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 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 caveats and feature information, see Bug Search Tool and 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 module.

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.

Prerequisites for Control Plane Policing

The Modular Quality of Service (QoS) Command-Line interface (CLI) (MQC) is used to configure the packet classification and policing functionality of the Control Plane Policing feature.

Before configuring Control Plane Policing (CoPP), you should understand the procedures for using the MQC. For information about the MQC, see the "Applying QoS Features Using the MQC" module.

Restrictions for Control Plane Policing

Aggregate and Distributed Control Plane Policing

Aggregate policing is supported in Cisco IOS Release 12.0(29)S, Cisco IOS Release 12.2(18)S, Cisco IOS Release 12.3(4)T, and later releases.

Distributed policing is supported only in Cisco IOS Release 12.0(30)S and later Cisco IOS 12.0S releases.

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, on page 9.

Output rate-limiting (policing) in silent mode is supported only in:

- Cisco IOS Release 12.2(25)S and later Cisco IOS 12.2S releases
- Cisco IOS Release 12.3(4)T and later Cisco IOS 12.3T releases

Output rate-limiting is not supported for distributed control plane services in Cisco IOS 12.0S releases or in Cisco IOS 12.2SX releases.

Output rate-limiting is not supported on the Cisco 7500 series and Cisco 10720 Internet router.

MQC Restrictions

The Control Plane Policing feature requires the MQC to configure packet classification and policing. All restrictions that apply when you use the MQC to configure policing also apply when you configure control plane policing. Only two MQC actions are supported in policy maps--**police** and **drop**.

Note On the Cisco 10720 Internet router, only the **police**command, not the **drop** command, is supported in policy maps. In addition, in a QoS service policy that is attached to the Cisco 10720 control plane, the **police**command does not support **set** actions as arguments in **conform-action**, **exceed-action**, and **violate-action** parameters.

Features that require Network-Based Application Recognition (NBAR) classification may not work well at the control plane level. The following classification (match) criteria are supported on all platforms:

- Standard and extended IP access lists (ACLs).
- In class-map configuration mode: **match ip dscp**, **match ip precedence**, and **match protocol arp,**and **match protocol pppoe**commands.

Note In the Cisco IOS 12.2SX release, the **match protocol arp** command is not supported.

On the Cisco 10720 Internet router, the following MQC commands are also supported in class-map configuration mode: **match input-interface**, **match mpls experimental**, **match protocol ipv6**, and **match qos-group**.

When using these commands for control plane policing on the Cisco 10720 Internet router, note the following restrictions:

- Packet classification using match criteria is not supported for packets that cannot be classified in the Cisco 10720 data path, such as unknown Layer 2 encapsulation and IP options.
- The following IPv6 fields are not be supported in packet classification for IPv6 QoS on the Cisco 10720 Internet router and are, therefore, not supported for control plane policing:
  - IPv6 source and destination addresses
  - Layer 2 class of service (CoS)
  - IPv6 routing header flag
  - IPv6 undetermined transport flag
  - IPv6 flow label
  - IP Real-Time transport Protocol (RTP)

Note Packets that are not supported for QoS packet classification on the Cisco 10720 Internet router are not policed in the default traffic class for control plane policing.

CISCO-CLASS-BASED-QOS-MIB Control Plane Support

In Cisco IOS Release 12.3(7)T and later Cisco IOS 12.3T releases, the CISCO-CLASS-BASED-QOS-MIB is extended to manage control plane QoS policies and provide information about the control plane.

Cisco IOS Release 12.2(18)SXD1

In Cisco IOS Release 12.2(18)SXD1 and later releases, Hardware Control Plane Interface for Control Plane Policing has the following restrictions:

- Supported only with Supervisor Engine 720. Not supported with Supervisor Engine 2.
- Does not support CoPP output rate-limiting (policing).
- Does not support the CoPP silent operation mode.
- Cisco IOS Release 12.2(18)SXD1 and later releases automatically install the CoPP service policy on all DFC-equipped switching modules.

For more information about control plane policing in Cisco IOS Release 12.2(18)SXD1 and later releases, see either of these publications:

- For Catalyst 6500 series switches, see the "Configuring Control Plane Policing (CoPP)" module.
- For Cisco 7600 series routers, see the "Configuring Denial of Service Protection" module.

