwarded or blocked

at device interfaces. For example, you can use access lists to permit e-mail traffic to be routed through a network and to block all Telnet traffic from entering the network.

- Control access to vty—Access lists on an inbound vty (Telnet) can control who can access the lines to a device. Access lists on an outbound vty can control the destinations that the lines from a device can reach.
- Identify or classify traffic for QoS features—Access lists provide congestion avoidance by setting the IP precedence for Weighted Random Early Detection (WRED) and committed access rate (CAR). Access lists also provide congestion management for class-based weighted fair queueing (CBWFQ), priority queueing, and custom queueing.
- Limit debug command output—Access lists can limit debug output based on an IP address or a protocol.
- Provide bandwidth control—Access lists on a slow link can prevent excess traffic on a network.
- Provide NAT control—Access lists can control which addresses are translated by Network Address Translation (NAT).
- Reduce the chance of DoS attacks—Access lists reduce the chance of denial-of-service (DoS) attacks. Specify IP source addresses to control traffic from hosts, networks, or users from accessing your network. Configure the TCP Intercept feature to can prevent servers from being flooded with requests for connection.
- Restrict the content of routing updates—Access lists can control routing updates that are sent, received, or redistributed in networks.
- Trigger dial-on-demand calls—Access lists can enforce dial and disconnect criteria.

IP Address Range-Based Filtering Support for CoPP ACL

IP Access Control Lists are a set of rules that perform packet filtering to control the flow of packets through a network. Packet filtering provides security by the following features:

- Limiting the access of traffic into a network.
- Restricting user and device access to a network.
- Preventing traffic from leaving a network.
- Reduce the chance of spoofing and denial-of-service attacks.

Table 1: Feature History Table

Feature Name	Release Information	Description
IP Address Range-Based Filtering Support for CoPP ACL	Cisco IOS XE Bengaluru 17.5.1	The CoPP ACL Template feature supports Ingress on In-band Management Loopback interface and Ingress on Data plane interface to block traffic using MPLS. CoPP ACL supports Source IP based filtering on the Cisco router.

Prior to the Cisco IOS XE Bengaluru 17.5.1 release, IP address Range-Based Filtering for CoPP ACL was not supported. Effective Cisco IOS XE Bengaluru 17.5.1 this feature enables you to securely manage MPLS traffic by supporting the following requirements:

- Ingress on In-Band Management Loopback interface.
- Ingress on Data plane interface to block MGMT Traffic on MPLS.

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 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.

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

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.

- *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

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show policy-map control-plane** [**all**] [**input** |**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.
- **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.

```
Router# show policy-map control-plane
Control Plane

Service-policy input: copp-ftp

Class-map: copp-ftp (match-any)
2234 packets, 223400 bytes
```

```
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: access-group name copp-ftp
police:
cir 10000000 bps, be 312500 bytes
conformed 2234 packets, 223400 bytes; actions:
transmit
exceeded 0 packets, 0 bytes; actions:
drop
conformed 0000 bps, exceeded 0000 bps

Class-map: class-default (match-any)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
```

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

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

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **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 111 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 4 **class-map [match-any | match-all | type]** *class-map-name*

Example:

```
Device(config)# class-map match-any MyClassMap
```

Creates a class-map and enters QoS class-map configuration mode.

Step 5 **match access-group** [*access-list-index* | *access-group-name*]

Example:

```
Device(config-cmap)# match access-group 111
```

Specifies access groups to apply to an identity policy. The range of valid values is 1-2799.

Step 6 **exit**

Example:

```
Device(config-cmap)# exit
```

Exits QoS class-map configuration mode and returns to global configuration mode.

Step 7 **policy-map** *policy-map-name*

Example:

```
Device(config)# policy-map Policy1
```

Specifies a service policy and enters QoS policy-map configuration mode.

Step 8 **class** [*class-map-name* | *class-default*]

Example:

```
Device(config-pmap)# class MyClassMap
```

Enters QoS policy-map class configuration more

Step 9 **police** {*rate-bps* | **cir** {*cir-bps* | **percent** *percent*}} [**bc** *burst-bytes*] [**conform-action** | **exceed-action** | **violate-action**]*action*] [ ]

Example:

```
police cir 10000000 bc 8000 pir 12000000 be 8000 conform-action transmit exceed-action transmit
violate-action drop
```

Configure a traffic policer based on the traffic rate or committed information rate (CIR). By default, no policer is defined.

