Flexible Packet Matching

First Published: October 31, 2006
Last Updated: July 19, 2007

Flexible Packet Matching (FPM) is the next generation access control list (ACL) pattern matching tool, providing more thorough and customized packet filters. FPM enables users to match on arbitrary bits of a packet at an arbitrary depth in the packet header and payload. FPM removes constraints to specific fields that had limited packet inspection.

FPM is useful because it enables users to create their own stateless packet classification criteria and to define policies with multiple actions (such as drop, log, or send Internet Control Message Protocol [ICMP] unreachable[1]) to immediately block new viruses, worms, and attacks.

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 Flexible Packet Matching" section on page 87.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

Contents

1. Send ICMP unreachable is currently not supported on the Supervisor Engine 32 PISA.

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

Prerequisites for Flexible Packet Matching

- In Cisco IOS Release 12.4(4)T, FPM is available only in advanced security images.
- In Cisco IOS Release 12.2(18)ZY, FPM is also available in ipbase and ipservices images for the Supervisor Engine 32 Programmable Intelligent Services Accelerator (PISA) platform.
- Although access to an XML editor is not required, XML will ease the creation of protocol header description files (PHDFs).

Restrictions for Flexible Packet Matching

- FPM cannot be used to mitigate an attack that requires stateful classification.
- Because FPM is stateless, it cannot keep track of port numbers being used by protocols that dynamically negotiate ports. Thus, when using FPM, port numbers must be explicitly specified.
- FPM cannot perform IP fragmentation or TCP flow reassembly.
- FPM inspects only IPv4 unicast packets.
- FPM cannot classify packets with IP options.
- FPM does not support multicast packet inspection.
- FPM is not supported on tunnel and MPLS interfaces.
- FPM cannot be configured on FlexWAN cards.
- Noninitial fragments will not be matched by the FPM engine.
- Offset can be only a constant in a match start construct.
- FPM cannot match across packets.
- Mapping of FPM policies to control-plane is not supported.

Information About Flexible Packet Matching

Before configuring FPM, you should understand the following concept:

Flexible Packet Matching Functional Overview

FPM allows customers to create their own filtering policies that can immediately detect and block new viruses and attacks.

A filtering policy is defined via the following tasks:

- Load a PHDF (for protocol header field matching)
- Define a class map and define the protocol stack chain (traffic class)
- Define a service policy (traffic policy)
- Apply the service policy to an interface

Protocol Header Description File

Protocol headers are defined in separate files called PHDFs; the field names that are defined within the PHDFs are used for defining the packet filters. A PHDF is a file that allows the user to leverage the flexibility of XML to describe almost any protocol header. The important components of the PHDF are the version, the XML file schema location, and the protocol field definitions. The protocol field definitions name the appropriate field in the protocol header, allow for a comment describing the field, provide the location of the protocol header field in the header (the offset is relative to the start of the protocol header), and provide the length of the field. Users can choose to specify the measurement in bytes or in bits.

Note The total length of the header must be specified at the end of each PHDF.

Users can write their own custom PHDFs via XML for existing or proprietary protocols. However, the following standard PHDFs can also be loaded onto the router via the **load protocol** command: ip.phdf, ether.phdf, tcp.phdf, and udp.phdf.

Note Because PHDFs are defined via XML, they are not shown in a running configuration. However, you can use the **show protocol phdf** command to verify the loaded PHDF.

Standard PHDFs are available on Cisco.com at the following URL:
http://www.cisco.com/cgi-bin/tablebuild.pl/fpm

Filter Description

A filter description is a definition of a traffic class that can contain the header fields defined in a PHDF (using the **match field** command). If a PHDF is not loaded, the traffic class can be defined via the datagram header start (Layer 2) or the network header start (Layer 3) (using the **match start** command). If a PHDF has been loaded onto the router, the class specification begins with a list of the protocol headers in the packet.

A filter definition also includes the policy map; that is, after a class map has been defined, a policy map is needed to bind the match to an action. A policy map is an ordered set of classes and associated actions, such as drop, log, or send ICMP unreachable.

For information on how to configure a class map and a policy map for FPM, see the following section "How to Configure a Flexible Packet Matching Traffic Class and Traffic Policy."

Traffic Classification Definition Files (TCDFs) for the Flexible Packet Matching XML Configuration

FPM uses a traffic classification definition file (TCDF) to define policies that can block attacks on the network. Before Cisco IOS Release 12.4(6)T, FPM defined traffic classes (class maps), policies (policy maps), and service policies (attach policy maps to class maps) through the use of CLI commands. With TCDFs, FPM can use XML as an alternative to the CLI to define classes of traffic and specify actions to apply to the traffic classes. Traffic classification behavior is the same whether you create the behavior using a TCDF or configure it using CLI commands. Once a TCDF is created, it can be loaded on any FPM-enabled device in the network.

TCDF Image Restriction

TCDF is part of the FPM subsystem. FPM is not included in the Cisco 871 securityk9 image; therefore, TCDF parsing is not present in the Cisco 871 securityk9 image.

For more information on configuring FPM using TCDFs, see *Flexible Packet Matching XML Configuration*.

FPM on PISA Overview

The PISA functions as a network-processor based daughter card that is mounted on the Catalyst 6500 Supervisor. PISA provides a superset of the multilater switch feature card 2a (MSFC2a) capabilities. In addition to performing all of the same functions as the MSFC2a, PISA also provides a dedicated hardware to accelerate certain features, such as FPM.

FPM occurs before Network-Based Application Recognition (NBAR); thus, packets that are dropped by FPM are not processed by NBAR.

Logging FPM Activity

In software-based FPM logging, every flow is logged and aggregated statistics are provided for each flow. Logging every flow for FPM on PISA would overwhelm the CPU; thus, only selective packets are logged. That is, when a packet matches a policy that is to be logged or the first time, the packet is logged, time-stamped, and stored. For every subsequent packet that matches any policy with a log action, the packet is checked for the difference between the current time (which is clocked by the global timer) and the last time stamp. If the current time is greater than the last time stamp, the packet is logged and the "stamp time" is updated with the current time.

Memory Requirements

Note Because memory requirements vary among system configurations, the requirements listed in this document are estimates.

- PISA will support a maximum of 1024 interfaces; however, it is expected that no more than 256 interfaces will be configured with FPM.
- A maximum of 32 classes per policy map, and a total of 1024 classes globally, are supported.
- A maximum of eight filters (such as match entries) per class map are supported.

How to Configure a Flexible Packet Matching Traffic Class and Traffic Policy

This section contains the following procedures that should be followed when configuring a FPM traffic class and traffic policy within your network:

- Creating a Traffic Class for Flexible Packet Matching, page 5
- Creating a Traffic Policy for Flexible Packet Matching, page 7

Creating a Traffic Class for Flexible Packet Matching

Perform this task to create an FPM traffic class; that is, create a stateless packet classification criteria that, when used in conjunction with an appropriately defined policy, can mitigate network attacks.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **load protocol** *location*:*filename*
4. **class-map** [**type** {**stack** | **access-control**}] *class-map-name* [**match-all** | **match-any**]
5. **description** *character-string*
6. **match field** *protocol protocol-field* {**eq** [*mask*] | **neq** [*mask*] | **gt** | **lt** | **range** *range* | **regex** *string*} *value* [**next** *next-protocol*]
7. **match start** {**l2-start** | **l3-start**} **offset** *number* **size** *number* {**eq** | **neq** | **gt** | **lt** | **range** *range* | **regex** *string*} *value* [*value2*]
8. **exit**
9. **show class-map** [**type** {**stack** | **access-control**}] [*class-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	**load protocol** *location*:*filename* **Example:** `Router(config)# load protocol disk2:udp.phdf`	(Optional) Loads a PHDF onto a router. • The specified location must be local to the router. **Note** If a PHDF is not loaded, only the **match start** command can be used; that is, you cannot issue the **match field** command.

	Command or Action	Purpose
Step 4	**class-map** [**type** {**stack** | **access-control**}] *class-map-name* [**match-all** | **match-any**] **Example:** `Router(config)# class-map type access-control slammer match-all`	Creates a class map to be used for matching packets to a specified class and enters class-map configuration mode. • **type stack** —Enables FPM to determine the correct protocol stack in which to examine. • **type access-control**—Determines the exact pattern to look for in the protocol stack of interest. • *class-map-name*—Can be a maximum of 40 alphanumeric characters. • If **match-all** or **match-any** are not specified, traffic must match all the match criterion to be classified as part of the traffic class.
Step 5	**description** *character-string* **Example:** `Router(config-cmap)# description "match on slammer packets"`	(Optional) Adds a description to the class map.
Step 6	**match field** *protocol protocol-field* {**eq** [*mask*] | **neq** [*mask*] | **gt** | **lt** | **range** *range* | **regex** *string*} *value* [**next** *next-protocol*] **Example:** `Router(config-cmap)# match field udp dest-port eq 0x59A`	(Optional) Configures the match criteria for a class map on the basis of the fields defined in the PHDFs.
Step 7	**match start** {**l2-start** | **l3-start**} **offset** *number* **size** *number* {**eq** | **neq** | **gt** | **lt** | **range** *range* | **regex** *string*} *value* [*value2*] **Example:** `Router(config-cmap)# match start l3-start offset 224 size 4 eq 0x4011010`	(Optional) Configures the match criteria for a class map on the basis of the datagram header (Layer 2) or the network header (Layer 3).

Step 8	**exit**
	
	Example:
	`Router(config-cmap)# exit`
	
	Example:
	`Router(config)# exit`
		Exits class-map configuration mode and global configuration mode.

Step 9	**show class-map** [**type** {**stack** | **access-control**}] [*class-map-name*] **Example:** `Router# show class-map type access-control slammer`	(Optional) Displays all configured FPM class maps.

Troubleshooting Tips

To track all FPM events, issue the **debug fpm event** command.

The following sample output is from the **debug fpm event** command:

```
*Jun 21 09:22:21.607: policy-classification-inline(): matches class: class-default *Jun 21
09:22:21.607: packet-access-control(): policy-map: fpm-policy, dir: input, match. retval:
0x0, ip-flags: 0x80000000
```

What to Do Next

After you have defined at least one class map for your network, you must create a traffic policy and apply that policy to an interface as shown in the following task "Creating a Traffic Policy for Flexible Packet Matching."

Creating a Traffic Policy for Flexible Packet Matching

Perform this task to create an FPM traffic policy and apply the policy to a given interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** [**type access-control**] *policy-map-name*
4. **description** *character-string*
5. **class** *class-name* [**insert-before** *class-name*]
6. **drop**
7. **service-policy** *policy-map-name*
8. **exit**
9. **interface** *type name*
10. **service-policy** [**type access-control**] {**input** | **output**} *policy-map-name*
11. **exit**
12. **show policy-map interface** [**type access-control**] *interface-name* [**input** | **output**]

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	**policy-map** [**type access-control**] *policy-map-name* **Example:** `Router(config)# policy-map type access-control fpm-udp-policy`	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy and enters policy-map configuration mode.
Step 4	**description** *character-string* **Example:** `Router(config-pmap)# description "policy for UDP based attacks"`	(Optional) Adds a description to the policy map.
Step 5	**class** *class-name* [**insert-before** *class-name*] **Example:** `Router(config-pmap)# class slammer`	Specifies the name of a predefined traffic class, which was configured with the **class-map** command, used to classify traffic to the traffic policy. • **insert-before** *class-name*—Adds a class map to any location within the policy map. If this option is not issued, the class map is appended to the end of the policy map.
Step 6	**drop** **Example:** `Router(config-pmap)# drop`	(Optional) Configures a traffic class to discard packets belonging to a specific class. If this command is issued, note the following restrictions: • Discarding packets is the only action that can be configured in a traffic class. • When a traffic class is configured with the **drop** command, a "child" (nested) policy cannot be configured for this specific traffic class through the **service policy** command. • Discarding packets cannot be configured for the default class specified via the c**lass class-default** command.
Step 7	**service-policy** *policy-map-name* **Example:** `Router(config-pmap-c)# service policy fpm-udp-policy`	Creates hierarchical service policies.

Step 8	**exit**
	
	Example:
	`Router(config-pmap-c)# exit`
	
	Example:
	`Router(config-pmap)# exit`
		Exits policy-map class configuration mode and policy-map configuration mode.

Step 9	**interface** *type number* **Example:** `Router(config)# interface gigabitEthernet 0/1`	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 10	**service-policy** [**type access-control**] {**input** | **output**} *policy-map-name* **Example:** `Router(config-if)# service-policy type access-control input fpm-policy`	Specifies the type and the name of the traffic policy to be attached to the input or output direction of an interface.

Step 11	**exit**
	
	Example:
	`Router(config-if)# exit`
	
	Example:
	`Router(config)# exit`
		Exits interface configuration and global configuration modes.

Step 12	**show policy-map interface** [**type access-control**] *interface-name* [**input** | **output**] **Example:** `Router# show policy-map interface type access-control interface gigabit 0/1`	(Optional) Verifies the FPM configuration.

