Control Plane Policing

Last Updated: November, 2006

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. 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 in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Control Plane Policing" section on page 34.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

CISCO SYSTEMS

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

Prerequisites for Control Plane Policing

- Understanding the concepts and general configuration procedure (class map and policy map) for applying quality-of-service (QoS) policies on a router

  For information about Cisco IOS QoS and the procedure for configuring QoS in your network using the modular QoS command-line interface (MQC), refer to *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.3 and *Cisco 10000 Series Router Quality of Service Configuration Guide*.

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, and 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 Output Rate-Limiting and Silent Mode Operation, page 10.

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, Cisco 10720 Internet router, and Cisco 10000 series router.

Modular QoS Restrictions

The Control Plane Policing feature requires the modular QoS command-line interface (CLI) (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**.

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** commands.

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

Cisco 10720 Internet Router

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 attached to the 10720 control plane, the **police** command does not support **set** actions as arguments in **conform-action**, **exceed-action**, and **violate-action** parameters.

The following MQC commands are 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 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)

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 10000 Series Router

In Cisco IOS Release 12.2(31)SB2, the Control Plane Policing feature is introduced on the Cisco 10000 series router. It supports traffic policing on the basis of packets per second (pps), as well as all other existing police operations for control plane traffic. The Cisco 10000 series router supports Parallel Express Forwarding (PXF) aggregate control plane policing.

The following MQC commands are supported in class-map configuration mode: **match input-interface**, **match protocol ipv6**, **match qos-group**, **match mpls experimental**, and **match protocol arp**. When using these commands for control plane policing, packet classification using match criteria is not supported for packets that cannot be classified in the data path, such as unknown Layer 2 encapsulation and IP options.

Packets that are not supported for QoS packet classification 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 Control Plane Policing output rate limiting (policing).
- Does not support the Control Plane Policing silent operation mode.

- Cisco IOS Release 12.2(18)SXD1 and later releases automatically install the Control Plane Policing service policy on all DFC-equipped switching modules.

Cisco IOS Release 12.2(31)SB2

Control Plane Policing has the following restrictions on the Cisco 10000 series router:

- Does not support Route Processor (RP) Control Plane Policing.
- Does not support Control Plane Policing output rate limiting (policing).
- Only the **police** command is supported in the control plane policy maps.
- Does not support nested policy maps.

For more information about Control Plane Policing in Cisco IOS Release 12.2(18)SXD1 and later releases, see these publications:

- For Control Plane Policing on Catalyst 6500 series switches:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/dos.htm
- For Control Plane Policing on Cisco 7600 series routers:

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/dos.htm

Information About Control Plane Policing

To configure the Control Plane Policing feature, you should understand the following concepts:

Benefits of Control Plane Policing

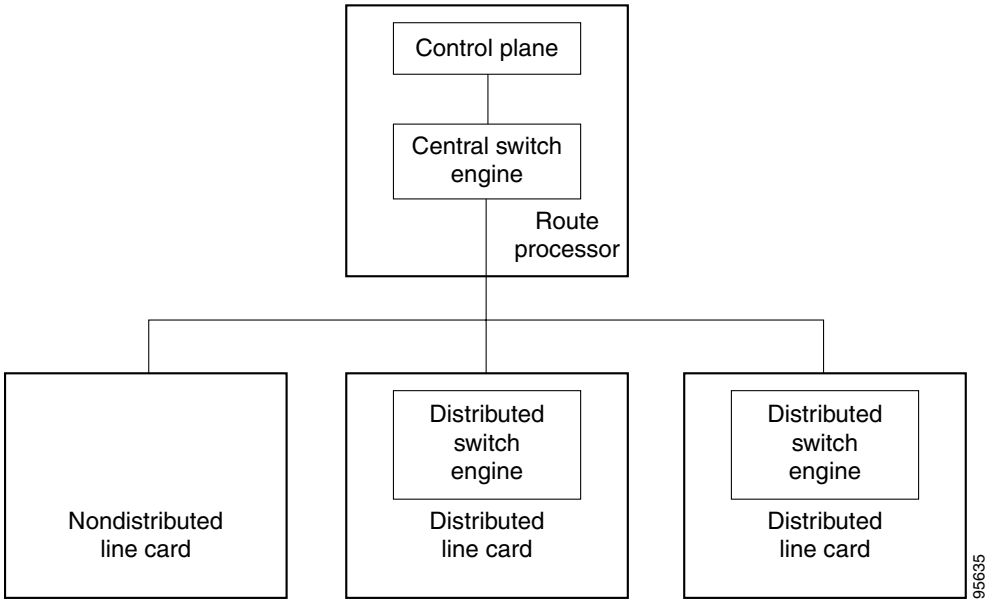
Configuring the Control Plane Policing feature on your Cisco router or switch provides the following benefits:

- 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. Figure 1 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 and the Cisco 10000 series 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 route processor shown in Figure 1. 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.