- *rate-bps*—Specifies average traffic rate in bits per second (b/s). The range is 64000 to 10000000000. Supply an optional postfix (K, M, G). Decimal point is allowed.
- **cir**—Specifies a committed information rate (CIR).
- *cir-bps*—Specifies a CIR in bits per second (b/s). The range is 64000 to 10000000000. Supply an optional postfix (K, M, G). Decimal point is allowed.
- **be** *burst-bytes*—(Optional) Specifies the conformed burst (be) or the number of acceptable burst bytes. The range is 8000 to 16000000.
- **conform-action** *action*— (Optional) Specifies action to take on packets that conform to the specified rate limit.
- **pir** *pir-bps*—(Optional) Specifies the peak information rate (PIR).

Note **cir percent** *percent* option is not supported on the router.

Step 10 **exit**

Example:

```
Device(config-pmap-c-police)# exit
```

Exits policy-map class police configuration mode

Step 11 **exit**

Example:

```
Device(config-pmap-c)# exit
```

Exits policy-map class configuration mode

Step 12 **exit**

Example:

```
Device(config-pmap)# exit
```

Exits policy-map configuration mode

Step 13 **control-plane**

Example:

```
Device(config)# control-plane
```

Enters control plane configuration mode.

Step 14 **service-policyinput** *policy-map-name*

Example:

```
Device(config-cp)# service-policy input Policy1
```

Attaches a policy map to a control plane.

Step 15 **exit**

Example:

```
Device(config-cp)# exit
```

Exits control plane configuration mode and returns to global configuration mode.

Step 16 **exit**

Example:

```
Device(config)# exit
```

Exits global configuration mode returns to privileged EXEC mode.

Configuring CoPP ACL

Before you begin

- To filter MPLS labelled packets, use the **platform qos-feature copp-mpls enable** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **platform qos-feature copp-mpls enable**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enter privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enter global configuration mode.
Step 3	**platform qos-feature copp-mpls enable** **Example:** `Router(config)#platform qos-feature copp-mpls enable`	Configure the CoPP MPLS command on the Cisco Router.
Step 4	**exit** **Example:** `Router(config)#exit`	Exit global configuration mode.

Verifying CoPP ACL

The following example shows how to verify the CoPP ACL on the Cisco Router.

```
Router(config)#sdm prefer enable_acl_copp
COPP ACL template change.
Current template = disable_acl_copp
Updated template = enable_acl_copp
Standby is reloaded, it will come up with in it required for new template
once standby comes up Please trigger SSO
```

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 but are still policed for a maximum rate.

All remaining Telnet packets are dropped by the control-plane.

```
! Define trusted host traffic.
DEVICE(config)#ip access-list extended telnet-trust
DEVICE(config-ext-nacl)#10 permit tcp host 10.1.1.1 any eq telnet
DEVICE(config-ext-nacl)#20 permit tcp host 10.1.1.2 any eq telnet
DEVICE(config-ext-nacl)#exit

! Define all other Telnet traffic.
DEVICE(config)#ip access-list extended telnet-drop
DEVICE(config-ext-nacl)#10 permit tcp any any eq telnet
DEVICE(config-ext-nacl)#exit

! Define class map for trusted hosts
DEVICE(config)#class-map match-all copp-trust
```

```
DEVICE(config-cmap)#match access-group name telnet-trust
DEVICE(config-cmap)#exit

! Define class map for un-trusted hosts
DEVICE(config)#class-map match-all copp-drop
DEVICE(config-cmap)#match access-group name telnet-drop
DEVICE(config-cmap)#exit

! Define the policy-map for both type of hosts
DEVICE(config)#policy-map control-plane-in
DEVICE(config-pmap)#class copp-trust
DEVICE(config-pmap-c)#police 1000000 conform-action transmit  exceed-action drop
DEVICE(config-pmap-c-police)#class copp-drop
DEVICE(config-pmap-c-police)#exit
DEVICE(config-pmap-c)#police 1000000 conform-action drop  exceed-action drop
DEVICE(config-pmap-c-police)#exit
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


! 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
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html

Standards and RFCs

Standard/RFC	Title
No specific Standards and RFCs are supported by the features in this document.	—

MIBs

MIB	MIBs Link
—	To locate and download MIBs for selected platforms, Cisco IOS 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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html