Configuration Examples for FPM Configuration

This section contains the following configuration examples:

Configuring FPM for Slammer Packets: Example

The following example shows how to define FPM traffic classes for slammer packets (UDP port 1434). The match criteria defined within the class maps is for slammer packets with an IP length not to exceed 404 bytes, UDP port 1434, and pattern 0x4011010 at 224 bytes from start of IP header. This example also shows how to define the service policy "fpm-policy" and apply it to the Gigabit Ethernet interface. Show commands have been issued to verify the FPM configuration. (Note that PHDFs are not displayed in show output because they are in XML format.)

```
Router(config)# load protocol disk2:ip.phdf
Router(config)# load protocol disk2:udp.phdf

Router(config)# class-map type stack match-all ip-udp
Router(config-cmap)# description "match UDP over IP packets"
Router(config-cmap)# match field ip protocol eq 0x11 next udp

Router(config)# class-map type access-control match-all slammer
Router(config-cmap)# description "match on slammer packets"
Router(config-cmap)# match field udp dest-port eq 0x59A
Router(config-cmap)# match field ip length eq 0x194
Router(config-cmap)# match start l3-start offset 224 size 4 eq 0x4011010
```

```
Router(config)# policy-map type access-control fpm-udp-policy
Router(config-pmap)# description "policy for UDP based attacks"
Router(config-pmap)# class slammer
Router(config-pmap-c)# drop


Router(config)# policy-map type access-control fpm-policy
Router(config-pmap)# description "drop worms and malicious attacks"
Router(config-pmap)# class ip-udp
Router(config-pmap-c)# service-policy fpm-udp-policy


Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy type access-control input fpm-policy


Router# show policy-map type access-control interface gigabit 0/1

GigabitEthernet0/1
Service-policy access-control input: fpm-policy
Class-map: ip-udp (match-all)
0 packets, 0 bytes
3 minute offered rate 0 bps
Match: field IP protocol eq 0x11 next UDP
Service-policy access-control : fpm-udp-policy
Class-map: slammer (match-all)
0 packets, 0 bytes
3 minute offered rate 0 bps, drop rate 0 bps
Match: field UDP dest-port eq 0x59A
Match: field IP length eq 0x194
Match: start l3-start offset 224 size 4 eq 0x4011010
drop
Class-map: class-default (match-any)
0 packets, 0 bytes
3 minute offered rate 0 bps, drop rate 0 bps
Match: any
Class-map: class-default (match-any)
0 packets, 0 bytes
3 minute offered rate 0 bps, drop rate 0 bps
Match: any

Router# show protocol phdf ip

Protocol ID: 1
Protocol name: IP
Description: Definition-for-the-IP-protocol
Original file name: disk2:ip.phdf
Header length: 20
Constraint(s):
Total number of fields: 12
Field id: 0, version, IP-version
Fixed offset. offset 0
Constant length. Length: 4
Field id: 1, ihl, IP-Header-Length
Fixed offset. offset 4
Constant length. Length: 4
Field id: 2, tos, IP-Type-of-Service
Fixed offset. offset 8
Constant length. Length: 8
Field id: 3, length, IP-Total-Length
Fixed offset. offset 16
Constant length. Length: 16
Field id: 4, identification, IP-Identification
```

```
Fixed offset. offset 32
Constant length. Length: 16
Field id: 5, flags, IP-Fragmentation-Flags
Fixed offset. offset 48
Constant length. Length: 3
Field id: 6, fragment-offset, IP-Fragmentation-Offset
Fixed offset. offset 51
Constant length. Length: l3
Field id: 7, ttl, Definition-for-the-IP-TTL
Fixed offset. offset 64
Constant length. Length: 8
Field id: 8, protocol, IP-Protocol
Fixed offset. offset 72
Constant length. Length: 8
Field id: 9, checksum, IP-Header-Checksum
Fixed offset. offset 80
Constant length. Length: 16
Field id: 10, source-addr, IP-Source-Address
Fixed offset. offset 96
Constant length. Length: 32
Field id: 11, dest-addr, IP-Destination-Address
Fixed offset. offset 128
Constant length. Length: 32

Router# show protocol phdf udp

Protocol ID: 3
Protocol name: UDP
Description: UDP-Protocol
Original file name: disk2:udp.phdf
Header length: 8
Constraint(s):
Total number of fields: 4
Field id: 0, source-port, UDP-Source-Port
Fixed offset. offset 0
Constant length. Length: 16
Field id: 1, dest-port, UDP-Destination-Port
Fixed offset. offset 16
Constant length. Length: 16
Field id: 2, length, UDP-Length
Fixed offset. offset 32
Constant length. Length: 16
Field id: 3, checksum, UDP-Checksum
Fixed offset. offset 48
Constant length. Length: 16
```

Configuring FPM for Blaster Packets: Example

The following example shows how to configure FPM for blaster packets. The class map contains the following match criteria: TCP port 135, 4444 or UDP port 69; and pattern 0x0030 at 3 bytes from start of IP header.

```
Router(config)# load protocol disk2:ip.phdf
Router(config)# load protocol disk2:tcp.phdf
Router(config)# load protocol disk2:udp.phdf

Router(config)# class-map type stack match-all ip-tcp
Router(config-cmap)# match field ip protocol eq 0x6 next tcp

Router(config)# class-map type stack match-all ip-udp
Router(config-cmap)# match field ip protocol eq 0x11 next udp
```

```
Router(config)# class-map type access-control match-all blaster1
Router(config-cmap)# match field tcp dest-port eq 135
Router(config-cmap)# match start l3-start offset 3 size 2 eq 0x0030

Router(config)# class-map type access-control match-all blaster2
Router(config-cmap)# match field tcp dest-port eq 4444
Router(config-cmap)# match start l3-start offset 3 size 2 eq 0x0030

Router(config)# class-map type access-control match-all blaster3
Router(config-cmap)# match field udp dest-port eq 69
Router(config-cmap)# match start l3-start offset 3 size 2 eq 0x0030

Router(config)# policy-map type access-control fpm-tcp-policy
Router(config-pmap)# class blaster1
Router(config-pmap-c)# drop
Router(config-pmap-c)# class blaster2
Router(config-pmap-c)# drop


Router(config)# policy-map type access-control fpm-udp-policy
Router(config-pmap)# class blaster3
Router(config-pmap-c)# drop


Router(config)# policy-map type access-control fpm-policy
Router(config-pmap)# class ip-tcp
Router(config-pmap-c)# service-policy fpm-tcp-policy
Router(config-pmap)# class ip-udp
Router(config-pmap-c)# service-policy fpm-udp-policy


Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy type access-control input fpm-policy
```

Configuring FPM for MyDoom Packets: Example

The following example shows how to configure FPM for MyDoom packets. The match criteria is as follows:

- 90 > IP length > 44
- pattern 0x47455420 at 40 bytes from start of IP header

  or

- IP length > 44
- pattern 0x6d3a3830 at 48 bytes from start of IP header
- pattern 0x47455420 at 40 bytes from start of IP header

```
Router(config)# load protocol disk2:ip.phdf
Router(config)# load protocol disk2:tcp.phdf

Router(config)# class-map type stack match-all ip-tcp
Router(config-cmap)# match field ip protocol eq 0x6 next tcp

Router(config)# class-map type access-control match-all mydoom1
Router(config-cmap)# match field ip length gt 44
Router(config-cmap)# match field ip length lt 90
Router(config-cmap)# match start l3-start offset 40 size 4 eq 0x47455420
```

```
Router(config)# class-map type access-control match-all mydoom2
Router(config-cmap)# match field ip length gt 44
Router(config-cmap)# match start l3-start offset 40 size 4 eq 0x47455420
Router(config-cmap)# match start l3-start offset 78 size 4 eq 0x6d3a3830

Router(config)# policy-map type access-control fpm-tcp-policy
Router(config-pmap)# class mydoom1
Router(config-pmap-c)# drop
Router(config-pmap-c)# class mydoom2
Router(config-pmap-c)# drop


Router(config)# policy-map type access-control fpm-policy
Router(config-pmap)# class ip-tcp
Router(config-pmap-c)# service-policy fpm-tcp-policy


Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy type access-control input fpm-policy
```

Additional References

The following sections provide references related to Flexible Packet Matching.

Related Documents

Related Topic	Document Title
Configuring FPM using traffic classification definition files (TCDFs).	*Flexible Packet Matching XML Configuration*, Cisco IOS Release 12.4(6)T
Additional configuration information for class maps and policy maps	The section "Modular Quality of Service Command-Line Interface" in the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4
Complete suite of QoS commands	*Cisco IOS Quality of Service Solutions Command Reference*, Release 12.4

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	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 Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Command Reference

This section documents only commands that are new or modified.

New Commands

- **debug fpm event**
- **description (class-map)**
- **load protocol**
- **match field**
- **match start**
- **show protocol phdf**

Modified Commands

- **class (policy-map)**
- **class-map**
- **policy-map**
- **service-policy**
- **show class-map**
- **show policy-map interface**

class (policy-map)

To specify the name of the class whose policy you want to create or change or to specify the default class (commonly known as the class-default class) before you configure its policy, use the **class** command in policy-map configuration mode. To remove a class from the policy map, use the **no** form of this command.

class {*class-name* | **class-default**} [**insert-before** *class-name*]

no class {*class-name* | **class-default**}

Syntax Description

class-name	Name of the class to be configured or whose policy is to be modified. The class name is used for both the class map and to configure a policy for the class in the policy map.
class-default	Specifies the default class so that you can configure or modify its policy.
insert-before *class-name*	(Optional) Adds a class map between any two existing class maps. Inserting a new class map between two existing class map provides more flexibility when modifying existing policy map configurations. Without this option, the class map is appended to the end of the policy map. This keyword is supported only on flexible packet matching (FPM) policies.

Command Default

No class is specified.

Command Modes

QoS policy-map configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.2(14)SX	Support for this command was introduced on Cisco 7600 routers.
12.2(17d)SXB	This command was implemented on the Cisco 7600 router and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXE	The **class-default** keyword was added to the Cisco 7600 router.
12.4(4)T	The **insert-before** *class-name* option was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was introduced on the PRE3 for the Cisco 10000 series router.
12.2(18)ZY	The **insert-before** *class-name* option was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).

Usage Guidelines

Policy Map Configuration Mode

Within a policy map, the **class** (policy-map) command can be used to specify the name of the class whose policy you want to create or change. First, the policy map must be identified.

To identify the policy map (and enter the required policy-map configuration mode), use the **policy-map** command before you use the **class** (policy-map) command. After you specify a policy map, you can configure policy for new classes or modify the policy for any existing classes in that policy map.

Class Characteristics

The class name that you specify in the policy map ties the characteristics for that class—that is, its policy—to the class map and its match criteria, as configured using the **class-map** command.

When you configure policy for a class and specify its bandwidth and attach the policy map to an interface, class-based weighted fair queueing (CBWFQ) determines if the bandwidth requirement of the class can be satisfied. If so, CBWFQ allocates a queue for the bandwidth requirement.

When a class is removed, available bandwidth for the interface is incremented by the amount previously allocated to the class.

The maximum number of classes that you can configure for a router—and, therefore, within a policy map—is 64.

Predefined Default Class

The **class-default** keyword is used to specify the predefined default class called class-default. The class-default class is the class to which traffic is directed if that traffic does not match any of the match criteria in the configured class maps.

Tail Drop or WRED

You can define a class policy to use either tail drop by using the **queue-limit** command or Weighted Random Early Detection (WRED) by using the **random-detect** command. When using either tail drop or WRED, note the following points:

- The **queue-limit** and **random-detect** commands cannot be used in the same class policy, but they can be used in two class policies in the same policy map.
- You can configure the **bandwidth** command when either the **queue-limit** command or the **random-detect** command is configured in a class policy. The **bandwidth** command specifies the amount of bandwidth allocated for the class.
- For the predefined default class, you can configure the **fair-queue** (class-default) command. The **fair-queue** command specifies the number of dynamic queues for the default class. The **fair-queue** command can be used in the same class policy as either the **queue-limit** command or the **random-detect** command. It cannot be used with the **bandwidth** command.

Cisco 10000 Series Router

The PRE2 allows you to configure 31 class queues in a policy map.

In a policy map, the PRE3 allows you to configure one priority level 1 queue, plus one priority level 2 queue, plus 12 class queues, plus one default queue.

Examples

The following example configures three class policies included in the policy map called policy1. Class1 specifies policy for traffic that matches access control list 136. Class2 specifies policy for traffic on interface ethernet101. The third class is the default class to which packets that do not satisfy configured match criteria are directed.

```
! The following commands create class-maps class1 and class2
! and define their match criteria:
class-map class1
 match access-group 136
class-map class2
 match input-interface ethernet101

! The following commands create the policy map, which is defined to contain policy
! specification for class1, class2, and the default class:
policy-map policy1

Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 2000
Router(config-pmap-c)# queue-limit 40

Router(config-pmap)# class class2
Router(config-pmap-c)# bandwidth 3000
Router(config-pmap-c)# random-detect
Router(config-pmap-c)# random-detect exponential-weighting-constant 10

Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 16
Router(config-pmap-c)# queue-limit 20
```

Class1 has these characteristics: A minimum of 2000 kbps of bandwidth is expected to be delivered to this class in the event of congestion, and the queue reserved for this class can enqueue 40 packets before tail drop is enacted to handle additional packets.

Class2 has these characteristics: A minimum of 3000 kbps of bandwidth is expected to be delivered to this class in the event of congestion, and a weight factor of 10 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop.

The default class has these characteristics: 16 dynamic queues are reserved for traffic that does not meet the match criteria of other classes whose policy is defined by the policy map called policy1, and a maximum of 20 packets per queue is enqueued before tail drop is enacted to handle additional packets.

Note When the policy map that contains these classes is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed, taking into account all class policies and Resource Reservation Protocol (RSVP), if configured.

The following example configures policy for the default class included in the policy map called policy8. The default class has these characteristics: 20 dynamic queues are available for traffic that does not meet the match criteria of other classes whose policy is defined by the policy map called policy8, and a weight factor of 14 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop.

```
Router(config)# policy-map policy8
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 20
Router(config-pmap-c)# random-detect exponential-weighting-constant 14
```

The following example configures policy for a class called acl136 included in the policy map called policy1. Class acl136 has these characteristics: a minimum of 2000 kbps of bandwidth is expected to be delivered to this class in the event of congestion, and the queue reserved for this class can enqueue 40 packets before tail drop is enacted to handle additional packets. Note that when the policy map that contains this class is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed, taking into account all class policies and RSVP, if configured.

```
Router(config)# policy-map policy1
Router(config-pmap)# class acl136
Router(config-pmap-c)# bandwidth 2000
Router(config-pmap-c)# queue-limit 40
```

The following example configures policy for a class called int101 included in the policy map called policy8. Class int101 has these characteristics: a minimum of 3000 kbps of bandwidth are expected to be delivered to this class in the event of congestion, and a weight factor of 10 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop. Note that when the policy map that contains this class is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed.

```
Router(config)# policy-map policy8
Router(config-pmap)# class int101
Router(config-pmap-c)# bandwidth 3000
Router(config-pmap-c)# random-detect exponential-weighting-constant 10
```

The following example configures policy for the class-default default class included in the policy map called policy1. The class-default default class has these characteristics: 10 hashed queues for traffic that does not meet the match criteria of other classes whose policy is defined by the policy map called policy1; and a maximum of 20 packets per queue before tail drop is enacted to handle additional enqueued packets.

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue
Router(config-pmap-c)# queue-limit 20
```

The following example configures policy for the class-default default class included in the policy map called policy8. The class-default default class has these characteristics: 20 hashed queues for traffic that does not meet the match criteria of other classes whose policy is defined by the policy map called policy8; and a weight factor of 14 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop.