For more information, refer to *Queueing Architecture and Modular Quality of Service (QoS) on the Cisco 10720 Internet Router* and *Cisco 10000 Series Router Quality of Service Configuration Guide*..

Note On the Cisco 10720 Internet router and the Cisco 10000 series 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 the PXF. Tunneled IPv4 packets and IPv4 packets with an unsupported encapsulation method are not dropped. For more information, refer to *ACL IP Options Selective Drop*.

- 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 only supported in 12.0(30)S and later 12.0S releases.

Control Plane Security and Packet QoS Overview

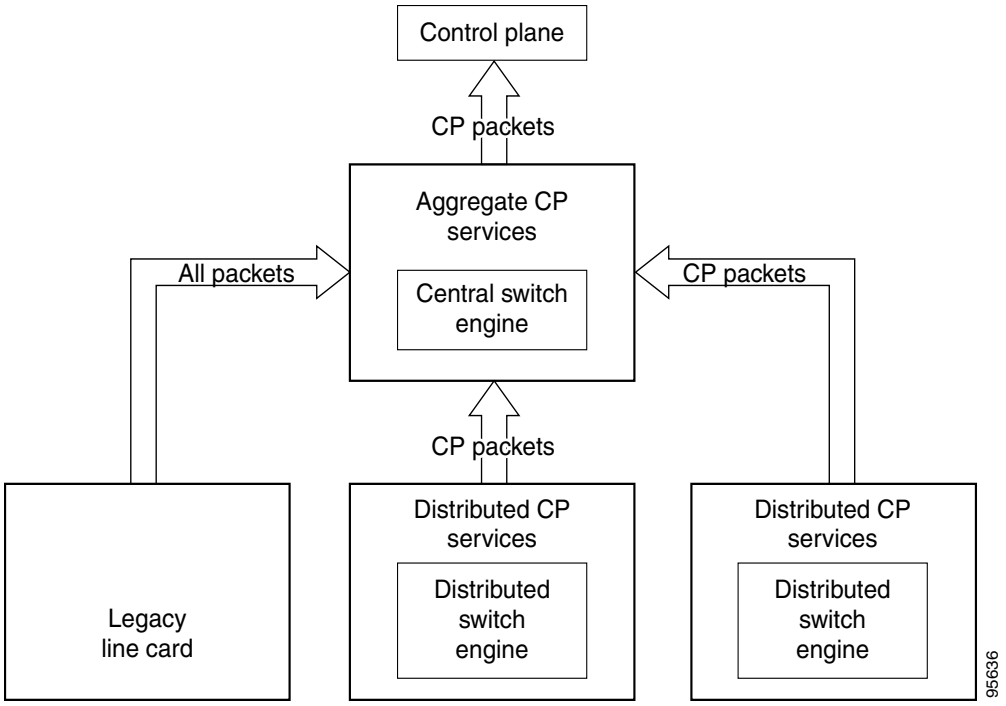
To protect the CP on a router from DoS attacks and to provide packet QoS, the Control Plane Policing feature treats the CP as a separate entity with its own ingress (input) and egress (output) ports, which are like ports on a router and switch. Because the Control Plane Policing feature treats the CP as a separate entity, a set of rules can be established and associated with the ingress and egress port 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 from 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 and a routing decision on the input path have been made. As shown in Figure 2, CP security and packet QoS are applied on:

- An aggregate level by the central switch engine and applied to all CP packets received from all line cards on the router (see Aggregate Control Plane Services, page 7)
- A distributed level by the distributed switch engine of a line card and applied to all CP packets received from all interfaces on the line card (see Distributed Control Plane Services, page 8)

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 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.

2. The interfaces perform normal (interface-level) input port services and QoS.
3. The central switch engine performs Layer 3 switching or makes a routing decision, determining whether or not the packet is destined for the CP.
4. The central switch engine performs aggregate CP services for all CP packets.
5. 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:

- Defined for a single input interface, such as the CP, and represents 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 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 or not 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.
- 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 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.
- Modular QoS 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 amount of CP packets received from all line cards on a router may exceed aggregate CP levels.

Using 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 modular QoS command-line interface 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 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 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 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 is 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 from 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

Note 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 the Control Plane Policing Feature

This section documents the following procedures:

Defining Aggregate Control Plane Services

Perform this task to configure aggregate CP services, such as packet rate control and silent packet discard, for the active route processor.

Prerequisites

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.

For information about how to classify traffic and create a QoS policy, refer to the "Modular Quality of Service Command-Line Interface" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide* and the *Cisco 10000 Series Router Quality of Service Configuration Guide*.

Restrictions

- 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*

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 to attach a QoS policy that manages CP traffic.
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. • **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.

Defining Distributed Control Plane Services

Perform this task to configure distributed control plane services, such as packet rate control, for packets that are destined for the control plane and sent from the interfaces on a line card.

Prerequisites

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.