Information About Control Plane Policing

Benefits of Control Plane Policing

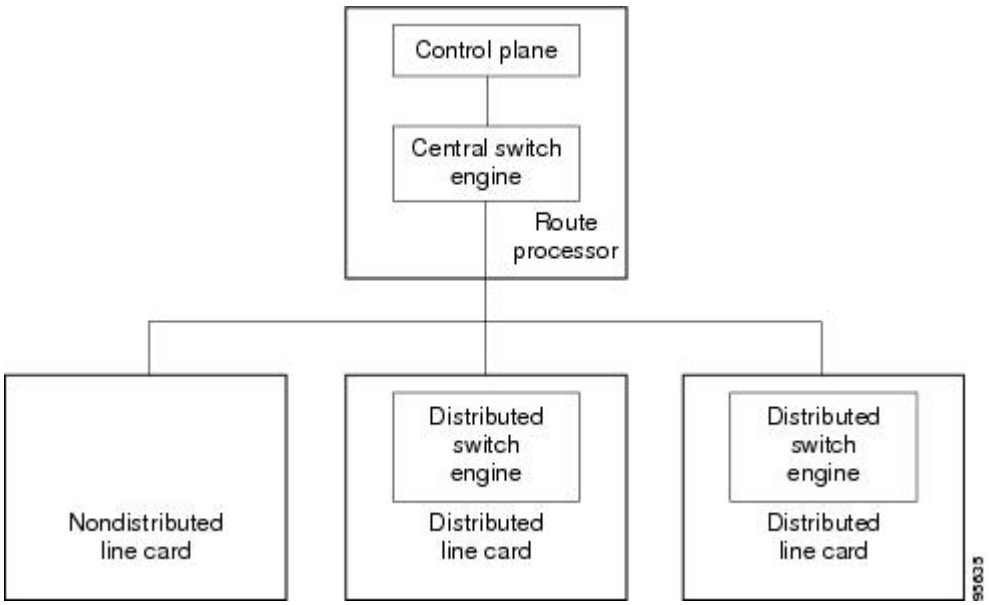
Configuring the Control Plane Policing feature on your Cisco router or switch provides the following benefits:

- 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

Terms to Understand

Because different platforms can have different architectures, the following set of terms is defined. The figure below illustrates how control plane policing works.

Figure 1: Layout of Control Plane, Central Switch Engine, Distributed Switch Engines, and Line Cards on a Router



- 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 functions.
- Central switch engine--A device that is responsible for high-speed routing of IP packets. It also typically performs high-speed input and output services for nondistributed interfaces. (See nondistributed line cards.) The central switch engine is used to implement aggregate CP protection for all interfaces on the router.

Note All IP packets that are destined for the CP should pass through the central switch engine before they are forwarded to the process level.

On the Cisco 10720 Internet router, control plane policing is implemented on Cisco Parallel eXpress Forwarding (PXF) in a Toaster-based architecture. PXF is a hardware-based central switch engine that can filter traffic at a higher rate than the route processor. PXF switches all data traffic separately from the route processor. PXF packet processing occurs at an intermediate step between the nondistributed line cards and the route processor shown in the figure above. In addition to the regular punting, PXF also punts certain types of packets (such as unknown Layer 2 encapsulation and packets with IP options) to the RP for further processing at interrupt level.

Note On the Cisco 10720 Internet router, you can configure enhanced RP protection by using the **ip option drop** command to drop IPv4 packets with IP options that are punted to the RP by PXF. Tunneled IPv4 packets and IPv4 packets with an unsupported encapsulation method are not dropped. For more information, see the "ACL IP Options Selective Drop" module.

- Distributed switch engine--A device that is responsible for high-speed switching of IP packets on distributed line cards without using resources from the central switch engine. It also typically performs input and output services for the line card. Each distributed switch engine is used to implement distributed CP services for all ports on a line card. Input CP services distribute the processing load across multiple line cards and conserve vital central switch engine resources. Distributed CP services are optional; however, they provide a more refined level of service than aggregate services.
- Nondistributed line cards--Line cards that are responsible for receiving packets and occasionally performing input and output services. All packets must be forwarded to the central switch engine for a routing or switching decision. Aggregate CP services provide coverage for nondistributed line cards.