```
Router(config)# policy-map policy8
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 20
Router(config-pmap-c)# random-detect exponential-weighting-constant 14
```

The following example shows how to configure FPM for blaster packets. The class map contains the following match criteria: TCP port 135, 4444 or UDP port 69; and pattern 0x0030 at 3 bytes from start of IP header.

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf

class-map type stack match-all ip-tcp
 match field ip protocol eq 0x6 next tcp

class-map type stack match-all ip-udp
 match field ip protocol eq 0x11 next udp

class-map type access-control match-all blaster1
```

```
 match field tcp dest-port eq 135
 match start 13-start offset 3 size 2 eq 0x0030

class-map type access-control match-all blaster2
 match field tcp dest-port eq 4444
Router(config-cmap)# match start 13-start offset 3 size 2 eq 0x0030

class-map type access-control match-all blaster3
 match field udp dest-port eq 69
 match start 13-start offset 3 size 2 eq 0x0030

policy-map type access-control fpm-tcp-policy
 class blaster1
 drop
 class blaster2
 drop


policy-map type access-control fpm-udp-policy
 class blaster3
 drop


policy-map type access-control fpm-policy
 class ip-tcp
 service-policy fpm-tcp-policy
 class ip-udp
 service-policy fpm-udp-policy


interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
class-map	Creates a class map to be used for matching packets to a specified class.
fair-queue (class-default)	Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
queue-limit	Specifies or modifies the maximum number of packets the queue can hold for a class policy configured in a policy map.
random-detect (interface)	Enables WRED or DWRED.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.

class-map

To create a class map to be used for matching packets to a specified class, use the **class-map** command in global configuration mode. To remove an existing class map from the router, use the **no** form of this command. The **class-map** command enters class-map configuration mode in which you can enter one of the **match** commands to configure the match criteria for this class.

Cisco 2600, 3660, 3845, 6500, 7200, 7401, and 7500 Series Routers

class-map [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging** *log-class*}] [**match-all** | **match-any**] *class-map-name*

no **class-map** [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging** *log-class*}] [**match-all** | **match-any**] *class-map-name*

Cisco 7600 Series Routers

class-map *class-map-name* [**match-all** | **match-any**]

no class-map *class-map-name* [**match-all** | **match-any**]

Syntax Description

type stack	(Optional) Enables flexible packet matching (FPM) functionality to determine the correct protocol stack to examine. If the appropriate protocol header description files (PHDFs) have been loaded onto the router (via the **load protocol** command), a stack of protocol headers can be defined so that the filter can determine which headers are present and in what order.
type access-control	(Optional) Determines the exact pattern to look for in the protocol stack of interest. **Note** You must specify a stack class map (via the **type stack** keywords) before you can specify an access-control class map (via the **type access-control** keywords).
type port-filter	(Optional) Creates a port-filter class map that enables the TCP/UDP port policing of control plane packets. When enabled, it provides filtering of traffic that is destined to specific ports on the control-plane host subinterface.
type queue-threshold	(Optional) Enables queue thresholding that limits the total number of packets for a specified protocol that are allowed in the control plane IP input queue. This feature applies only to the control-plane host subinterface.
type logging *log-class*	(Optional) Enables logging of packet traffic on the control plane. The *log-class* is the name of the log class. The name can be a maximum of 40 alphanumeric characters.
match-all	(Optional) Determines how packets are evaluated when multiple match criteria exist. Matches statements under this class map based on the logical AND function. One statement and another are accepted. If you do not specify the **match-all** or **match-any** keyword, the default keyword is **match-all**.

match-any	(Optional) Determines how packets are evaluated when multiple match criteria exist. Matches statements under this class map based on the logical OR function. One statement or another is accepted. If you do not specify the **match-any** or **match-all** keyword, the default keyword is **match-all**.
class-map-name	Name of the class for the class map. The name can be a maximum of 40 alphanumeric characters. The class name is used for both the class map and to configure a policy for the class in the policy map.

Command Default

No class map is configured by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.2(14)SX	Support for this command was introduced on Cisco 7600 series routers.
12.2(17d)SXB	This command was implemented on the Cisco 7600 series routers and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(4)T	The **type stack** and **type access-control** keywords were added to support FPM. The **type port-filter** and **type queue-threshold** keywords were added to support Control Plane Protection.
12.4(6)T	The **type logging** keyword was added to support control plane packet logging.
12.2(18)ZY	The **type stack** and **type access-control** keywords were integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA)

Usage Guidelines

Cisco 2600, 3660, 3845, 6500, 7200, 7401, and 7500 Series Routers

Use the **class-map** command to specify the class that you will create or modify to meet the class-map match criteria. This command enters class-map configuration mode in which you can enter one of the **match** commands to configure the match criteria for this class. Packets that arrive at either the input interface or the output interface (determined by how the **service-policy** command is configured) are checked against the match criteria configured for a class map to determine if the packets belong to that class.

When configuring a class map, you can use one or more **match** commands to specify match criteria. For example, you can use the **match access-group** command, the **match protocol** command, or the **match input-interface** command. The **match** commands vary according to the Cisco IOS release. For more information about match criteria and **match** commands, see the "Modular Quality of Service Command-Line Interface (CLI) (MQC)" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Cisco 7600 Series Routers

You apply the **class-map** command and its subcommands on a per-interface basis to define packet classification, marking, aggregate, and flow policing as part of a globally named service policy.

You can attach a service policy to an EtherChannel. Do not attach a service policy to a port that is a member of an EtherChannel.

After you are in class-map configuration mode, the following configuration commands are available:

- **exit**—Used to exit from class-map configuration mode.
- **no**—Used to remove a match statement from a class map.
- **match**—Used to configure classification criteria. The following optional **match** subcommands are available:
  - **access-group** {*acl-index* | *acl-name*}
  - **ip** {**dscp** | **precedence**} *value1 value2 ... value8*

The following subcommands appear in the CLI help but are not supported on LAN interfaces or WAN interfaces on the Optical Service Modules (OSMs):

- **input-interface** {*interface-type interface-number* | **null** *number* | **vlan** *vlan-id*}
- **protocol** *link-type*
- **destination-address mac** *mac-address*
- **source-address mac** *mac-address*

OSMs are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

Policy Feature Card (PFC) QoS does not support the following commands:

- **input-interface** {*interface-type interface-number* | **null** *number* | **vlan** *vlan-id*}
- **protocol** *link-type*
- **destination-address mac** *mac-address*
- **source-address mac** *mac-address*
- **qos-group** *group-value*

If you enter these subcommands, PFC QoS does not detect the unsupported keywords until you attach a policy map to an interface. When you try to attach the policy map to an interface, you get an error message. For additional information, see the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide* and the *Cisco IOS Release 12.2 Command Reference* publications.

After you have configured the class-map name and are in class-map configuration mode, you can enter the **match access-group** and **match ip dscp** subcommands. The syntax for these subcommands is as follows:

match [[**access-group** {*acl-index* | *acl-name*}] | [**ip** {**dscp** | **precedence**} *value*]]

See Table 1 for a syntax description of the **match** subcommands.

Table 1 match Syntax Description

Optional Subcommand	Description
access-group *acl-index* | *acl-name*	(Optional) Specifies the access list index or access list names; valid access list index values are from 1 to 2699.
access-group *acl-name*	(Optional) Specifies the named access list.

Table 1 match Syntax Description (continued)

Optional Subcommand	Description
ip dscp *value1 value2 ... value8*	(Optional) Specifies the IP DSCP values to match; valid values are from 0 to 63. You can enter up to 8 DSCP values and separate each value with one white space.
ip precedence *value1 value2 ... value8*	(Optional) Specifies the IP precedence values to match; valid values are from 0 to 7. You can enter up to 8 precedence values and separate each value with one white space.

Examples

The following example specifies class101 as the name of a class, and it defines a class map for this class. The class called class101 specifies policy for traffic that matches access control list 101.

```
Router(config)# class-map class101
Router(config-cmap)# match access-group 101
```

The following example shows how to define FPM traffic classes for slammer and UDP packets. The match criteria defined within the class maps are for slammer and UDP packets with an IP length not to exceed 404 bytes, UDP port 1434, and pattern 0x4011010 at 224 bytes from the start of the IP header.

```
Router(config)# load protocol disk2:ip.phdf
Router(config)# load protocol disk2:udp.phdf

Router(config)# class-map type stack match-all ip-udp
Router(config-cmap)# description "match UDP over IP packets"
Router(config-cmap)# match field ip protocol eq 0x11 next udp

Router(config)# class-map type access-control match-all slammer
Router(config-cmap)# description "match on slammer packets"
Router(config-cmap)# match field udp dest-port eq 0x59A
Router(config-cmap)# match field ip length eq 0x194
Router(config-cmap)# match start 13-start offset 224 size 4 eq 0x4011010
```

The following example shows how to configure a port-filter policy to drop all traffic that is destined to closed or "nonlistened" ports except SNMP.

```
Router(config)# class-map type port-filter pf-class
Router(config-cmap)# match not port udp 123
Router(config-cmap)# match closed-ports
Router(config-cmap)# exit
Router(config)# policy-map type port-filter pf-policy
Router(config-pmap)# class pf-class
Router(config-pmap-c)# drop
Router(config-pmap-c)# end
```

The following example shows how to access the **class-map** commands and subcommands, configure a class map named ipp5, and enter a match statement for IP precedence 5:

```
Router(config)# class-map ipp5
Router(config-cmap)# match ip precedence 5
```

Related Commands

Command	Description
class (policy-map)	Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.
class class-default	Specifies the default class for a service policy map.
match (**class-map**)	Configures the match criteria for a class map on the basis of port filter and/or protocol queue policies.
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match ip dscp	Identifies one or more DSCP, AF, and CS values as a match criterion
match mpls experimental	Configures a class map to use the specified EXP field value as a match criterion.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or virtual circuit (VC) or to an output interface or VC to be used as the service policy for that interface or VC.
show class-map	Displays class-map information.
show policy-map interface	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

debug fpm event

To display protocol information from the designated protocol header description field (PHDF), use the **debug fpm event** command in privileged EXEC mode. To disable debugging messages, use the **no** form of this command.

debug fpm event

no debug fpm event

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(18)ZY	This command was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).

Examples

The following sample output is from the **debug fpm event** command:

```
Router# debug fpm event

*Jun 21 09:22:21.607: policy-classification-inline(): matches class: class-default *Jun 21
09:22:21.607: packet-access-control(): policy-map: fpm-policy, dir: input, match. retval:
0x0, ip-flags: 0x80000000
```

description (class-map)

To add a description to the class map or the policy map, use the **description** command in class-map configuration or policy-map configuration mode. To remove the description from the class map or the policy map, use the **no** form of this command.

description *character-string*

no description

Syntax Description

character-string	Comment or a description that is added to the class map or the policy map. The character-string cannot exceed 161 characters.

Defaults

If this command is not issued, a description does not exist.

Command Modes

Class-map configuration

Policy-map configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(18)ZY	This command was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).

Usage Guidelines

The **description** command is meant solely as a comment to be put in the configuration to help you remember information about the class map or policy map, such as which packets are included within the class map.

Examples

The following example shows how to specify a description within the class map “ip-udp” and the policy map “fpm-policy”:

```
class-map type stack match-all ip-udp
 description “match UDP over IP packets”
 match field ip protocol eq 0x11 next udp
!
policy-map type access-control fpm-policy
 description “drop worms and malicious attacks”
 class ip-udp
 service-policy fpm-udp-policy
!
!
interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Create or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

load protocol

To load a protocol header description file (PHDF) onto a router, use the **load protocol** command in global configuration mode. To unload all protocols from a specified location or a single protocol, use the **no** form of this command.

load protocol *location*:*filename*

no load protocol {*location*:*filename* | *protocol-name*}

Syntax Description

location:*filename*	Location of the PHDF that is to be loaded onto the router. When used with the no version of this command, all protocols loaded from the specified filename will be unloaded. **Note** The location must be local to the router.
protocol-name	Unloads only the specified protocol. **Note** If you attempt to unload a protocol that is being referenced by a filter, you will receive an error.

Command Default

If this command is not issued, no PHDFs will be loaded onto the router.

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(18)ZY	This command was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).

Usage Guidelines

Flexible packet matching allows users to classify traffic on the basis of any portion of a packet header given the protocol field, length, and pattern. Protocol headers are defined in separate files called PHDFs; the field names that are defined within the PHDFs are used for defining the packet filters. A PHDF is a file that allows the user to leverage the flexibility of extensible markup language (XML) to describe almost any protocol header. The important components of the PHDF are the version, the XML file schema location, and the protocol field definitions. The protocol field definitions name the appropriate field in the protocol header, allow for a comment describing the field, provide the location of the protocol header field in the header (the offset is relative to the start of the protocol header), and provide the length of the field. Users can choose to specify the measurement in bytes or in bits.

Note The total length of the header must be specified at the end of each PHDF.

In case of a redundant setup, users should ensure all PHDFs that are used in the flexible packet matching configuration are present on the corresponding standby disk. If the PHDFs are not on standby disk, all flexible packet matching policies using the PHDFs will be broken.

Users can write their own custom PHDFs via XML. However, the following standard PHDFs can also be loaded onto the router: ip.phdf, ether.phdf, tcp.phdf, and udp.phdf.

Standard PHDFs are available on Cisco.com at the following URL:
http://www.cisco.com/cgi-bin/tablebuild.pl/fpm

Because PHDFs are defined via XML, they are not shown in a running configuration.

Issue the **load protocol** command to apply filters to a protocol by defining and loading a PHDF for that protocol header.

Examples

The following example shows how to configure FPM for blaster packets. The class map contains the following match criteria: TCP port 135, 4444 or UDP port 69; and pattern 0x0030 at 3 bytes from start of IP header.