For information about how to classify traffic and create a QoS policy, refer to the "Modular Quality of Service Command-Line Interface" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide* and the *Cisco 10000 Series Router Quality of Service Configuration Guide*.

Restrictions

- 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, Supervisor Engine 720 automatically installs the service policy on all DFC-equipped switching modules.
- The Cisco 10000 series router only supports aggregate input control plane services.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **control-plane** [**slot** *slot-number*]
4. **service-policy input** *policy-map-name*

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.

	Command or Action	Purpose

Step 3	**control-plane** [**slot** *slot-number*]
	
	Example:
	`Router(config)# control-plane slot 3`
	`Router(config)# control-plane slot`
		Enters control-plane configuration mode to attach a QoS policy to manage CP traffic on the line card in the specified slot.

Step 4	**service-policy input** *policy-map-name* **Example:** `Router(config-cp)# service-policy input control-plane-policy`	Attaches a QoS service policy to filter and manage CP traffic on a specified line card before the aggregate CP policy is applied. • **input**—Applies the specified service policy using the distributed switch engine to CP packets received from all interfaces on the line card. • *policy-map-name*—Name of the service policy to attach.

Verifying Aggregate CP Services

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

SUMMARY STEPS

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

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. • **all**—(Optional) Service policy information about all QoS policies used in aggregate and distributed CP services. • **input**—(Optional) Statistics for the attached input policy. • **class** *class-name*—(Optional) Statistics for an individual traffic class. • **output**—(Optional) Statistics for the attached output policy. **Note** The **output** keyword is supported only in Cisco IOS Release 12.3(4)T and later Cisco IOS 12.3T releases.

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. Table 2 on page 32 describes the significant fields in the display.

```
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 CP Services

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

SUMMARY STEPS

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

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. • **all**—Service policy information about all QoS policies used in aggregate and distributed CP services. • **slot** *slot-number*—Service policy information about the QoS policy used to perform distributed CP services on the specified line card. • **input**—Statistics for the attached input policy. • **output**—Statistics for the attached output policy. • **class** *class-name*—Name of the traffic class whose configuration and statistics are displayed.

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. (Table 2 describes the significant fields shown in the display.)

```
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)
```

Configuration Examples for Control Plane Policing

This section contains examples that shows how to configure aggregate control plane services on both an input and an output interface:

Configuring Control Plane Policing on Input Telnet Traffic: Example

The following example shows how to apply a QoS policy for aggregate CP services to Telnet traffic 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.
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 aggregate control plane service for the active Route Processor.
Router(config)# control-plane
Router(config-cp)# service-policy input control-plane-in
Router(config-cp)# exit
```

Configuring Control Plane Policing on Output Telnet Traffic: Example

The following example shows how to apply a QoS policy for aggregate CP services to Telnet traffic transmitted from the control plane. Trusted networks with source addresses 3.3.3.0 and 4.4.4.0 receive Internet Control Management Protocol (ICMP) port-unreachable responses without constraint, while allowing all remaining ICMP port-unreachable responses to be dropped:

```
! Allow 3.3.3.0 trusted network traffic.
Router(config)# access-list 141 deny icmp 3.3.3.0 0.0.0.255 any port-unreachable
! Allow 4.4.4.0 trusted network traffic.
Router(config)# access-list 141 deny icmp 4.4.4.0 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)# drop
Router(config-pmap-c)# exit
```

```
Router(config-pmap)# exit
Router(config)# control-plane
! Define aggregate control plane service for the active route processor.
Router(config-cp)# service-policy output control-plane-out
Router(config-cp)# exit
```

Configuring Control Plane Policing on Input Distributed CP Traffic: Example

The following example shows how to attach a QoS policy to perform distributed CP services on packets destined for the CP from the interfaces on the line card in slot 1.