Note Distributed CP services are supported only in Cisco IOS Release 12.0(30)S and later 12.0S releases.

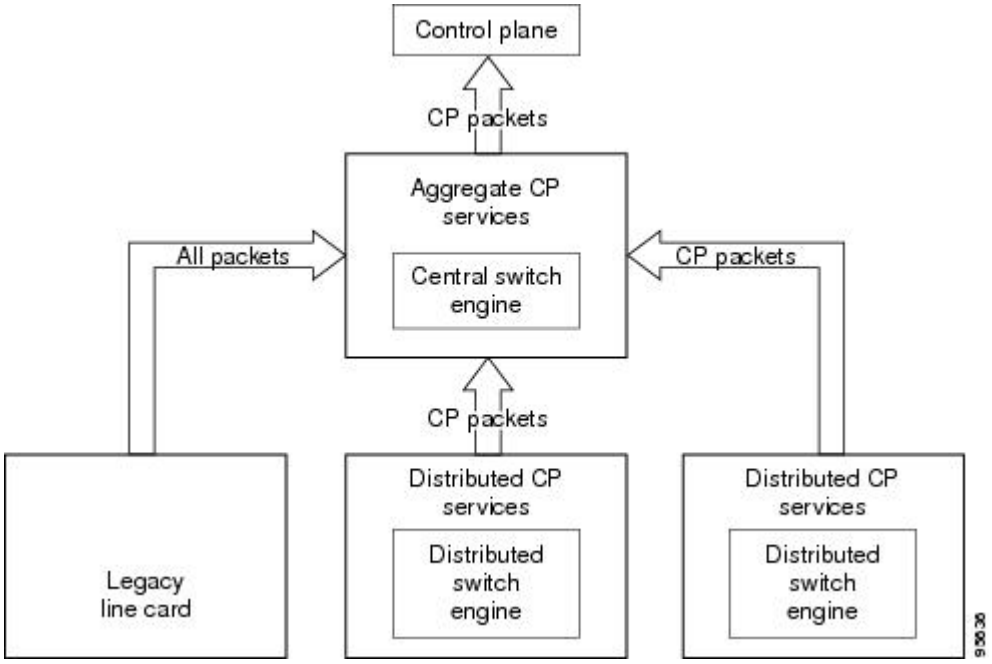
Control Plane Security and Packet QoS Overview

To protect the CP on a router from DoS attacks and to provide packet QoS, the Control Plane Policing feature treats the CP as a separate entity with its own ingress (input) and egress (output) ports, which are like ports on a router and switch. Because the Control Plane Policing feature treats the CP as a separate entity, a set of rules can be established and associated with the ingress and egress ports of the CP.

These rules are applied only after the packet has been determined to have the CP as its destination or when a packet exits the CP. Thereafter, you can configure a service policy 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.

Input CP services are executed after router input port services have been performed and after a routing decision on the input path has been made. As shown in the figure below, CP security and packet QoS are applied on:

Figure 2: Input Control Plane Services: Aggregate and Distributed Services



The following types of Layer 3 packets are forwarded to the control plane and processed by aggregate and distributed control plane policing:

- Routing protocol control packets
- Packets destined for the local IP address of the router
- Packets from management protocols (such as Simple Network Management Protocol [SNMP], Telnet, and secure shell [SSH])

Note Ensure that Layer 3 control packets have priority over other packet types that are destined for the control plane.

Aggregate Control Plane Services

Aggregate control plane services provide control plane policing for all CP packets that are received from all line-card interfaces on the router.

The central switch engine executes normal input port services and makes routing decisions for an incoming packet: if the packet is destined for the CP, aggregate services are performed. Because CP traffic from all line cards must pass through aggregate CP services, these services manage the cumulative amount of CP traffic that reaches the CP.

Aggregate CP service steps are as follows:

1. The line card receives a packet and delivers it to the central switch engine.

Note Before the packet is sent to the central switch engine, additional processing may be necessary for platforms that support hardware-level policing or platform-specific aggregate policing. It is possible that the packet may undergo multiple checks before it undergoes the generic Cisco IOS check.