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf

class-map type stack match-all ip-tcp
 match field ip protocol eq 0x6 next tcp

class-map type stack match-all ip-udp
 match field ip protocol eq 0x11 next udp

class-map type access-control match-all blaster1
 match field tcp dest-port eq 135
 match start 13-start offset 3 size 2 eq 0x0030

class-map type access-control match-all blaster2
 match field tcp dest-port eq 4444
 match start 13-start offset 3 size 2 eq 0x0030

class-map type access-control match-all blaster3
 match field udp dest-port eq 69
 match start 13-start offset 3 size 2 eq 0x0030

policy-map type access-control fpm-tcp-policy
 class blaster1
 drop
 class blaster2
 drop

policy-map type access-control fpm-udp-policy
 class blaster3
 drop

policy-map type access-control fpm-policy
 class ip-tcp
 service-policy fpm-tcp-policy
 class ip-udp
 service-policy fpm-udp-policy

interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

The following example is the XML setup for the PHDF “ip.phdf:”

```
<?xml version="1.0" encoding="UTF-8"?>
<phdf xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchem
aLocation="D:\harinadh\Doc\Projects\FPME\XML\ex.xsd">
<protocol name="ip" description="Definition-for-the-IP-protocol">
<field name="version" description="IP-version">
<offset type="fixed-offset" units="bits"> 0 </offset>
<length type="fixed" units="bits">4</length>
</field>
<field name="ihl" description="IP-Header-Length">
<offset type="fixed-offset" units="bits">4</offset>
<length type="fixed" units="bits">4</length>
</field>
<field name="tos" description="IP-Type-of-Service">
<offset type="fixed-offset" units="bits">8</offset>
<length units="bits" type="fixed">8</length>
</field>
<field name="length" description="IP-Total-Length">
<offset type="fixed-offset" units="bytes">2</offset>
<length type="fixed" units="bytes">2</length>
</field>
<field name="identification" description="IP-Identification">
<offset type="fixed-offset" units="bytes">4</offset>
<length type="fixed" units="bytes">2</length>
</field>
<field name="flags" description="IP-Fragmentation-Flags">
<offset type="fixed-offset" units="bytes">6</offset>
<length type="fixed" units="bits">3</length>
</field>
<field name="fragment-offset" description="IP-Fragmentation-Offset”>
<offset type="fixed-offset" units="bits">51</offset>
<length type="fixed" units="bits">13</length>
</field>
<field name="ttl" description="Definition-for-the-IP-TTL">
<offset type="fixed-offset" units="bytes">8</offset>
<length type="fixed" units="bytes">1</length>
</field>
<field name="protocol" description="IP-Protocol">
<offset type="fixed-offset" units="bytes">9</offset>
<length type="fixed" units="bytes">1</length>
</field>
<field name="checksum" description="IP-Header-Checksum">
<offset type="fixed-offset" units="bytes">10</offset>
<length type="fixed" units="bytes">2</length>
</field>
<field name="source-addr" description="IP-Source-Address">
<offset type="fixed-offset" units="bytes">12</offset>
<length type="fixed" units="bytes">4</length>
</field>
<field name="dest-addr" description="IP-Destination-Address">
<offset type="fixed-offset" units="bytes">16</offset>
<length type="fixed" units="bytes">4</length>
</field>
<headerlength type="fixed" value="20"></headerlength>
</protocol>
</phdf>
```

match field

To configure the match criteria for a class map on the basis of the fields defined in the protocol header description files (PHDFs), use the **match field** command in class-map configuration mode. To remove the specified match criteria, use the **no** form of this command.

match field *protocol protocol-field* {**eq** [*mask*] | **neq** [*mask*] | **gt** | **lt** | **range** *range* | **regex** *string*} *value* [**next** *next-protocol*]

no match field *protocol protocol-field* {**eq** [*mask*] | **neq** [*mask*] | **gt** | **lt** | **range** *range* | **regex** *string*} *value* [**next** *next-protocol*]

Syntax Description

protocol	Name of protocol whose PHDF has been loaded onto a router.
protocol field	Match criteria is based upon the specified field within the loaded protocol.
eq	Match criteria is met if the packet is equal to the specified value or mask.
neq	Match criteria is met if the packet is not equal to the specified value or mask.
mask *mask*	(Optional) Can be used when the **eq** or the **neq** keywords are issued.
gt	Match criteria is met if the packet does not exceed the specified value.
lt	Match criteria is met if the packet is less than the specified value.
range *range*	Match criteria is based upon a lower and upper boundary protocol field range.
regex *string*	Match criteria is based upon a string that is to be matched.
value	Value for which the packet must be in accordance with.
next *next-protocol*	Specify the next protocol within the stack of protocols that is to be used as the match criteria.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(18)ZY	This command was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).

Usage Guidelines

Before issuing the **match-field** command, you must load a PHDF onto the router via the **load protocol** command. Thereafter, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

Match criteria are defined via a start point, offset, size, value to match, and mask. A match can be defined on a pattern with any protocol field.

Examples

The following example shows how to configure FPM for blaster packets. The class map contains the following match criteria: TCP port 135, 4444 or UDP port 69; and pattern 0x0030 at 3 bytes from start of IP header.

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf

class-map type stack match-all ip-tcp
 match field ip protocol eq 0x6 next tcp

class-map type stack match-all ip-udp
 match field ip protocol eq 0x11 next udp

class-map type access-control match-all blaster1
 match field tcp dest-port eq 135
 match start 13-start offset 3 size 2 eq 0x0030

class-map type access-control match-all blaster2
 match field tcp dest-port eq 4444
 match start 13-start offset 3 size 2 eq 0x0030

class-map type access-control match-all blaster3
 match field udp dest-port eq 69
 match start 13-start offset 3 size 2 eq 0x0030

policy-map type access-control fpm-tcp-policy
 class blaster1
 drop
 class blaster2
 drop

policy-map type access-control fpm-udp-policy
 class blaster3
 drop

policy-map type access-control fpm-policy
 class ip-tcp
 service-policy fpm-tcp-policy
 class ip-udp
 service-policy fpm-udp-policy

interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
load protocol	Loads a PHDF onto a router.
match start	Configures the match criteria for a class map on the basis of the datagram header (Layer 2) or the network header (Layer 3).

match start

To configure the match criteria for a class map on the basis of the datagram header (Layer 2) or the network header (Layer 3), use the **match start** command in class-map configuration mode. To remove the specified match criteria, use the **no** form of this command.

match start {**l2-start** | **l3-start**} **offset** *number* **size** *number*
{**eq** | **neq** | **gt** | **lt** | **range** *range* | **regex** *string*} {*value* [*value2*] | [*string*]}

no match start {**l2-start** | **l3-start**} **offset** *number* **size** *number*
{**eq** | **neq** | **gt** | **lt** | **range** *range* | **regex** *string*} {*value* [*value2*] | [*string*]}

Syntax Description

l2-start	Match criterion starts from the datagram header.
l3-start	Match criterion starts from the network header.
offset *number*	Match criterion can be made according to any aribitrary offset.
size *number*	Number of bytes in which to match.
eq	Match criteria is met if the packet is equal to the specified value or mask.
neq	Match criteria is met if the packet is not equal to the specified value or mask.
mask	(Optional) Can be used when the **eq** or the **neq** keywords are issued.
gt	Match criteria is met if the packet is greater than the specified value.
lt	Match criteria is met if the packet is less than the specified value.
range *range*	Match critera is based upon a lower and upper boundary protocol field range.
regex *string*	Match critera is based upon a string that is to be matched.
value	Value for which the packet must be in accordance with.

Defaults

No match criteria are configured.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(18)ZY	This command was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).

Usage Guidelines

To the match criteria that is to be used for flexible packet matching, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. Thereafter, you can enter one of the following commands:

- **match-field** (which configures the match criteria for a class map on the basis of the fields defined in the protocol header description files [PHDFs])

- **match-start** (which can be used if a PHDF is not loaded onto the router)

Examples

The following example shows how to configure FPM for blaster packets. The class map contains the following match criteria: TCP port 135, 4444 or UDP port 69; and pattern 0x0030 at 3 bytes from start of IP header.

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf

class-map type stack match-all ip-tcp
 match field ip protocol eq 0x6 next tcp

class-map type stack match-all ip-udp
 match field ip protocol eq 0x11 next udp

class-map type access-control match-all blaster1
 match field tcp dest-port eq 135
 match start 13-start offset 3 size 2 eq 0x0030

class-map type access-control match-all blaster2
 match field tcp dest-port eq 4444
 match start 13-start offset 3 size 2 eq 0x0030

class-map type access-control match-all blaster3
 match field udp dest-port eq 69
 match start 13-start offset 3 size 2 eq 0x0030

policy-map type access-control fpm-tcp-policy
 class blaster1
 drop
 class blaster2
 drop

policy-map type access-control fpm-udp-policy
 class blaster3
 drop

policy-map type access-control fpm-policy
 class ip-tcp
 service-policy fpm-tcp-policy
 class ip-udp
 service-policy fpm-udp-policy

interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
load protocol	Loads a PHDF onto a router.
match field	Configures the match criteria for a class map on the basis of the fields defined in the PHDFs.

policy-map

To create or modify a policy map that can be attached to one or more interfaces to specify a service policy, use the **policy-map** command in global configuration mode. To delete a policy map, use the **no** form of this command. The **policy-map** command enters QoS policy-map configuration mode in which you can configure or modify the class policies for that policy map.

Supported Platforms Other Than Cisco 10000 Series Routers

policy-map [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging** *log-policy*}] *policy-map-name*

no policy-map [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging** *log-policy*}] *policy-map-name*

Cisco 10000 Series Router

policy-map [**type** {**control** | **service**}] *policy-map-name*

no policy-map [**type** {**control** | **service**}] *policy-map-name*

Syntax Description

type stack	(Optional) Determines the exact pattern to look for in the protocol stack of interest.
type access-control	(Optional) Enables the policy map for the flexible packet matching feature.
type port-filter	(Optional) Enables the policy map for the port-filter feature.
type queue-threshold	(Optional) Enables the policy map for the queue-threshold feature.
type logging	(Optional) Enables the policy map for the control-plane packet logging feature.
log-policy	Type of log policy for control-plane logging.
policy-map-name	Name of the policy map. The name can be a maximum of 40 alphanumeric characters.
type control	(Optional) Creates a control policy map.
type service	(Optional) Creates a service policy map.

Command Default

The default is no policy-map configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.4(4)T	The **type access-control** keywords were added to support flexible packet matching. The **type port-filter** and **type queue-threshold** keywords were added to support control-plane protection.

Release	Modification
12.4(6)T	The **type logging** keywords were added to support control-plane packet logging.
12.2(31)SB	The **type control** and **type service** keywords were added to support the Cisco 10000 series router.
12.2(18)ZY	The **type access-control** keywords were integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).

Usage Guidelines

Use the **policy-map** command to specify the name of the policy map to be created, added to, or modified before you configure policies for classes whose match criteria are defined in a class map. The **policy-map** command enters QoS policy-map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. You use the **class-map** and **match** commands to configure the match criteria for a class. Because you can configure a maximum of 64 class maps, no policy map can contain more than 64 class policies.

A single policy map can be attached to multiple interfaces concurrently. When you attempt to attach a policy map to an interface, the attempt is denied if the available bandwidth on the interface cannot accommodate the total bandwidth requested by class policies comprising the policy map. In this case, if the policy map is already attached to other interfaces, it is removed from them.

Whenever you modify class policy in an attached policy map, class-based weighted fair queueing (CBWFQ) is notified and the new classes are installed as part of the policy map in the CBWFQ system.

Class Queues (Cisco 10000 Series Routers Only)

The PRE2 allows you to configure 31 class queues in a policy map.

In a policy map, the PRE3 allows you to configure one priority level 1 queue, plus one priority level 2 queue, plus 12 class queues, plus one default queue.

Control Policies (Cisco 10000 Series Routers Only)

Control policies define the actions that your system will take in response to specified events and conditions.

A control policy is made of one or more control policy rules. A control policy rule is an association of a control class and one or more actions. The control class defines the conditions that must be met before the actions will be executed.

There are three steps involved in defining a control policy:

1. Create one or more control class maps, by using the **class-map type control** command.
2. Create a control policy map, using the **policy-map type control** command.

   A control policy map contains one or more control policy rules. A control policy rule associates a control class map with one or more actions. Actions are numbered and executed sequentially.
3. Apply the control policy map to a context, using the **service-policy type control** command.

Service Policies (Cisco 10000 Series Routers Only)

Service policy maps and service profiles contain a collection of traffic policies and other functionality. Traffic policies determine which functionality will be applied to which session traffic. A service policy map or service profile may also contain a network-forwarding policy, which is a specific type of traffic policy that determines how session data packets will be forwarded to the network.

Examples

The following example creates a policy map called policy1 and configures two class policies included in that policy map. The class policy called class1 specifies policy for traffic that matches access control list (ACL) 136. The second class is the default class to which packets that do not satisfy configured match criteria are directed.

```
! The following commands create class-map class1 and define its match criteria:
class-map class1
 match access-group 136

! The following commands create the policy map, which is defined to contain policy
! specification for class1 and the default class:
policy-map policy1

class class1
 bandwidth 2000
 queue-limit 40

class class-default
 fair-queue 16
 queue-limit 20
```

The following example creates a policy map called policy9 and configures three class policies to belong to that map. Of these classes, two specify policy for classes with class maps that specify match criteria based on either a numbered ACL or an interface name, and one specifies policy for the default class called class-default to which packets that do not satisfy configured match criteria are directed.

```
policy-map policy9

class acl136
 bandwidth 2000
 queue-limit 40

class ethernet101
 bandwidth 3000
 random-detect exponential-weighting-constant 10

class class-default
 fair-queue 10
 queue-limit 20
```

Examples for Cisco 10000 Series Routers Only

The following example shows the configuration of a control policy map named rule4. Control policy map rule4 contains one policy rule, which is the association of the control class named class3 with the action to authorize subscribers using the network access server (NAS) port ID. The **service-policy type control** command is used to apply the control policy map globally.

```
class-map type control match-all class3
 match access-type pppoe
 match domain cisco.com
 available nas-port-id
!
policy-map type control rule4
 class type control class3
```

```
  authorize nas-port-id
!
service-policy type control rule4
```