As in the previous example, trusted hosts are configured with source addresses 10.1.1.1 and 10.1.1.2 to forward Telnet packets to the control plane without constraint, while allowing all remaining Telnet packets that enter through slot 1 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 aggregate control plane service for the active Route Processor.
Router(config)# control-plane slot 1
Router(config-cp)# service-policy input control-plane-in
Router(config-cp)# exit
```

Additional References

The following sections provide references related to Control Plane Policing.

Related Documents

Related Topic	Document Title
QoS information and configuration tasks	*Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.3 *Cisco 10000 Series Router Quality of Service Configuration Guide*, Release 12.2(31)SB
Additional QoS commands	*Cisco IOS Quality of Service Solutions Command Reference*, Release 12.3T

Standards

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

MIBs

MIBs	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

RFCs	Title
None	—

Technical Assistance

Description	Link
The Cisco Technical Support website, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html

Command Reference

This section documents new and modified commands.

New Commands in Cisco IOS Release 12.2(18)S

- **control-plane**
- **service-policy (control-plane)**
- **show policy-map control-plane**

Modified Commands in Cisco IOS Release 12.3(4)T

- **service-policy (control-plane)**
- **show policy-map control-plane**

New Command in Cisco IOS Release 12.3(7)T

- **service-policy (control-plane)**

Modified Commands in Cisco IOS Release 12.0(30)S

- **control-plane** [**slot** *slot-number*]
- **show policy-map control-plane** [**slot** *slot-number*]

Modified Command in Cisco IOS Release 12.2(31)SB2

- **control-plane**
- **police rate (control-plane)**
- **service-policy (control-plane)**
- **show policy-map control-plane**

control-plane

To enter control-plane configuration mode and apply an existing quality of service (QoS) policy to police traffic destined for the control plane, use the **control-plane** command in global configuration mode. To remove an existing control-plane configuration from the router, use the **no** form of this command.

Syntax for T Releases

control-plane [**host | transit | cef-exception**]

no control-plane [**host | transit | cef-exception**]

Syntax for 12.0 S Releases

control-plane [**slot** *slot-number*] [**host | transit | cef-exception**]

no control-plane [**slot** *slot-number*] [**host | transit | cef-exception**]

Syntax for Cisco 10000 Series Router

control-plane

no control-plane

Syntax Description

host	(Optional) Applies policies to host control-plane traffic.
transit	(Optional) Applies policies to transit control-plane traffic.
cef-exception	(Optional) Applies policies to CEF-exception control-plane traffic.
slot *slot number*	(Optional) Specifies the slot number for the line card to which you want to attach a QoS policy to perform distributed control-plane services.

Command Default

No control-plane service policies are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.0(29)S	This command was integrated into Cisco IOS Release 12.0(29)S.
12.0(30)S	The **slot** *slot-number* parameter was added to configure distributed CP services.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.4(4)T	The **host**, **transit,** and **cef-exception** keywords were added.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

After you enter the **control-plane** command, you can define aggregate control-plane policing policies for the route processor (RP). You can configure a service policy to police all traffic destined to the control plane:

- From all line cards on the router (aggregate CP services)
- From all interfaces on a line card (distributed CP services)

Aggregate CP services manage traffic destined for the control plane and received on the central switch engine from all line cards in the router.

Distributed CP services manage CP traffic from interfaces on a specified line card before CP packets are forwarded to the central switch engine where aggregate CP services are applied.

Note On the Cisco 12000 series Internet router, you can combine distributed and aggregate CP services to protect the control plane from DoS attacks and provide packet QoS. The **slot** *slot-number* parameter is used only for distributed CP services configurations.

Control-plane policing in this version includes enhanced control-plane functionality. It provides a mechanism for early dropping of packets directed toward closed or nonlistened Cisco IOS TCP/UPD ports on the router. It also provides the ability to limit protocol queue usage such that no single misbehaving protocol process can wedge the control plane interface hold queue.

With this enhancement, you can classify control-plane traffic into different categories of traffic. These categories are as follows:

- **Control-plane host subinterface**—Subinterface that receives all control-plane IP traffic that is directly destined for one of the router interfaces. Examples of control-plane host IP traffic include tunnel termination traffic, management traffic or routing protocols such as SSH, SNMP, BGP, OSPF, and EIGRP. All host traffic terminates on and is processed by the router. Most control-plane protection features and policies operate strictly on the control-plane host subinterface. Since most critical router control-plane services, such as routing protocols and management traffic, is received on the control-plane host subinterface, it is critical to protect this traffic through policing and protection policies. CoPP, port-filtering, and per-protocol queue thresholding protection features can be applied on the control-plane host subinterface.
- **Control-plane transit subinterface**—Subinterface that receives all control-plane IP traffic that is software switched by the route processor. This means packets not directly destined to the router itself but rather traffic traversing through the router. Non-terminating tunnels handled by the router are an example of this type of control-plane traffic. Control-plane protection allows specific aggregate policing of all traffic received at this subinterface.
- **Control-plane CEF-exception subinterface**—Subinterface that receives all traffic that is either redirected as a result of a configured input feature in the CEF packet forwarding path for process switching or directly enqueued in the control-plane input queue by the interface driver (for example, ARP, L2 Keepalives and all non-IP host traffic). Control-plane protection allows specific aggregate policing of this specific type of control-plane traffic.

Cisco 10000 Series Router

The **control-plane** command has no arguments or keywords. After you issue the **control-plane** command, you can begin defining aggregate control plane services for the PXF; for example, you can associate a service policy to police all traffic that is destined to the control plane.

Examples

The following example shows how to configure trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 to forward Telnet packets to the control plane without constraint, while allowing all remaining Telnet packets to be policed at the specified rate. The QoS policy is then applied for aggregate CP services to all packets that are entering the control plane from all line cards in the router.

```
! 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 aggregate control plane service for the active Route Processor.
Router(config)# control-plane
Router(config-cp)# service-policy input control-plane-in
Router(config-cp)# exit
```

The next example also shows how to configure trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 to forward Telnet packets to the control plane without constraint, while allowing all remaining Telnet packets that enter through slot 1 to be policed at the specified rate. The QoS policy is applied for distributed CP services to all packets that enter through the interfaces on the line card in slot 1 and are destined for the control plane.