1. The interfaces perform normal (interface-level) input port services and QoS.
2. The central switch engine performs Layer 3 switching or makes a routing decision, determining whether or not the packet is destined for the CP.
3. The central switch engine performs aggregate CP services for all CP packets.
4. On the basis of the results of the aggregate CP services, the central switch engine either drops the packet or delivers the packet to the CP for final processing.

Functionality Highlights of Aggregate CP Services

The following list highlights the functionality of aggregate CP services:

- Aggregate CP services are defined for a single input interface, such as the CP, and represent an aggregate for all ports on a router.
- Modular QoS is used to define CP services. Class maps and policy maps for both DoS protection and packet QoS are defined for a single aggregate CP service policy.
- Modular QoS does not prevent a single bad port from consuming all allocated bandwidth. Class maps that match an interface or subinterface may be able to constrain the contribution of each interface through an interface-specific policy map.

Distributed Control Plane Services

Distributed control plane services provide control plane policing for all CP packets that are received from the interfaces on a line card.

A distributed switch engine executes normal input port services and makes routing decisions for a packet: if the packet is destined for the CP, distributed CP services are performed. Afterwards, CP traffic from each line card is forwarded to the central switch engine where aggregate CP services are applied.

Note Distributed CP services may also forward conditioned packets to the central switch engine. In this case, aggregate CP services are also performed on the conditioned CP traffic.

Distributed CP service steps are as follows:

1. A line card receives a packet and delivers it to the distributed switch engine.
2. The distributed switch engine performs normal (interface-level) input port services and QoS.

3 The distributed switch engine performs Layer 2 or Layer 3 switching or makes a routing decision, determining whether the packet is destined for the CP.

4 The distributed switch engine performs distributed CP services for all CP packets.

5 On the basis of the results of the distributed CP services, the distributed switch engine either drops the packet or marks the packet and delivers it to the central switch engine for further processing.

6 The central switch engine performs aggregate CP services and delivers the packet to the CP for final processing.

Functionality Highlights of Distributed CP Services

The following list highlights the functionality of distributed CP services:

- Distributed CP services are defined for a single input interface, such as the distributed CP, and represent an aggregate for all ports on a line card.
- The MQC is used to define CP services. Class maps and policy maps for both DoS protection and packet QoS are defined for a single distributed CP service policy. Each line card may have a unique CP service policy that applies traffic classifications, QoS policies, and DoS services to packets received from all ports on the line card in an aggregate way.
- The MQC does not prevent one bad port from consuming all allocated bandwidth on a line card. Class maps that match an interface or subinterface may be able to constrain the contribution of each interface through an interface-specific policy map.
- Distributed CP services allow you to limit the number of CP packets forwarded from a line card to the central switch engine. The total number of CP packets received from all line cards on a router may exceed aggregate CP levels.

Usage of Distributed CP Services

The purpose of CP protection and packet QoS is to apply sufficient control to the packets that reach the control plane. To successfully configure this level of CP protection, you must:

- Apply traditional QoS services using the MQC to CP packets.
- Protect the path to the control plane against indiscriminate packet dropping due to resource exhaustion. If packets are not dropped according to user-defined QoS policies, but are dropped due to a resource limitation, the QoS policy is not maintained.

Distributed CP services allow you to configure specific CP services that are enforced at the line-card level and are required for the following reasons:

- While under a DoS attack, line-card resources may be consumed. In this case, you must configure a drop policy to identify important packets. The drop policy ensures that all important packets arrive to the central switch engine for aggregate CP protection and arrive later to the CP. Distributed CP services allow routers to apply the appropriate drop policy when resources are consumed and therefore maintain the desired QoS priorities. If a line card indiscriminately drops packets, the aggregate CP filter becomes ineffective and the QoS priorities are no longer maintained.
- It is not possible to prevent one interface from consuming all aggregate CP resources. A DoS attack on one port may negatively impact CP processing of traffic from other ports. Distributed CP services allow you to limit the amount of important traffic that is forwarded by a line card to the CP. For example, you

can configure a layered approach in which the combined rates of all line cards are over-subscribed compared to the aggregate rate. The rate of each individual line card would be below the aggregate rate, but combined together, the rates of all line cards exceed it. This over-subscription model is commonly used for other resource-related functions and helps limit the contribution of CP packets from any one line card.