The following example shows the configuration of a service policy map named redirect-profile:

```
policy-map type service redirect-profile
 class type traffic CLASS-ALL
  redirect to group redirect-sg
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
class (policy-map)	Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.
class class-default	Specifies the default class whose bandwidth is to be configured or modified.
class-map	Creates a class map to be used for matching packets to a specified class.
fair-queue (class-default)	Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy.
queue-limit	Specifies or modifies the maximum number of packets that the queue can hold for a class policy configured in a policy map.
random-detect (interface)	Enables WRED or DWRED.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.
service-policy	Attaches a policy map to an input interface or VC or an output interface or VC to be used as the service policy for that interface or VC.

service-policy

To attach a policy map to an input interface, a virtual circuit (VC), an output interface, or to a VC that will be used as the service policy for the interface or VC, use the **service-policy** command in the appropriate configuration mode. To remove a service policy from an input or output interface or from an input or output VC, use the **no** form of this command.

service-policy [**type access-control**] {**input** | **output**} *policy-map-name*

no service-policy [**type access-control**] {**input** | **output**} *policy-map-name*

Cisco 7600 Series Routers

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

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

Cisco 10000 Series Routers

service-policy [**history** | {**input** | **output**} *policy-map-name* | **type control** *control-policy-name*]

no service-policy [**history** | {**input** | **output**} *policy-map-name* | **type control** *control-policy-name*]

Syntax Description

type access-control	Determines the exact pattern to look for in the protocol stack of interest.
input	Attaches the specified policy map to the input interface or input VC.
output	Attaches the specified policy map to the output interface or output VC.
policy-map-name	The 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.
history	Maintains a history of QoS metrics.
type control *control-policy-name*	Creates a Class–Based Policy Language (CPL) control policy map that is applied to a context.

Command Default

No service policy is specified.

A control policy is not applied to a context.

No policy map is attached.

Command Modes

Interface configuration
VC submode (for a standalone VC)
Bundle-VC configuration (for ATM VC bundle members)
PVC range subinterface configuration (for a range of ATM PVCs)
PVC-in-range configuration (for an individual PVC within a PVC range)
Map-class configuration (for Frame Relay VCs)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.0(17)SL	This command was implemented on the Cisco 10000 series routers.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(2)T	This command was modified to enable low latency queueing (LLQ) on Frame Relay VCs.
12.2(14)SX	Support for this command was implemented on Cisco 7600 series routers. This command was changed to support output policy maps.
12.2(15)BX	This command was implemented on the ESR–PRE2.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(2)T	This command was made available in the PVC range subinterface configuration mode and in the PVC-in-range configuration mode to extend policy map functionality on an ATM VC to the ATM VC range.
12.4(4)T	The **type stack** and the **type access-control** keywords were added to support flexible packet matching (FPM).
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.3(7)XI2	This command was modified to support PVC range configuration mode and PVC-in-range configuration mode for ATM VCs on the Cisco 10000 series router and the Cisco 7200 series router.
12.2(18)ZY	The **type stack** and the **type access-control** keywords were integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).

Usage Guidelines

You can attach a single policy map to one or more interfaces or to one or more VCs to specify the service policy for those interfaces or VCs.

Currently a service policy specifies class-based weighted fair queueing (CBWFQ). The class policies that comprise the policy map are then applied to packets that satisfy the class map match criteria for the class.

To successfully attach a policy map to an interface or ATM VC, the aggregate of the configured minimum bandwidths of the classes that make up the policy map must be less than or equal to 75 percent of the interface bandwidth or the bandwidth allocated to the VC.

To enable Low Latency Queuing (LLQ) for Frame Relay (priority queueing [PQ]/CBWFQ), you must first enable Frame Relay Traffic Shaping (FRTS) on the interface using the **frame-relay traffic-shaping** command in interface configuration mode. You then attach an output service policy to the Frame Relay VC using the **service-policy** command in map-class configuration mode.

For a policy map to be successfully attached to an interface or ATM VC, the aggregate of the configured minimum bandwidths of the classes that make up the policy map must be less than or equal to 75 percent of the interface bandwidth or the bandwidth allocated to the VC. For a Frame Relay VC, the total amount

of bandwidth allocated must not exceed the minimum committed information rate (CIR) configured for the VC less any bandwidth reserved by the **frame-relay voice bandwidth** or **frame-relay ip rtp priority** map-class commands. If not configured, the minimum CIR defaults to half of the CIR.

Configuring CBWFQ on a physical interface is only possible if the interface is in the default queueing mode. Serial interfaces at E1 (2.048 Mbps) and below use WFQ by default. Other interfaces use FIFO by default. Enabling CBWFQ on a physical interface overrides the default interface queueing method. Enabling CBWFQ on an ATM permanent virtual circuit (PVC) does not override the default queueing method.

When you attach a service policy with CBWFQ enabled to an interface, commands related to fancy queueing such as those pertaining to fair queueing, custom queueing, priority queueing, and Weighted Random Early Detection (WRED) are available using the modular quality of service command line interface (MQC). However, you cannot configure these features directly on the interface until you remove the policy map from the interface.

You can modify a policy map attached to an interface or VC, changing the bandwidth of any of the classes that comprise the map. Bandwidth changes that you make to an attached policy map are effective only if the aggregate of the bandwidth amounts for all classes comprising the policy map, including the modified class bandwidth, is less than or equal to 75 percent of the interface bandwidth or the VC bandwidth. If the new aggregate bandwidth amount exceeds 75 percent of the interface bandwidth or VC bandwidth, the policy map is not modified.

After you apply the **service-policy** command to set a class of service (CoS) bit to an Ethernet interface, the policy is set in motion as long as there is a subinterface that is performing 8021.Q or Inter-Switch Link (ISL) trunking. Upon reload, however, the service policy is removed from the configuration due to the following error message:

```
Process 'set' action associated with class-map voip failed: Set cos supported only with
IEEE 802.1Q/ISL interfaces.
```

Cisco 10000 Series Router Usage Guidelines

The Cisco 10000 series router does not support applying class-based weighted fair queuing (CBWFQ) policies to unspecified bit rate (UBR) VCs.

To successfully attach a policy map to an interface or a VC, the aggregate of the configured minimum bandwidths of the classes comprising the policy map must be less than or equal to 99 percent of the interface bandwidth or the bandwidth allocated to the VC. If you attempt to attach a policy map to an interface when the sum of the bandwidth assigned to classes is greater than 99 percent of the available bandwidth, the router logs a warning message and does not allocate the requested bandwidth to all of the classes. If the policy map is already attached to other interfaces, it is removed from them.

The total bandwidth is the speed (rate) of the ATM layer of the physical interface. The router converts the minimum bandwidth that you specify to the nearest multiple of 1/255 (ESR-PRE1) or 1/65535 (ESR-PRE2) of the interface speed. When you request a value that is not a multiple of 1/255 or 1/65535, the router chooses the nearest multiple.

The bandwidth percentage is based on the interface bandwidth. In a hierarchical policy, the bandwidth percentage is based on the nearest parent shape rate.

By default, a minimum bandwidth guaranteed queue has buffers for up to 50 milliseconds of 256-byte packets at line rate, but not less than 32 packets.

For Cisco IOS Release 12.0(22)S and later releases, to enable LLQ for Frame Relay (priority queueing (PQ)/CBWFQ) on the Cisco 10000 series router, first create a policy map and then assign priority to a defined traffic class using the **priority** command. For example, the following sample configuration shows how to configure a priority queue with a guaranteed bandwidth of 8000 kbps. In the example, the

Business class in the policy map named Gold is configured as the priority queue. The Gold policy also includes the Non-Business class with a minimum bandwidth guarantee of 48 kbps. The Gold policy is attached to serial interface 2/0/0 in the outbound direction.

```
class-map Business
 match ip precedence 3
policy-map Gold
 class Business
  priority
  police 8000
 class Non-Business
  bandwidth 48
interface serial 2/0/0
 frame-relay encapsulation
 service-policy output Gold
```

On the PRE2, you can use the **service-policy** command to attach a QoS policy to an ATM subinterface or to a PVC. However, on the PRE3, you can attach a QoS policy only to a PVC.

Cisco 7600 Series Routers

The **output** keyword is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Do not attach a service policy to a port that is a member of an EtherChannel.

Although the CLI allows you to configure PFC-based QoS on the WAN ports on the OC-12 ATM OSMs and on the WAN ports on the channelized OSMs, PFC-based QoS is not supported on the WAN ports on these OSMs. OSMs are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

PFC QoS supports the optional **output** keyword only on VLAN interfaces. You can attach both an input policy map and an output-policy map to a VLAN interface.

Cisco 10000 Series Routers Control Policy Maps

A control policy map must be activated by applying it to a context. A control policy map can be applied to one or more of the following types of contexts:

1. Global
2. Interface
3. Subinterface
4. Virtual template
5. VC class
6. PVC

In general, control policy maps that are applied to more specific contexts take precedence over policy maps applied to more general contexts. In the list, the context types are numbered in order of precedence. For example, a control policy map that is applied to a permanent virtual circuit (PVC) takes precedence over a control policy map that is applied to an interface.

Control policies apply to all sessions hosted on the context. Only one control policy map can be applied to a given context.

Examples

The following example shows how to attach a policy map to a Fast Ethernet interface:

```
Router(config)# interface fastethernet 5/20
Router(config-if)# service-policy input pmap1
```

The following example shows how to attach the service policy map called policy9 to data-link connection identifier (DLCI) 100 on output serial interface 1 and enables LLQ for Frame Relay:

```
Router(config)# interface Serial1/0.1 point-to-point
Router(config-if)# frame-relay interface-dlci 100
Router(config-if)# class fragment
!
Router(config-if)# map-class frame-relay fragment
Router(config-if)# service-policy output policy9
```

The following example shows how to attach the service policy map called policy9 to input serial interface 1:

```
Router(config)# interface Serial1
Router(config-if)# service-policy input policy9
```

The following example attaches the service policy map called policy9 to the input PVC called cisco:

```
Router(config)# pvc cisco 0/34
Router(config)# service-policy input policy9
Router(config)# vbr-nt 5000 3000 500
Router(config)# precedence 4-7
```

The following example shows how to attach the policy called policy9 to output serial interface 1 to specify the service policy for the interface and enable CBWFQ on it:

```
Router(config)# interface serial1
Router(config-if)# service-policy output policy9
```

The following example attaches the service policy map called policy9 to the output PVC called cisco:

```
Router(config)# pvc cisco 0/5
Router(config)# service-policy output policy9
Router(config)# vbr-nt 4000 2000 500
Router(config)# precedence 2-3
```

Cisco 10000 Series Router Examples

The following example shows how to attach the service policy named user_policy to data link connection identifier (DLCI) 100 on serial subinterface 1/0/0.1 for outbound packets.

```
interface serial 1/0/0.1 point-to-point
 frame-relay interface-dlci 100
  service-policy output user_policy
```

Note You must be running Cisco IOS Release 12.0(22)S or later releases to attach a policy to a DLCI in this way. If you are running a release prior to Cisco IOS Release 12.0(22)S, attach the service policy as described in the previous configuration examples using the Frame Relay legacy commands.

The following example shows how to attach a QoS service policy named bronze to PVC 0/101 on the ATM subinterface 3/0/0.1 for inbound traffic.

```
interface atm 3/0/0
 atm pxf queuing
interface atm 3/0/0.1
 pvc 0/101
    service-policy input bronze
```

The following example shows how to attach a service policy named myQoS to the physical Gigabit Ethernet interface 1/0/0 for inbound traffic. VLAN 4, configured on the GigabitEthernet subinterface 1/0/0.3, inherits the service policy of the physical Gigabit Ethernet interface 1/0/0.

```
interface GigabitEthernet 1/0/0
 service-policy input myQoS
interface GigabitEthernet 1/0/0.3
 encapsulation dot1q 4
```

The following example shows how to apply the policy map named policy1 to the virtual template named virtual-template1 for all inbound traffic. In this example, the virtual template configuration also includes CHAP authentication and point-to-point protocol (PPP) authorization and accounting.

```
interface virtual-template1
 ip unnumbered Loopback1
 no peer default ip address
 ppp authentication chap vpn1
 ppp authorization vpn1
 ppp accounting vpn1
 service-policy policy1
```

The following example shows how to attach the service policy map called voice to ATM VC 2/0/0 within a PVC range of a total of 3 PVCs and enable PVC range configuration mode where a point-to-point subinterface is created for each PVC in the range. Each PVC created as part of the range has the voice service policy attached to it.

```
configure terminal
 interface atm 2/0/0
  range pvc 1/50 1/52
   service-policy input voice
```

The following example shows how to attach the service policy map called voice to ATM VC 2/0/0 within a PVC range, where every VC created as part of the range has the voice service policy attached to it. The exception is PVC 1/51, which is configured as an individual PVC within the range and has a different service policy called data attached to it in PVC-in-range configuration mode.

```
configure terminal
 interface atm 2/0/0
  range pvc 1/50 1/52
   service-policy input voice
  pvc-in-range 1/51
   service-policy input data
```

Related Commands

Command	Description
class-map	Accesses the QoS class map configuration mode to configure QoS class maps.
frame-relay ip rtp priority	Reserves a strict priority queue on a Frame Relay PVC for a set of RTP packet flows belonging to a range of UDP destination ports,

Command	Description
frame-relay traffic-shaping	Enables both traffic shaping and per-virtual-circuit queueing for all PVCs and SVCs on a Frame Relay interface.
frame-relay voice bandwidth	Specifies the amount of bandwidth to be reserved for voice traffic on a specific DLCI.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.

show class-map

To display all class maps and their matching criteria, use the **show class-map** command in user or privileged EXEC mode.

Cisco 3660, 3845, 6500, 7400, and 7500 Series Routers

show class-map [**type** {**stack** | **access-control**}] [*class-map-name*]

Cisco 7600 Series Routers

show class-map [*class-map-name*]

Syntax Description

type stack	(Optional) Displays class maps configured to determine the correct protocol stack in which to examine via flexible packet matching (FPM).
type access-control	(Optional) Displays class maps configured to determine the exact pattern to look for in the protocol stack of interest.
class-map-name	(Optional) Name of the class map. The class map name can be a maximum of 40 alphanumeric characters.

Command Default

Shows all class maps.

Command Modes

User or privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(13)T	This command was modified to display the Frame Relay data-link connection identifier (DLCI) number as a criterion for matching traffic inside a class map. In addition, this command was modified to display Layer 3 packet length as a criterion for matching traffic inside a class map.
12.2(14)SX	Support for this command was introduced on the Cisco 7600 series routers.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(4)T	The **type**, **stack**, and **access-control** keywords were added to support FPM.
12.2(18)ZY	The **type**, **stack**, and **access-control** keywords were integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).

Usage Guidelines

You can use the **show class-map** command to display all class maps and their matching criteria. If you enter the optional *class-map-name* argument, the specified class map and its matching criteria will be displayed.

Examples

In the following example, three class maps are defined. Packets that match access list 103 belong to class c3, IP packets belong to class c2, and packets that come through input Ethernet interface 1/0 belong to class c1. The output from the **show class-map** command shows the three defined class maps.