```
! 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 aggregate control plane service for the active Route Processor.
Router(config)# control-plane slot 1
Router(config-cp)# service-policy input control-plane-in
Router(config-cp)# exit
```

The following shows how to apply an aggregate CoPP policy to the host control-plane traffic by applying it to the host control-plane feature path:

```
Router(config)# control-plane host
Router(config-cp)# service-policy input cpp-policy-host
```

The following shows how to apply an aggregate CoPP policy to the transit control-plane traffic by applying it to the control-plane transit feature path:

```
Router(config)# control-plane transit
Router(config-cp)# service-policy input cpp-policy-transit
```

The following shows how to apply an aggregate CoPP policy to the cef-exception control-plane traffic by applying it to the control-plane CEF-exception feature path:

```
Router(config)# control-plane unidentified
Router(config-cp)# service-policy input cpp-policy-unidentified
```

Cisco 10000 Series Router

The following example shows how to configure trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 to 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-policy
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 aggregate control plane service for the active Route Processor.
Router(config)# control-plane
Router(config-cp)# service-policy input control-plane-policy
Router(config-cp)# exit
```

Related Commands

Command	Description
service-policy (control-plane)	Attaches a policy map to the control plane for aggregate or distributed control-plane services.
show policy-map control-plane	Displays the configuration of a class or all classes for the policy map attached to the control plane.

police rate (control-plane)

To configure traffic policing for traffic that is destined for the control plane, use the **police rate** command in policy-map class configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

Syntax for Cisco 10000 Series Router

police rate *units* **pps** [**burst** *burst-in-packets* **packets**] [**peak-rate** *peak-rate-in-pps* **pps**] [**peak-burst** *peak-burst-in-packets* **packets**] [**conform-action** *action* [**exceed-action** *action*] [**violate-action** *action*]

no police rate *units* **pps** [**burst** *burst-in-packets* **packets**] [**peak-rate** *peak-rate-in-pps* **pps**] [**peak-burst** *peak-burst-in-packets* **packets**] [**conform-action** *action*] [**exceed-action** *action*] [**violate-action** *action*]

Syntax for Packets per Seconds

police rate *units* **pps** [**burst** *burst-in-packets* **packets**] [**peak-rate** *peak-rate-in-pps* **pps**] [**peak-burst** *peak-burst-in-packets* **packets**]

no police rate *units* **pps** [**burst** *burst-in-packets* **packets**] [**peak-rate** *peak-rate-in-pps* **pps**] [**peak-burst** *peak-burst-in-packets* **packets**]

Syntax for Bytes per Seconds

police rate *units* **bps** [**burst** *burst-in-bytes* **bytes**] [**peak-rate** *peak-rate-in-bps* **bps**] [**peak-burst** *peak-burst-in-bytes* **bytes**]

no police rate *units* **bps** [**burst** *burst-in-bytes* **bytes**] [**peak-rate** *peak-rate-in-bps* **bps**] [**peak-burst** *peak-burst-in-bytes* **bytes**]

Syntax for Percent

police rate percent *percentage* [**burst** *ms* **ms**] [**peak-rate percent** *percentage*] [**peak-burst** *ms* **ms**]

no police rate percent *percentage* [**burst** *ms* **ms**] [**peak-rate percent** *percentage*] [**peak-burst** *ms* **ms**]

Syntax Description

units	Specifies the police rate. If the police rate is specified in packets per second (pps), the valid ranges of values are: • Cisco 10000 series router—Valid range is 1 to 500000 • Other platforms—Valid range is 1 to 2000000 If the police rate is specified in bps, the valid range of values is 8000 to 10000000000.
pps	Specifies that packets per seconds (pps) will be used to determine the rate at which traffic is policed.