- Distributed CP services provide for slot-level (line-card) filtering. Customer-facing interfaces may have greater security requirements (with more restrictions or for billing reasons) than network-facing interfaces to backbone devices.
- Because distributed CP protection allows you to configure packet filters on a per-line-card basis, processing cycles on line cards may offload aggregate level processing. You can configure Border Gateway Protocol (BGP) filtering at the distributed level for interfaces that use BGP, allowing the aggregate level to filter packets with the remaining filter requirements. Or you can configure identical filters for distributed and aggregate CP services with a distributed packet marking scheme that informs the aggregate filter that a packet has already been checked. Distributed CP service processing further reduces aggregate processing and can significantly reduce the load on aggregate CP services.

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 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.

When control plane policing is configured for output traffic, error messages are not generated in the following cases:

- Traffic that is being transmitted to a port to which the router is not listening
- A connection to a legitimate address and port that is rejected because of a malformed request

The silent mode functionality and output policing on CP traffic are supported only in:

- Cisco IOS Release 12.2(25)S and later Cisco IOS 12.2S releases
- Cisco IOS Release 12.3(4)T and later Cisco IOS 12.3T releases

Silent mode and output policing on CP traffic are not supported for distributed control plane services.

How to Use Control Plane Policing

Defining Aggregate Control Plane Services

To configure aggregate CP services, such as packet rate control and silent packet discard, for the active route processor, complete the following steps.

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.
- Support for output policing is available only in Cisco IOS Release 12.3(4)T and later T-train releases. (Note that 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 Aggregate Control Plane Services).
Step 4	**service-policy** {**input**| **output** *policy-map-name*	Attaches a QoS service policy to the control plane. Note the following points:

	Command or Action	Purpose
	Example: `Router(config-cp)# service-policy input control-plane-policy`	• **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. The name can be a maximum of 40 alphanumeric characters.
Step 5	**end** **Example:** `Router(config-cp)# end`	(Optional) Returns to privileged EXEC mode.

Defining Distributed Control Plane Services

To configure distributed CP services, such as packet rate control, for packets that are destined for the CP and sent from the interfaces on a line card, complete the following steps.

Before You Begin

Before you enter control-plane configuration mode to attach an existing QoS policy for performing distributed control-plane services, 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.
- Support for output policing is available only in Cisco IOS Release 12.3(4)T and later T-train releases. (Note that output policing does not provide any performance benefits. It simply controls the information that is leaving the device.)
- With Cisco IOS 12.2SX releases, the Supervisor Engine 720 automatically installs the service policy on all DFC-equipped switching modules.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **control-plane** [**slot** *slot-number*]
4. **service-policy input** *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** [**slot** *slot-number*] **Example:** `Router(config)# control-plane slot 3`	Enters control-plane configuration mode, which allows you to optionally attach a QoS policy (used to manage CP traffic) to the specified slot. • Enter the **slot** keyword and the slot number, as applicable.
Step 4	**service-policy input** *policy-map-name* **Example:** `Router(config-cp)# service-policy input control-plane-policy`	Attaches a QoS policy map to filter and manage CP traffic on a specified line card before the aggregate CP policy is applied. Note the following points: • **input** --Applies the specified policy map using the distributed switch engine to CP packets that are received from all interfaces on the line card. • *policy-map-name* --Name of a service policy map (created using the **policy-map** command) to be attached. The name can be a maximum of 40 alphanumeric characters. **Note** The **service-policy output** *policy-map-name* command is not supported for applying a QoS policy map for distributed control plane services.
Step 5	**end** **Example:** `Router(config-cp)# end`	(Optional) Returns to privileged EXEC mode.

Verifying Aggregate Control Plane Services

To display information about the service policy attached to the control plane for aggregate CP services, complete the following steps.