```
Router# show class-map

 Class Map c3
 Match access-group 103

 Class Map c2
 Match protocol ip

 Class Map c1
 Match input-interface Ethernet1/0
```

In the following example, a class map called "c1" has been defined, and the Frame Relay DLCI number of 500 has been specified as a match criterion:

```
Router# show class-map

class map match-all c1
   match fr-dlci 500
```

The following example shows how to display class-map information for all class maps:

```
Router# show class-map

 Class Map match-any class-default (id 0)
   Match any
 Class Map match-any class-simple (id 2)
   Match any
 Class Map match-all ipp5 (id 1)
   Match ip precedence 5

 Class Map match-all agg-2 (id 3)
```

The following example shows how to display class-map information for a specific class map:

```
Router# show class-map ipp5

 Class Map match-all ipp5 (id 1)
   Match ip precedence 5
```

Table 2 describes the significant fields shown in the display.

Table 2 show class-map Field Descriptions[1]

Field	Description
Class Map	Class of traffic being displayed. Output is displayed for each configured class map in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
Match	Match criteria specified for the class map. Criteria include the Frame Relay DLCI number, Layer 3 packet length, IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) groups.

1. A number in parentheses may appear next to the class-map name and match criteria information. The number is for Cisco internal use only and can be disregarded.

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match fr-dlci	Specifies the Frame Relay DLCI number as a match criterion in a class map.
match packet length (class-map)	Specifies and uses the length of the Layer 3 packet in the IP header as a match criterion in a class map.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

show policy-map interface

To display the statistics and the configurations of the input and output policies that are attached to an interface, use the **show policy-map interface** command in privileged EXEC mode.

Cisco 3660, 3845, 6500, 7200, 7400, and 7500 Series Routers

show policy-map interface [**type access-control**] *type number* [**vc** [*vpi*/] *vci*] [**dlci** *dlci*] [**input** | **output**]

ATM Shared Port Adapters

show policy-map interface *slot*/*subslot*/*port*[.*subinterface*]

Cisco 7600 Series Routers

show policy-map interface [*interface-type interface-number* | **null** *interface-number* | **vlan** *vlan-id*] [**input** | **output**]

Syntax Description

type access-control	(Optional) Displays class maps configured to determine the exact pattern to look for in the protocol stack of interest.
type	Type of interface or subinterface whose policy configuration is to be displayed.
number	Port, connector, or interface card number.
vc	(Optional) For ATM interfaces only, shows the policy configuration for a specified PVC.
vpi/	(Optional) ATM network virtual path identifier (VPI) for this permanent virtual circuit (PVC). On the Cisco 7200 and 7500 series routers, this value ranges from 0 to 255. The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0. The absence of both the forward slash (/) and a *vpi* value defaults the *vpi* value to 0. If this value is omitted, information for all virtual circuits (VCs) on the specified ATM interface or subinterface is displayed.
vci	(Optional) ATM network virtual channel identifier (VCI) for this PVC. This value ranges from 0 to 1 less than the maximum value set for this interface by the **atm vc-per-vp** command. Typically, the lower values 0 to 31 are reserved for specific traffic (F4 Operation, Administration, and Maintenance [OAM], switched virtual circuit [SVC] signaling, Integrated Local Management Interface [ILMI], and so on) and should not be used. The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only. The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0.
dlci	(Optional) Indicates a specific PVC for which policy configuration will be displayed.

dlci	(Optional) A specific data-link connection identifier (DLCI) number used on the interface. Policy configuration for the corresponding PVC will be displayed when a DLCI is specified.
input	(Optional) Indicates that the statistics for the attached input policy will be displayed.
output	(Optional) Indicates that the statistics for the attached output policy will be displayed.
slot	(ATM shared port adapter only) Chassis slot number. See the appropriate hardware manual for slot information. For SIPs, see the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.
/subslot	(ATM shared port adapter only) Secondary slot number on an SPA interface processor (SIP) where a SPA is installed. See the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on an SPA" topic in the platform-specific SPA software configuration guide for subslot information.
/port	(ATM shared port adapter only) Port or interface number. See the appropriate hardware manual for port information. For SPAs, see the corresponding "Specifying the Interface Address" topics in the platform-specific SPA software configuration guide.
.subinterface	(ATM shared port adapter only—Optional) Subinterface number. The number that precedes the period must match the number to which this subinterface belongs. The range is 1 to 4,294,967,293.
interface-type	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**.
interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
null *interface-number*	(Optional) Specifies the null interface; the valid value is 0.
vlan *vlan-id*	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

Defaults

This command displays the packet statistics of all classes that are configured for all service policies on the specified interface or subinterface or on a specific permanent virtual circuit (PVC) on the interface.

The absence of both the forward slash (**/**) and a *vpi* value defaults the *vpi* value to 0. If this value is omitted, information for all virtual circuits (VCs) on the specified ATM interface or subinterface is displayed.

ATM Shared Port Adapter

When used with the ATM shared port adapter, this command has no default behavior or values.

Command Modes

Privileged EXEC

ATM Shared Port Adapter

When used with the ATM shared port adapter, user EXEC or privileged EXEC.

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.0(28)S	This command was modified for the QoS: Percentage-Based Policing feature to include milliseconds when calculating the committed (conform) burst (bc) and excess (peak) burst (be) sizes.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(2)T	This command was modified to display information about the policy for all Frame Relay PVCs on the interface or, if a DLCI is specified, the policy for that specific PVC. This command was also modified to display the total number of packets marked by the quality of service (QoS) set action.
12.1(3)T	This command was modified to display per-class accounting statistics.
12.2(4)T	This command was modified for two-rate traffic policing. It now can display burst parameters and associated actions.
12.2(8)T	The command was modified for the Policer Enhancement—Multiple Actions feature and the WRED—Explicit Congestion Notification (ECN) feature. For the Policer Enhancement—Multiple Actions feature, the command was modified to display the multiple actions configured for packets conforming to, exceeding, or violating a specific rate. For the WRED—Explicit Congestion Notification (ECN) feature, the command displays ECN marking information.
12.2(13)T	The following modifications were made: • This command was modified for the Percentage-Based Policing and Shaping feature. • This command was modified for the Class-Based RTP and TCP Header Compression feature. • This command was modified as part of the Modular QoS CLI (MQC) Unconditional Packet Discard feature. Traffic classes in policy maps can now be configured to discard packets belonging to a specified class. • This command was modified to display the Frame Relay DLCI number as a criterion for matching traffic inside a class map. • This command was modified to display Layer 3 packet length as a criterion for matching traffic inside a class map. • This command was modified for the Enhanced Packet Marking feature. A mapping table (table map) can now be used to convert and propagate packet-marking values.
12.2(14)SX	Support for this command was introduced on Cisco 7600 series routers.
12.2(15)T	This command was modified to display Frame Relay voice-adaptive traffic-shaping information.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
12.3(14)T	This command was modified to display bandwidth estimation parameters.

Release	Modification
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE. This command was modified to display aggregate WRED statistics for the ATM shared port adapter. Note that changes were made to the syntax, defaults, and command modes. These changes are labelled "ATM Shared Port Adapter."
12.4(4)T	The **type access-control** keywords were added to support flexible packet matching.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB, and the following modifications were made: • This command was modified to display either legacy (undistributed processing) QoS or hierarchical queueing framework (HQF) parameters on Frame Relay interfaces or PVCs. • This command was modified to display information about Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunnel marking.
12.2(31)SB2	The following modifications were made: • This command was enhanced to display statistical information for each level of priority service configured and information about bandwidth-remaining ratios, and this command was implemented on the Cisco 10000 series router for the PRE3. • This command was modified to display statistics for matching packets on the basis of VLAN identification numbers. As of Cisco IOS Release 12.2(31)SB2, matching packets on the basis of VLAN identification numbers is supported on Cisco 10000 series routers only.
12.2(18)ZY	The **type access-control** keywords were integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).

Usage Guidelines

Cisco 3660, 3845, 6500, 7200, 7400, and 7500 Series Routers

The **show policy-map interface** command displays the packet statistics for classes on the specified interface or the specified PVC only if a service policy has been attached to the interface or the PVC.

The counters displayed after the **show policy-map interface** command is entered are updated only if congestion is present on the interface.

The **show policy-map interface** command displays policy information about Frame Relay PVCs only if Frame Relay Traffic Shaping (FRTS) is enabled on the interface.

The **show policy-map interface** command displays ECN marking information only if ECN is enabled on the interface.

To determine if shaping is active with HQF, check the queue depth field of the "(queue depth/total drops/no-buffer drops)" line in the **show policy-map interface** command output.

Cisco 7600 Series Routers

The **pos**, **atm**, and **ge-wan** keywords are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

Cisco 7600 series routers that are configured with a Supervisor Engine 2 display packet counters, and Cisco 7600 series routers that are configured with a Supervisor Engine 720 display byte counters.

The output does not display policed-counter information; 0 is displayed in its place (for example, 0 packets, 0 bytes). To display dropped and forwarded policed-counter information, enter the **show mls qos** command.

For OSM WAN interfaces only, if you configure policing within a policy map, the hardware counters are displayed and the class-default counters are not displayed. If you do not configure policing within a policy map, the class-default counters are displayed.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Examples

This section provides sample output from typical **show policy-map interface** commands. Depending upon the interface or platform in use and the options enabled, the output you see may vary slightly from the ones shown below.

Weighted Fair Queueing (WFQ) on Serial Interface: Example

The following sample output of the **show policy-map interface** command displays the statistics for the serial 3/1 interface, to which a service policy called mypolicy (configured as shown below) is attached. Weighted fair queueing (WFQ) has been enabled on this interface. See Table 3 for an explanation of the significant fields that commonly appear in the command output.

```
policy-map mypolicy
  class voice
    priority 128
  class gold
   bandwidth 100
  class silver
   bandwidth 80
   random-detect

Router# show policy-map interface serial3/1 output

 Serial3/1

  Service-policy output: mypolicy

    Class-map: voice (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 5
      Weighted Fair Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 128 (kbps) Burst 3200 (Bytes)
        (pkts matched/bytes matched) 0/0
        (total drops/bytes drops) 0/0

    Class-map: gold (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 2
      Weighted Fair Queueing
        Output Queue: Conversation 265
        Bandwidth 100 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: silver (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 1
      Weighted Fair Queueing
        Output Queue: Conversation 266
        Bandwidth 80 (kbps)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0
         exponential weight: 9
         mean queue depth: 0
```

```
class     Transmitted       Random drop      Tail drop    Minimum Maximum  Mark
          pkts/bytes        pkts/bytes       pkts/bytes    thresh  thresh  prob
0             0/0               0/0              0/0          20      40  1/10
1             0/0               0/0              0/0          22      40  1/10
2             0/0               0/0              0/0          24      40  1/10
3             0/0               0/0              0/0          26      40  1/10
4             0/0               0/0              0/0          28      40  1/10
5             0/0               0/0              0/0          30      40  1/10
6             0/0               0/0              0/0          32      40  1/10
7             0/0               0/0              0/0          34      40  1/10
rsvp          0/0               0/0              0/0          36      40  1/10

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

Traffic Shaping on Serial Interface: Example

The following sample output from the **show policy-map interface** command displays the statistics for the serial 3/2 interface, to which a service policy called p1 (configured as shown below) is attached. Traffic shaping has been enabled on this interface. See Table 3 for an explanation of the significant fields that commonly appear in the command output.

```
policy-map p1
  class c1
   shape average 320000

Router# show policy-map interface serial3/2 output

 Serial3/2

  Service-policy output: p1

    Class-map: c1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 0
      Traffic Shaping
        Target    Byte   Sustain   Excess    Interval  Increment Adapt
        Rate      Limit  bits/int  bits/int  (ms)      (bytes)   Active
        320000    2000   8000      8000      25        1000      -

        Queue     Packets   Bytes     Packets   Bytes     Shaping
        Depth                         Delayed   Delayed   Active
        0         0         0         0         0         no

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

Table 3 describes significant fields commonly shown in the displays. The fields in the table are grouped according to the relevant QoS feature.

Table 3 show policy-map interface Field Descriptions[1]

Field	Description
Fields Associated with Classes or Service Policies	
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets and bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
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.
Note In distributed architecture platforms (such as the Cisco 7500 series platform), the value of the transfer rate, calculated as the difference between the offered rate and the drop rate counters, can sporadically deviate from the average by up to 20 percent or more. This can occur while no corresponding burst is registered by independent traffic analyser equipment.	
Match	Match criteria specified for the class of traffic. Choices include criteria such as IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental (EXP) value, access groups, and QoS groups. For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Table 3 show policy-map interface Field Descriptions[1] (continued)

Field	Description
Fields Associated with Queueing (if Enabled)	
Output Queue	The weighted fair queueing (WFQ) conversation to which this class of traffic is allocated.
Bandwidth	Bandwidth, in either kbps or percentage, configured for this class and the burst size.
pkts matched/bytes matched	Number of packets (also shown in bytes) matching this class that were placed in the queue. This number reflects the total number of matching packets queued at any time. Packets matching this class are queued only when congestion exists. If packets match the class but are never queued because the network was not congested, those packets are not included in this total. However, if process switching is in use, the number of packets is always incremented even if the network is not congested.
depth/total drops/no-buffer drops	Number of packets discarded for this class. No-buffer indicates that no memory buffer exists to service the packet.
Fields Associated with Weighted Random Early Detection (WRED) (if Enabled)	
exponential weight	Exponent used in the average queue size calculation for a WRED parameter group.
mean queue depth	Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a fluctuating average. The minimum and maximum thresholds are compared against this value to determine drop decisions.
class	IP precedence level.
Transmitted pkts/bytes	Number of packets (also shown in bytes) passed through WRED and not dropped by WRED. **Note** If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped *after* the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as "no-buffer drops") are not taken into account by the WRED packet counter.
Random drop pkts/bytes	Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence level.
Tail drop pkts/bytes	Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence level.
Minimum thresh	Minimum threshold. Minimum WRED threshold in number of packets.
Maximum thresh	Maximum threshold. Maximum WRED threshold in number of packets.
Mark prob	Mark probability. Fraction of packets dropped when the average queue depth is at the maximum threshold.

Table 3 show policy-map interface Field Descriptions[1] (continued)

Field	Description
Fields Associated with Traffic Shaping (if Enabled)	
Target Rate	Rate used for shaping traffic.
Byte Limit	Maximum number of bytes that can be transmitted per interval. Calculated as follows: ((Bc+Be) /8) x 1
Sustain bits/int	Committed burst (Bc) rate.
Excess bits/int	Excess burst (Be) rate.
Interval (ms)	Time interval value in milliseconds (ms).
Increment (bytes)	Number of credits (in bytes) received in the token bucket of the traffic shaper during each time interval.
Queue Depth	Current queue depth of the traffic shaper.
Packets	Total number of packets that have entered the traffic shaper system.
Bytes	Total number of bytes that have entered the traffic shaper system.
Packets Delayed	Total number of packets delayed in the queue of the traffic shaper before being transmitted.
Bytes Delayed	Total number of bytes delayed in the queue of the traffic shaper before being transmitted.
Shaping Active	Indicates whether the traffic shaper is active. For example, if a traffic shaper is active, and the traffic being sent exceeds the traffic shaping rate, a “yes” appears in this field.

1. A number in parentheses may appear next to the service-policy output name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

Precedence-Based Aggregate WRED on ATM Shared Port Adapter: Example

The following sample output of the **show policy-map interface** command displays the statistics for the ATM shared port adapter interface 4/1/0.10, to which a service policy called prec-aggr-wred (configured as shown below) is attached. Because aggregate WRED has been enabled on this interface, the class through Mark Prob statistics are aggregated by subclasses. See Table 4 for an explanation of the significant fields that commonly appear in the command output.