burst *burst-in-packets* **packets**	(Optional) Specifies the burst rate, in packets, will be used for policing traffic. Valid ranges of values are: • Cisco 10000 series router—Valid range is 1 to 25000 • Other platforms—Valid range is 1 to 512000
peak-rate *peak-rate-in-pps* **pps**	(Optional) Specifies the peak information rate (PIR) will be used for policing traffic and calculating the PIR. Valid ranges of values are: • Cisco 10000 series router—Valid range is 1 to 500000 • Other platforms—Valid range is 1 to 512000
peak-burst *peak-burst-in-packets* **packets**	(Optional) Specifies the peak burst value, in packets, will be used for policing traffic. Valid ranges of values are: • Cisco 10000 series router—Valid range is 1 to 25000 • Other platforms—Valid range is 1 to 512000
conform-action *action*	(Optional) Specifies the action to take on packets that conform to the police rate limit. See the "Usage Guidelines" section for the actions you can specify.
exceed-action *action*	(Optional) Specifies the action to take on packets that exceed the rate limit. See the "Usage Guidelines" section for the actions you can specify.
violate-action *action*	(Optional) Specifies the action to take on packets that continuously exceed the police rate limit. See the "Usage Guidelines" section for the actions you can specify.
bps	(Optional) Specifies that bits per second (bps) will be used to determine the rate at which traffic is policed.
burst *burst-in-bytes* **bytes**	(Optional) Specifies the burst rate, in bits, will be used for policing traffic. Valid range is from 1000 to 512000000.
peak-rate *peak-rate-in-bps* **bps**	(Optional) Specifies the peak burst value, in bits, for the peak rate. Valid range is from 1000 to 512000000.
peak-burst *peak-burst-in-bytes* **bytes**	(Optional) Specifies the peak burst value, in bits, will be used for policing traffic. Valid range is from 1000 to 512000000.
percent	A percentage of interface bandwidth will be used to determine the rate at which traffic is policed.
percentage	Specifies the bandwidth percentage. Valid range is from 1 to 100.
burst *ms* **ms**	(Optional) Specifies the burst rate, in milliseconds, will be used for policing traffic. Valid range is from 1 to 2000.
peak-rate percent *percentage*	(Optional) Specifies a percentage of interface bandwidth will be used to determine the PIR. Valid range is from 1 to 100.
peak-burst *ms* **ms**	(Optional) Specifies the peak burst rate, in milliseconds, will be used for policing traffic. Valid range is from 1 to 2000.

Defaults Disabled

Command Modes Policy-map class configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(18)SXD1	Support for this command was introduced on the Supervisor Engine 720.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Use the **police rate** command to limit traffic that is destined for the control plane on the basis of pps, bps, or a percentage of interface bandwidth. If the **police rate** command is issued, but the a rate is not specified, traffic that is destined for the control plane is policed on the basis of bits per second (bps).

Cisco 10000 Series Router

Table 1 lists the actions you can specify for the **conform-action**, **exceed-action**, and **violate-action** keywords. You can specify only one action in a command line.

Table 1 Actions Keyword Options

Action	Description
drop	Drops the packet. This is the default action for traffic that exceeds or violates the committed police rate.
set-clp-transmit *value*	Sets the ATM Cell Loss Priority (CLP) bit to 1 on the ATM cell.
set-discard-class-transmit *value*	Sets the discard class attribute of a packet and transmits the packet with the new discard class setting. Valid values are from 0 to 7.
set-dscp-transmit *value*	Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value setting. Valid values are from 0 to 63.
set-dscp-tunnel-transmit *value*	Rewrites the tunnel packet DSCP and transmits the packet with the new tunnel DSCP value. Valid values are from 0 to 63.
set-frde-transmit	Sets the Frame Relay Discard Eligibility (DE) bit from 0 to 1 on the Frame Relay frame and transmits the packet with the DE bit set to 1.
set-mpls-exp-imposition-transmit *value*	Sets the Multiprotocol Label Switching (MPLS) experimental (EXP) bits in the imposed label headers and transmits the packet with the new MPLS EXP bit value setting. Valid values are from 0 to 7.
set-mpls-exp-transmit *value*	Sets the MPLS EXP field value in the MPLS label header at the input and/or output interfaces. Valid values are from 0 to 7.
set-prec-transmit *value*	Sets the IP precedence and transmits the packet with the new IP precedence value. Valid values are from 0 to 7.
set-prec-tunnel-transmit *value*	Sets the tunnel packet IP precedence and transmits the packet with the new IP precedence value. Valid values are from 0 to 7.

Table 1 Actions Keyword Options

Action	Description
set-qos-transmit *value*	Sets the qos-group and transmits the packet with the new qos-group value. Valid values are from 0 to 63.
transmit	Transmits the packet. The packet is not altered.

Examples

The following example shows how to configure policing on a class to limit traffic to an average rate of 1,500,000 pps:

```
Router(config)# class-map telnet-class
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-policy
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police rate 1500000 pps burst 500000 packets
Router(config-pmap-c)# exit
```

Cisco 10000 Series Router

The following example shows how to configure the action to take on packets that conform to the police rate limit:

```
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
Router(config)# access-list 140 permit tcp any any eq telnet
Router(config)# class-map match-any pps-1
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map copp-pps
Router(config-pmap)# class pps-1
Router(config-pmap)# police rate 10000 pps burst 100 packets peak-rate 10100 pps
peak-burst 150 packets conform-action transmit
Router(config-cmap)# exit
Router(config)# control-plane
Router(config-cp)# service-policy input copp-pps
Router(config-cp)# exit
```

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.

service-policy (control-plane)

To attach a policy map to a control plane for aggregate or distributed control plane services, use the **service-policy** command in control-plane configuration mode. To remove a service policy from a control plane, use the **no** form of this command.

service-policy {**input** | **output**} *policy-map-name*

no service-policy {**input** | **output**} *policy-map-name*

Syntax for Cisco 6500 Router, Cisco 7500 Series, Cisco 10720 Internet Router, and Cisco 10000 Series Router

service-policy input *policy-map-name*

no service-policy input *policy-map-name*

Syntax Description

input	Applies the specified service policy to packets that are entering the control plane.
output	Applies the specified service policy to packets that are exiting 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.