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 in aggregate and distributed CP services. • **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.
Step 3	**exit** **Example:** `Router(config-cp)# 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
```

Verifying Distributed Control Plane Services

To display information about the service policy attached to the control plane to perform distributed CP services, complete the following steps.

SUMMARY STEPS

1. **enable**
2. **show policy-map control-plane** [**all**][**slot** *slot-number*] [**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**][**slot** *slot-number*] [**input** [**class** *class-name*] | output [class class-name]] **Example:** `Router# show policy-map control-plane slot 2`	Displays information about the service policy used to apply distributed CP services on the router. Note the following points: • **all** --(Optional) Service policy information about all QoS policies used in aggregate and distributed CP services. • **slot** *slot-number* --(Optional) Service policy information about the QoS policy map used to perform distributed CP services on the specified line card. • **input** --(Optional) Statistics for the attached input policy map. • **output** --(Optional) Statistics for the attached output policy map. • **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 how to display information about the classes of CP traffic received from all interfaces on the line card in slot 1 to which the policy map TESTII is applied for distributed CP services. This policy map polices traffic that matches the traffic class TESTII, while allowing all other traffic (that matches the class map "class-default") to go through as is.

```
Router# show policy-map control-plane slot 1
Control Plane - slot 1
Service-policy input: TESTII (1048)
Class-map: TESTII (match-all) (1049/4)
        0 packets, 0 bytes
        5 minute offered rate 0 bps, drop rate 0 bps
        Match: protocol arp (1050)
        police:
            cir 8000 bps, bc 4470 bytes, be 4470 bytes
          conformed 0 packets, 0 bytes; actions:
            transmit
          exceeded 0 packets, 0 bytes; actions:
            drop
          violated 0 packets, 0 bytes; actions:
            drop
          conformed 0 bps, exceed 0 bps, violate 0 bps
Class-map: class-default (match-any) (1052/0)
        0 packets, 0 bytes
        5 minute offered rate 0 bps, drop rate 0 bps
        Match: any  (1053)
```

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.
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.

	Command or Action	Purpose
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: 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

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

Additional References

The following sections provide references related to the Control Plane Policing feature.

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	"Control Plane Security Overview" module in the *Cisco IOS Security Configuration Guide: Securing the Control Plane*
Control plane policing in Cisco IOS Release 12.2(18)SXD1 and later releases	For Catalyst 6500 series switches, see the "Configuring Control Plane Policing (CoPP)" module. For Cisco 7600 series routers, see the "Configuring Denial of Service Protection" module.
Enhanced RP protection	"ACL IP Options Selective Drop" 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 **Note** Supported only in Cisco IOS Release 12.3(7)T.	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

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 . An account on Cisco.com is not required.

Table 1: Feature Information for Control Plane Policing

Feature Name	Releases	Feature Information
Control Plane Policing	12.2(18)S 12.3(4)T 12.3(7)T 12.0(29)S 12.2(18)SXD1 12.0(30)S 12.2(27)SBC 12.0(32)S 12.3(31)SB2 15.0(1)S	

Feature Name	Releases	Feature Information
		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 Release 12.2(18)S, this feature was introduced. For Release 12.3(4)T, this feature was integrated into Cisco IOS Release 12.3(4)T, and the output rate-limiting (silent mode operation) feature was added. For Release 12.3(7)T, the CISCO-CLASS-BASED-QOS-MIB was extended to manage control plane QoS policies, and the **police rate**command was introduced to support traffic policing on the basis of packets per second for control plane traffic. For Release 12.0(29)S, this feature was integrated into Cisco IOS Release 12.0(29)S. For Release 12.2(18)SXD1, this feature was integrated into Cisco IOS Release 12.2(18)SXD1. For Release 12.0(30)S, this feature was modified to include support for distributed control plane services on the Cisco 12000 series Internet router. For Release 12.2(27)SBC, this feature was integrated into Cisco IOS Release 12.2(27)SBC. For Release 12.0(32)S, this feature was modified to include support for aggregate control plane services on the Cisco 10720 Internet router. For Release 12.3(31)SB2, this feature was implemented on the Cisco 10000 series router for the PRE3.

Feature Name	Releases	Feature Information
		For Release 15.0(1)S, this feature was integrated into Cisco IOS Release 15.0(1)S.