```
Router(config)# policy-map prec-aggr-wred
Router(config-pmap)# class class-default
Router(config-pmap-c)# random-detect aggregate
Router(config-pmap-c)# random-detect precedence values 0 1 2 3 minimum thresh 10
maximum-thresh 100 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 4 5 minimum-thresh 40
maximum-thresh 400 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 6 minimum-thresh 60 maximum-thresh
600 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 7 minimum-thresh 70 maximum-thresh
700 mark-prob 10
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface ATM4/1/0.10 point-to-point
```

```
Router(config-if)# ip address 10.0.0.2 255.255.255.0
Router(config-if)# pvc 10/110
Router(config-if)# service-policy output prec-aggr-wred


Router# show policy-map interface atm4/1/0.10

 ATM4/1/0.10: VC 10/110 -

  Service-policy output: prec-aggr-wred

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        Exp-weight-constant: 9 (1/512)
        Mean queue depth: 0
        class       Transmitted     Random drop      Tail drop     Minimum   Maximum  Mark
    pkts/bytespkts/bytespkts/bytesthreshthreshprob

        0  1  2  3       0/0              0/0              0/0           10      100  1/10
        4  5             0/0              0/0              0/0           40      400  1/10
        6                0/0              0/0              0/0           60      600  1/10
        7                0/0              0/0              0/0           70      700  1/10
```

DSCP-Based Aggregate WRED on ATM Shared Port Adapter: Example

The following sample output of the **show policy-map interface** command displays the statistics for the ATM shared port adapter interface 4/1/0.11, to which a service policy called dscp-aggr-wred (configured as shown below) is attached. Because aggregate WRED has been enabled on this interface, the class through Mark Prob statistics are aggregated by subclasses. See Table 4 for an explanation of the significant fields that commonly appear in the command output.

```
Router(config)# policy-map dscp-aggr-wred
Router(config-pmap)# class class-default
Router(config-pmap-c)# random-detect dscp-based aggregate minimum-thresh 1 maximum-thresh
10 mark-prob 10
Router(config-pmap-c)# random-detect dscp values 0 1 2 3 4 5 6 7 minimum-thresh 10
maximum-thresh 20 mark-prob 10
Router(config-pmap-c)# random-detect dscp values 8 9 10 11 minimum-thresh 10
maximum-thresh 40 mark-prob 10
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface ATM4/1/0.11 point-to-point
Router(config-subif)# ip address 10.0.0.2 255.255.255.0
Router(config-subif)# pvc 11/101
Router(config-subif)# service-policy output dscp-aggr-wred

Router# show policy-map interface a4/1/0.11

 ATM4/1/0.11: VC 11/101 -

  Service-policy output: dscp-aggr-wred

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

```
Match: any
  Exp-weight-constant: 0 (1/1)
  Mean queue depth: 0
  class       Transmitted     Random drop      Tail drop     Minimum   Maximum  Mark
            pkts/bytespkts/bytespkts/bytesthreshthreshprob
  default          0/0               0/0              0/0           1      10  1/10
  0  1  2  3
  4  5  6  7       0/0               0/0              0/0          10      20  1/10
  8  9  10 11      0/0               0/0              0/0          10      40  1/10
```

Table 4 describes the significant fields shown in the display when aggregate WRED is configured for an ATM shared port adapter.

Table 4 show policy-map interface Field Descriptions—Configured for Aggregate WRED on ATM Shared Port Adapter

Field	Description
exponential weight	Exponent used in the average queue size calculation for a Weighted Random Early Detection (WRED) parameter group.
mean queue depth	Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a fluctuating average. The minimum and maximum thresholds are compared against this value to determine drop decisions.
Note When Aggregate Weighted Random Early Detection (WRED) is enabled, the following WRED statistics will be aggregated based on their subclass (either their IP precedence or differentiated services code point (DSCP) value).	
class	IP precedence level or differentiated services code point (DSCP) value.
Transmitted pkts/bytes	Number of packets (also shown in bytes) passed through WRED and not dropped by WRED. **Note** If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped *after* the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as "no-buffer drops") are not taken into account by the WRED packet counter.
Random drop pkts/bytes	Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence level or DSCP value.
Tail drop pkts/bytes	Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence level or DSCP value.
Minimum thresh	Minimum threshold. Minimum WRED threshold in number of packets.
Maximum thresh	Maximum threshold. Maximum WRED threshold in number of packets.
Mark prob	Mark probability. Fraction of packets dropped when the average queue depth is at the maximum threshold.

Frame Relay Voice-Adaptive Traffic-Shaping: Example

The following sample output shows that Frame Relay voice-adaptive traffic shaping is currently active and has 29 seconds left on the deactivation timer. With traffic shaping active and the deactivation time set, this means that the current sending rate on DLCI 201 is minCIR, but if no voice packets are detected for 29 seconds, the sending rate will increase to CIR.

```
Router# show policy interface Serial3/1.1

 Serial3/1.1:DLCI 201 -

  Service-policy output:MQC-SHAPE-LLQ1

    Class-map:class-default (match-any)
      1434 packets, 148751 bytes
      30 second offered rate 14000 bps, drop rate 0 bps
      Match:any
      Traffic Shaping
           Target/Average   Byte   Sustain   Excess    Interval  Increment
             Rate           Limit  bits/int  bits/int  (ms)      (bytes)
            63000/63000     1890   7560      7560      120       945

        Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
        Active Depth                         Delayed   Delayed   Active
        BECN   0         1434      162991    26        2704      yes
        Voice Adaptive Shaping active, time left 29 secs
```

Table 5 describes the significant fields shown in the display. Significant fields that are not described in Table 5 are described in Table 3, "show policy-map interface Field Descriptions."

Table 5 show policy-map interface Field Descriptions—Configured for Frame Relay Voice-Adaptive Traffic Shaping

Field	Description
Voice Adaptive Shaping active/inactive	Indicates whether Frame Relay voice-adaptive traffic shaping is active or inactive.
time left	Number of seconds left on the Frame Relay voice-adaptive traffic shaping deactivation timer.

Two-Rate Traffic Policing: Example

The following is sample output from the **show policy-map interface** command when two-rate traffic policing has been configured. In the example below, 1.25 Mbps of traffic is sent ("offered") to a policer class.

```
Router# show policy-map interface serial3/0

 Serial3/0

  Service-policy output: policy1

   Class-map: police (match all)
    148803 packets, 36605538 bytes
    30 second offered rate 1249000 bps, drop rate 249000 bps
    Match: access-group 101
    police:
     cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
     conformed 59538 packets, 14646348 bytes; action: transmit
     exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
     violated 29731 packets, 7313826 bytes; action: drop
     conformed 499000 bps, exceed 500000 bps violate 249000 bps
```

```
   Class-map: class-default (match-any)
    19 packets, 1990 bytes
    30 seconds offered rate 0 bps, drop rate 0 bps
    Match: any
```

The two-rate traffic policer marks 500 kbps of traffic as conforming, 500 kbps of traffic as exceeding, and 250 kbps of traffic as violating the specified rate. Packets marked as conforming will be sent as is, and packets marked as exceeding will be marked with IP Precedence 2 and then sent. Packets marked as violating the specified rate are dropped.

Table 6 describes the significant fields shown in the display.

Table 6 show policy-map interface Field Descriptions—Configured for Two-Rate Traffic Policing

Field	Description
police	Indicates that the **police** command has been configured to enable traffic policing. Also, displays the specified CIR, conform burst size, peak information rate (PIR), and peak burst size used for marking packets.
conformed	Displays the action to be taken on packets conforming 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 exceeding 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 violating a specified rate. Displays the number of packets and bytes on which the action was taken.

Multiple Traffic Policing Actions: Example

The following is sample output from the **show policy-map** command when the Policer Enhancement—Multiple Actions feature has been configured. The sample output from the **show policy-map interface** command displays the statistics for the serial 3/2 interface, to which a service policy called “police” (configured as shown below) is attached.

```
policy-map police
  class class-default
   police cir 1000000 pir 2000000
     conform-action transmit
     exceed-action set-prec-transmit 4
     exceed-action set-frde-transmit
     violate-action set-prec-transmit 2
     violate-action set-frde-transmit

Router# show policy-map interface serial3/2

Serial3/2: DLCI 100 -

Service-policy output: police

    Class-map: class-default (match-any)
      172984 packets, 42553700 bytes
      5 minute offered rate 960000 bps, drop rate 277000 bps
      Match: any
     police:
         cir 1000000 bps, bc 31250 bytes, pir 2000000 bps, be 31250 bytes
       conformed 59679 packets, 14680670 bytes; actions:
         transmit
exceeded 59549 packets, 14649054 bytes; actions:
         set-prec-transmit 4
         set-frde-transmit
```

```
    violated 53758 packets, 13224468 bytes; actions:
      set-prec-transmit 2
      set-frde-transmit
    conformed 340000 bps, exceed 341000 bps, violate 314000 bps
```

The sample output from **show policy-map interface** command shows the following:

- 59679 packets were marked as conforming packets (that is, packets conforming to the CIR) and were transmitted unaltered.
- 59549 packets were marked as exceeding packets (that is, packets exceeding the CIR but not exceeding the PIR). Therefore, the IP Precedence value of these packets was changed to an IP Precedence level of 4, the discard eligibility (DE) bit was set to 1, and the packets were transmitted with these changes.
- 53758 packets were marked as violating packets (that is, exceeding the PIR). Therefore, the IP Precedence value of these packets was changed to an IP Precedence level of 2, the DE bit was set to 1, and the packets were transmitted with these changes.

Note Actions are specified by using the *action* argument of the **police** command. For more information about the available actions, see the **police** command reference page.

Table 7 describes the significant fields shown in the display.

Table 7 show policy-map interface Field Descriptions—Configured for Multiple Traffic Policing Actions

Field	Description
police	Indicates that the **police** command has been configured to enable traffic policing. Also, displays the specified CIR, conform burst size (BC), PIR, and peak burst size (BE) used for marking packets.
conformed, packets, bytes, actions	Displays the number of packets (also shown in bytes) marked as conforming to a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately.
exceeded, packets, bytes, actions	Displays the number of packets (also shown in bytes) marked as exceeding a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately.
violated, packets, bytes, actions	Displays the number of packets (also shown in bytes) marked as violating a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately.

Explicit Congestion Notification: Example

The following is sample output from the **show policy-map interface** command when the WRED — Explicit Congestion Notification (ECN) feature has been configured. The words “explicit congestion notification” included in the output indicate that ECN has been enabled.

```
Router# show policy-map interface Serial4/1

 Serial4/1

  Service-policy output:policy_ecn
        Class-map:prec1 (match-all)
          1000 packets, 125000 bytes
          30 second offered rate 14000 bps, drop rate 5000 bps
          Match:ip precedence 1
```

```
     Weighted Fair Queueing
       Output Queue:Conversation 42
       Bandwidth 20 (%)
       Bandwidth 100 (kbps)
       (pkts matched/bytes matched) 989/123625
    (depth/total drops/no-buffer drops) 0/455/0
        exponential weight:9
        explicit congestion notification
        mean queue depth:0

class    Transmitted  Random drop  Tail drop   Minimum     Maximum     Mark
         pkts/bytes   pkts/bytes    pkts/bytes threshold   threshold   probability
  0        0/0          0/0          0/0          20          40         1/10
  1      545/68125      0/0          0/0          22          40         1/10
  2        0/0          0/0          0/0          24          40         1/10
  3        0/0          0/0          0/0          26          40         1/10
  4        0/0          0/0          0/0          28          40         1/10
  5        0/0          0/0          0/0          30          40         1/10
  6        0/0          0/0          0/0          32          40         1/10
  7        0/0          0/0          0/0          34          40         1/10
rsvp       0/0          0/0          0/0          36          40         1/10
class    ECN Mark
         pkts/bytes
  0       0/0
  1      43/5375
  2       0/0
  3       0/0
  4       0/0
  5       0/0
  6       0/0
  7       0/0
rsvp      0/0
```

Table 8 describes the significant fields shown in the display.

Table 8 show policy-map interface Field Descriptions—Configured for ECN

Field	Description
explicit congestion notification	Indication that Explicit Congestion Notification is enabled.
mean queue depth	Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a moving average. The minimum and maximum thresholds are compared against this value to determine drop decisions.
class	IP precedence value.
Transmitted pkts/bytes	Number of packets (also shown in bytes) passed through WRED and not dropped by WRED. **Note** If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped *after* the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as "no-buffer drops") are not taken into account by the WRED packet counter.
Random drop pkts/bytes	Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence value.

Table 8 show policy-map interface Field Descriptions—Configured for ECN (continued)

Field	Description
Tail drop pkts/bytes	Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence value.
Minimum threshold	Minimum WRED threshold in number of packets.
Maximum threshold	Maximum WRED threshold in number of packets.
Mark probability	Fraction of packets dropped when the average queue depth is at the maximum threshold.
ECN Mark pkts/bytes	Number of packets (also shown in bytes) marked by ECN.

Class-Based RTP and TCP Header Compression: Example

The following sample output from the **show policy-map interface** command shows the RTP header compression has been configured for a class called "prec2" in the policy map called "p1".

The **show policy-map interface** command output displays the type of header compression configured (RTP), the interface to which the policy map called "p1" is attached (Serial 4/1), the total number of packets, the number of packets compressed, the number of packets saved, the number of packets sent, and the rate at which the packets were compressed (in bits per second (bps)).