Command Default

No service policy is specified.

Command Modes

Control-plane configuration

Command History

Release	Modification
12.2(18)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T, and support for the **output** keyword was added.
12.0(29)S	This command was integrated into Cisco IOS Release 12.0(29)S.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(25)S	Support for the **output** keyword was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

After entering the **control-plane** command, use the **service-policy** command to configure a quality of service (QoS) policy. This policy is attached to the control plane interface for aggregate or distributed control plane services, and controls the number or rate of packets that are going to the process level.

When you configure output policing on control-plane traffic, using the **service-policy output** *policy-map-name* command, a router is automatically enabled to silently discard packets. Output policing is supported as follows:

- 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.
  - Cisco IOS Release 12.2(18)SXD1 and later Cisco IOS 12.2SX releases.
- Not supported for attaching a QoS policy for distributed control-plane services.
- Not supported on the Cisco 6500 router, Cisco 7500 series, Cisco 10720 Internet router, and Cisco 10000 series router.

The **service-policy output** command configures output policing, which is performed in silent mode to silently discard packets exiting from the control plane according to the attached QoS policy. Silent mode allows a router that is running Cisco IOS software to operate without sending any system messages. If a packet that is exiting from the control plane is discarded for output policing, you do not receive an error message.

Silent mode allows a router that is running Cisco IOS software to operate without sending any system messages. If a packet that is destined for the router is discarded for any reason, users will not receive an error message. Some events that will not generate error messages are as follows:

- 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

Examples

The following example shows how to configure trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 to 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-policy
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 aggregate control plane service for the active Route Processor.
Router(config)# control-plane
Router(config-cp)# service-policy input control-plane-policy
Router(config-cp)# exit
```

The next example shows how to configure trusted networks with source addresses 10.0.0.0 and 10.0.0.2 to receive Internet Control Message Protocol (ICMP) port-unreachable responses without constraint, while allowing all remaining ICMP port-unreachable to be dropped:

```
! Allow 10.0.0.0 trusted network traffic.
Router(config)# access-list 141 deny icmp host 10.0.0.0 255.255.255.224 any
port-unreachable
```

```
! Allow 10.0.0.2 trusted network traffic.
Router(config)# access-list 141 deny icmp host 10.0.0.2 255.255.255.224 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-policy
! Drop all traffic that matches the class "icmp-class."
Router(config-pmap)# class icmp-class
Router(config-pmap-c)# drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# control-plane
! Define aggregate control plane service for the active route processor.
Router(config-cp)# service-policy output control-plane-out-policy
Router(config-cp)# exit
```

Related Commands

Command	Description
control-plane	Enters control-plane configuration mode to apply a QoS policy to police traffic destined for the control plane.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
show policy-map control-plane	Displays the configuration of a class or all classes for the policy map attached to the control plane.

show policy-map control-plane

To display the configuration and statistics for a traffic class or all traffic classes in the policy maps attached to the control plane for aggregate and distributed control plane policing services, use the **show policy-map control-plane** command in privileged EXEC mode.

show policy-map control-plane [**type** *policy-type*] [**all** | **slot** *slot-number*] [**host** | **transit** | **cef-exception**] [{**input** | **output**} [**class** *class-name*]]

Syntax Description

type *policy-type*	(Optional) Specifies policy-map type for which you want statistics (for example, port-filter or queue-threshold).
all	(Optional) Displays information about all QoS policies used in aggregate and distributed CP services.
slot *slot-number*	(Optional) Displays information about the QoS policy used to perform distributed CP services on the specified line card.
host	(Optional) Displays policy-map and class-map statistics for the host subinterface.
transit	(Optional) Displays policy-map and class-map statistics for the transit subinterface.
cef-exception	(Optional) Displays policy-map and class-map statistics for the cef-exception subinterface.
input	(Optional) Displays statistics for the attached input policy.
output	(Optional) Displays statistics for the attached output policy. **Note** The **output** keyword is supported only in Cisco IOS Release 12.3(4)T and later Cisco IOS 12.3T releases.
class *class-name*	(Optional) Displays statistics for an individual traffic class.

Command Default

Information displays for all classes of the policy map of the control plane.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T, and support for the **output** keyword was added.
12.0(29)S	This command was integrated into Cisco IOS Release 12.0(29)S.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.0(30)S	The **slot** *slot-number* parameter was added to support distributed CP services.
12.4(4)T	Support was added for **the type** *policy-type* keyword and argument combination, and for the **host**, **transit**, and **cef-exception** keywords.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

The **show policy-map control-plane** command displays information for aggregate and distributed control-plane policing services, which manage the number or rate of CP packets sent to the process level of the Route Processor.

Information for distributed control-plane service is displayed for a specified line card. Distributed CP services are performed on a line card's distributed switch engine and manage CP traffic sent from all interfaces on the line card to the route processor, where aggregate CP services (for CP packets received from all line cards on the router) are performed.

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 called "class-default") to go through as is. Table 2 describes the significant fields shown in the display.

```
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
```

Table 2 show policy-map control-plane Field Descriptions

Field	Description
Fields Associated with Classes or Service Policies	
Service-policy input	Name of the input service policy that is applied to the control plane. (This field will also show the output service policy, if configured.)
Class-map	Class of traffic being displayed. Traffic is displayed for each configured class. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
offered rate	Rate, in kbps, at which packets are coming into the class.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.

Table 2 show policy-map control-plane Field Descriptions (continued)

Field	Description
Match	Match criteria for the specified class of traffic. For more information about the variety of match criteria options available, see the "Configuring the Modular Quality of Service Command-Line Interface" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*.
Fields Associated with Traffic Policing	
police	Indicates that the **police** command has been configured to enable traffic policing.
conformed	Displays the action to be taken on packets that conform to a specified rate. Displays the number of packets and bytes on which the action was taken.
exceeded	Displays the action to be taken on packets that exceed a specified rate. Displays the number of packets and bytes on which the action was taken.
violated	Displays the action to be taken on packets that violate a specified rate. Displays the number of packets and bytes on which the action was taken.

Cisco 10000 Series Router

The following example shows information for all QoS policies attached to the control plane. Table 2 describes the significant fields shown in the display.

```
Router# show policy-map control-plane all
Control Plane
Service-policy input: copp_policy
Class-map: mfib_224 (match-any)
2400000 packets, 340800000 bytes
5 minute offered rate 6894000 bps, drop rate 4313000 bps
Match: ip precedence 2
2400000 packets, 340800000 bytes
5 minute rate 6894000 bps
Police:
rate 5000 pps, 250 limit, peak-rate 7500 pps, 500 extended limit
conformed 600245 packets, 85234790 bytes; action: set-qos-transmit 2
exceeded 300247 packets, 42635074 bytes; action: transmit
violated 1499508 packets, 212930136 bytes; action: drop
Class-map: arp (match-any)
1200000 packets, 170400000 bytes
5 minute offered rate 3452000 bps, drop rate 2419000 bps
Match: protocol arp
1200000 packets, 170400000 bytes
5 minute rate 3452000 bps
Police:
rate 2500 pps, 250 limit, peak-rate 3000 pps, 500 extended limit
conformed 300248 packets, 42635216 bytes; action: transmit
exceeded 60250 packets, 8555500 bytes; action: transmit
violated 839502 packets, 119209284 bytes; action: drop
Class-map: fib_dest (match-any)
1200036 packets, 170402704 bytes
5 minute offered rate 3452000 bps, drop rate 870000 bps
Match: not protocol ipv6
1200036 packets, 170402704 bytes
5 minute rate 3452000 bps
```

```
Police:
rate 5000 pps, 250 limit, peak-rate 7500 pps, 500 extended limit
conformed 600255 packets, 85234909 bytes; action: transmit
exceeded 300245 packets, 42634721 bytes; action: transmit
violated 299536 packets, 42533074 bytes; action: drop
Class-map: class-default (match-any)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: any
0 packets, 0 bytes
5 minute rate 0 bps
```

Related Commands

Command	Description
control-plane	Enters control-plane configuration mode to apply a QoS policy to police traffic destined for the control plane.
service-policy (control-plane)	Attaches a policy map to the control plane for aggregate or distributed control-plane services.

Feature Information for Control Plane Policing

Table 2 lists the features in this module and provides links to specific configuration information.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 Feature Information for Control Plane Policing

Feature Name	Releases	Feature Information
Control Plane Policing	12.0(29)S 12.0(30)S 12.0(32)S 12.2(18)S 12.2(18)SXD1 12.2(27)SBC 12.3(4)T 12.3(7)T 12.2(31)SB2	The Control Plane Policing feature was introduced to allow users to configure a 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 DoS attacks. This feature was integrated into Cisco IOS Release 12.0(29)S. In 12.0(30)S, support for distributed control plane services on the Cisco 12000 series Internet router was added. In 12.0(32)S, support for aggregate control plane services on the Cisco 10720 Internet router was added. In 12.2(18)S, this feature was introduced. This feature was integrated into Cisco IOS Release 12.2(18)SXD1. This feature was integrated into Cisco IOS Release 12.2(27)SBC. This feature was integrated into Cisco IOS Release 12.3(4)T, and the output rate-limiting (silent mode operation) feature was added. In 12.3(7)T, 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. This feature was introduced on the Cisco 10000 series router and integrated into Cisco IOS Release 12.2(31)SB2.