In this example, User Datagram Protocol (UDP)/RTP header compressions have been configured, and the compression statistics are included at the end of the display.

```
Router# show policy-map interface Serial4/1

Serial4/1

Service-policy output:p1

    Class-map:class-default (match-any)
      1005 packets, 64320 bytes
      30 second offered rate 16000 bps, drop rate 0 bps
      Match:any
compress:
          header ip rtp
          UDP/RTP Compression:
          Sent:1000 total, 999 compressed,
                41957 bytes saved, 17983 bytes sent
                3.33 efficiency improvement factor
                99% hit ratio, five minute miss rate 0 misses/sec, 0 max
                 rate 5000 bps
```

Table 9 describes the significant fields shown in the display.

Table 9 show policy-map interface Field Descriptions—Configured for Class-Based RTP and TCP Header Compression[1]

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.

Table 9 show policy-map interface Field Descriptions—Configured for Class-Based RTP and TCP Header Compression[1] (continued)

Field	Description
offered rate	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
UDP/RTP Compression	Indicates that RTP header compression has been configured for the class.
Sent total	Count of every packet sent, both compressed packets and full-header packets.
Sent compressed	Count of number of compressed packets sent.
bytes saved	Total number of bytes saved (that is, bytes not needing to be sent).
bytes sent	Total number of bytes sent for both compressed and full-header packets.
efficiency improvement factor	The percentage of increased bandwidth efficiency as a result of header compression. For example, with RTP streams, the efficiency improvement factor can be as much as 2.9 (or 290 percent).
hit ratio	Used mainly for troubleshooting purposes, this is the percentage of packets found in the context database. In most instances, this percentage should be high.
five minute miss rate	The number of new traffic flows found in the last five minutes.
misses/sec max	The average number of new traffic flows found per second, and the highest rate of new traffic flows to date.
rate	The actual traffic rate (in bits per second) after the packets are compressed.

1. A number in parentheses may appear next to the service-policy output name and the class-map name. The number is for Cisco internal use only and can be disregarded.

Modular QoS CLI (MQC) Unconditional Packet Discard: Example

The following sample output from the **show policy-map interface** command displays the statistics for the Serial2/0 interface, to which a policy map called "policy1" is attached. The discarding action has been specified for all the packets belonging to a class called "c1." In this example, 32000 bps of traffic is sent ("offered") to the class and all of them are dropped. Therefore, the drop rate shows 32000 bps.

```
Router# show policy-map interface Serial2/0

 Serial2/0

  Service-policy output: policy1

    Class-map: c1 (match-all)
       10184 packets, 1056436 bytes
       5 minute offered rate 32000 bps, drop rate 32000 bps
       Match: ip precedence 0
       drop
```

Table 10 describes the significant fields shown in the display.

Table 10 show policy-map interface Field Descriptions—Configured for MQC Unconditional Packet Discard[1]

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
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 10 show policy-map interface Field Descriptions—Configured for MQC Unconditional Packet Discard[1] (continued)

Field	Description
Note	In distributed architecture platforms (such as the C7500), the value of the tranfer rate, calculated as the difference between the offered rate and the drop rate counters, can sporadically diviate from the average by up to 20 percent or more. This can occur while no corresponding burst is registered by independent traffic analyser equipment.
Match	Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and QoS groups. For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide*.
drop	Indicates that the packet discarding action for all the packets belonging to the specified class has been configured.

1. A number in parentheses may appear next to the service-policy output name and the class-map name. The number is for Cisco internal use only and can be disregarded.

Percentage-Based Policing and Shaping: Example

The following sample output from the **show policy-map interface** command shows traffic policing configured using a CIR based on a bandwidth of 20 percent. The CIR and committed burst (Bc) in milliseconds (ms) are included in the display.

```
Router# show policy-map interface Serial3/1

 Serial3/1

  Service-policy output: mypolicy

    Class-map: gold (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      police:
          cir 20 % bc 10 ms
          cir 2000000 bps, bc 2500 bytes
          pir 40 % be 20 ms
          pir 4000000 bps, be 10000 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
```

Table 11 describes the significant fields shown in the display.

Table 11 show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping[1]

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
police	Indicates that traffic policing based on a percentage of bandwidth has been enabled. Also, displays the bandwidth percentage, the CIR, and the committed burst (Bc) size in ms.
conformed, actions	Displays the number of packets and bytes marked as conforming to the specified rates, and the action to be taken on those packets.
exceeded, actions	Displays the number of packets and bytes marked as exceeding the specified rates, and the action to be taken on those packets.

1. A number in parentheses may appear next to the service-policy output name and the class-map name. The number is for Cisco internal use only and can be disregarded.

Traffic Shaping: Example

The following sample output from the **show policy-map interface** command (shown below) displays the statistics for the serial 3/2 interface. Traffic shaping has been enabled on this interface, and an average rate of 20 percent of the bandwidth has been specified.

```
Router# show policy-map interface Serial3/2

Serial3/2

  Service-policy output: p1

    Class-map: c1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

```
Traffic Shaping
  Target/Average      Byte   Sustain    Excess      Interval  Increment  Adapt
  Rate              Limit  bits/int  bits/int    (ms)     (bytes)   Active
   20 %                        10 (ms)    20 (ms)
  201500/201500       1952   7808       7808        38         976       -

  Queue     Packets   Bytes     Packets   Bytes     Shaping
  Depth                         Delayed   Delayed   Active
  0         0         0         0         0         no
```

Table 12 describes the significant fields shown in the display.

Table 12 show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping (with Traffic Shaping Enabled)[1]

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
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.
Match	Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and quality of service (QoS) groups. For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide*.
Traffic Shaping	Indicates that traffic shaping based on a percentage of bandwidth has been enabled.
Target /Average Rate	Rate (percentage) used for shaping traffic and the number of packets meeting that rate.

Table 12 show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping (with Traffic Shaping Enabled)[1] (continued)

Field	Description
Byte Limit	Maximum number of bytes that can be transmitted per interval. Calculated as follows: ((Bc+Be) /8) x 1
Sustain bits/int	Committed burst (Bc) rate.
Excess bits/int	Excess burst (Be) rate.
Interval (ms)	Time interval value in milliseconds (ms).
Increment (bytes)	Number of credits (in bytes) received in the token bucket of the traffic shaper during each time interval.
Adapt Active	Indicates whether adaptive shaping is enabled.
Queue Depth	Current queue depth of the traffic shaper.
Packets	Total number of packets that have entered the traffic shaper system.
Bytes	Total number of bytes that have entered the traffic shaper system.
Packets Delayed	Total number of packets delayed in the queue of the traffic shaper before being transmitted.
Bytes Delayed	Total number of bytes delayed in the queue of the traffic shaper before being transmitted.
Shaping Active	Indicates whether the traffic shaper is active. For example, if a traffic shaper is active, and the traffic being sent exceeds the traffic shaping rate, a “yes” appears in this field.

1. A number in parentheses may appear next to the service-policy output name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

Packet Classification Based on Layer 3 Packet Length: Example

The following sample output from the **show policy-map interface** command displays the packet statistics for the Ethernet4/1 interface, to which a service policy called “mypolicy” is attached. The Layer 3 packet length has been specified as a match criterion for the traffic in the class called “class1”.

```
Router# show policy-map interface Ethernet4/1

 Ethernet4/1

  Service-policy input: mypolicy

    Class-map: class1 (match-all)
       500 packets, 125000 bytes
       5 minute offered rate 4000 bps, drop rate 0 bps
       Match: packet length min 100 max 300
       QoS Set
         qos-group 20
           Packets marked 500
```

Table 13 describes the significant fields shown in the display.

Table 13 show policy-map interface Field Descriptions—Configured for Packet Classification Based on Layer 3 Packet Length[1]

Field	Description
Service-policy input	Name of the input service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
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.
Match	Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and QoS groups.
QoS Set, qos-group, Packets marked	Indicates that class-based packet marking based on the QoS group has been configured. Includes the qos-group number and the number of packets marked.

1. A number in parentheses may appear next to the service-policy input name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

Enhanced Packet Marking: Example

The following sample output of the **show policy-map interface** command shows the service policies attached to a FastEthernet subinterface. In this example, a service policy called “policy1” has been attached. In “policy1”, a table map called “table-map1” has been configured. The values in “table-map1” will be used to map the precedence values to the corresponding class of service (CoS) values.

```
Router# show policy-map interface

 FastEthernet1/0.1

  Service-policy input: policy1
```

```
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      QoS Set
        precedence cos table table-map1
          Packets marked 0
```

Table 14 describes the fields shown in the display.

Table 14 show policy-map interface Field Descriptions—Configured for Enhanced Packet Marking[1]

Field	Description
Service-policy input	Name of the input service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of the packets coming into the class.
Match	Match criteria specified for the class of traffic. Choices include criteria such as Precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) group (set). For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide*.
QoS Set	Indicates that QoS group (set) has been configured for the particular class.
precedence cos table table-map1	Indicates that a table map (called "table-map1") has been used to determine the precedence value. The precedence value will be set according to the CoS value defined in the table map.
Packets marked	Total number of packets marked for the particular class.

1. A number in parentheses may appear next to the service-policy input name and the class-map name. The number is for Cisco internal use only and can be disregarded.

Traffic Policing: Example

The following is sample output from the **show policy-map interface** command. This sample displays the statistics for the serial 2/0 interface on which traffic policing has been enabled. The committed (conform) burst (bc) and excess (peak) burst (be) are specified in milliseconds (ms).

```
Router# show policy-map interface serial2/0

 Serial2/0

  Service-policy output: policy1 (1050)

    Class-map: class1 (match-all) (1051/1)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 0  (1052)
      police:
          cir 20 % bc 300 ms
          cir 409500 bps, bc 15360 bytes
          pir 40 % be 400 ms
```

```
        pir 819000 bps, be 40960 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) (1054/0)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any  (1055)
      0 packets, 0 bytes
      5 minute rate 0 bps
```

In this example, the CIR and PIR are displayed in bps, and both the committed burst (bc) and excess burst (be) are displayed in bits.

The CIR, PIR bc, and be are calculated on the basis of the formulas described below.

Formula for Calculating the CIR: Example

When calculating the CIR, the following formula is used:

- CIR percentage specified (as shown in the output from the **show policy-map** command) * bandwidth (BW) of the interface (as shown in the output from the **show interfaces** command) = total bits per second

According to the output from the **show interfaces** command for the serial 2/0 interface, the interface has a bandwidth (BW) of 2048 kbps.

```
Router # show interfaces s2/0

Serial2/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

The following values are used for calculating the CIR:

20 % * 2048 kbps = 409600 bps

Formula for Calculating the PIR: Example

When calculating the PIR, the following formula is used:

- PIR percentage specified (as shown in the output from the **show policy-map** command) * bandwidth (BW) of the interface (as shown in the output from the **show interfaces** command) = total bits per second

According to the output from the **show interfaces** command for the serial 2/0 interface, the interface has a bandwidth (BW) of 2048 kbps.

```
Router # show interfaces serial2/0

Serial2/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

The following values are used for calculating the PIR:

40 % * 2048 kbps = 819200 bps

Note Discrepancies between this total and the total shown in the output from the **show policy-map interface** command can be attributed to a rounding calculation or to differences associated with the specific interface configuration.

Formula for Calculating the Committed Burst (bc): Example

When calculating the bc, the following formula is used:

- The bc in milliseconds (as shown in the **show policy-map** command) * the CIR in bits per seconds = total number bytes

The following values are used for calculating the bc:

300 ms * 409600 bps = 15360 bytes

Formula for Calculating the Excess Burst (be): Example

When calculating the bc and the be, the following formula is used:

- The be in milliseconds (as shown in the **show policy-map** command) * the PIR in bits per seconds = total number bytes

The following values are used for calculating the be:

400 ms * 819200 bps = 40960 bytes

Table 15 describes the significant fields shown in the display.

Table 15 show policy-map interface Field Descriptions

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets and bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to 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.
Match	Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) groups. For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide*.
police	Indicates that traffic policing has been enabled. Display includes the CIR, PIR (in both a percentage of bandwidth and in bps) and the bc and be in bytes and milliseconds. Also displays the optional conform, exceed, and violate actions, if any, and the statistics associated with these optional actions.

Bandwidth Estimation: Example

The following sample output from the **show policy-map interface** command displays statistics for the Fast Ethernet 0/1 interface on which bandwidth estimates for quality of service (QoS) targets have been generated.

The Bandwidth Estimation section indicates that bandwidth estimates for QoS targets have been defined. These targets include the packet loss rate, the packet delay rate, and the timeframe in milliseconds. Confidence refers to the drop-one-in value (as a percentage) of the targets. Corvil Bandwidth means the bandwidth estimate in kilobits per second.

When no drop or delay targets are specified, "none specified, falling back to drop no more than one packet in 500" appears in the output.

```
Router# show policy-map interface FastEthernet0/1

 FastEthernet0/1

  Service-policy output: my-policy

    Class-map: icmp (match-all)
      199 packets, 22686 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: access-group 101
      Bandwidth Estimation:
        Quality-of-Service targets:
          drop no more than one packet in 1000 (Packet loss < 0.10%)
          delay no more than one packet in 100 by 40 (or more) milliseconds
            (Confidence: 99.0000%)
        Corvil Bandwidth: 1 kbits/sec

    Class-map: class-default (match-any)
      112 packets, 14227 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      Bandwidth Estimation:
        Quality-of-Service targets:
          <none specified, falling back to drop no more than one packet in 500
        Corvil Bandwidth: 1 kbits/sec
```

Shaping with HQF Enabled: Example

The following sample output from the **show policy-map interface** command shows that shaping is active (as seen in the queue depth field) with HQF enabled on the serial 4/3 interface. All traffic is classified to the class-default queue.

```
Router# show policy-map interface serial4/3

 Serial4/3

  Service-policy output: shape

    Class-map: class-default (match-any)
      2203 packets, 404709 bytes
      30 second offered rate 74000 bps, drop rate 14000 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 64/354/0
      (pkts output/bytes output) 1836/337280
      shape (average) cir 128000, bc 1000, be 1000
      target shape rate 128000
        lower bound cir 0,  adapt to fecn 0
```

```
Service-policy : LLQ

  queue stats for all priority classes:

    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0

  Class-map: c1 (match-all)
    0 packets, 0 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 1
    Priority: 32 kbps, burst bytes 1500, b/w exceed drops: 0

  Class-map: class-default (match-any)
    2190 packets, 404540 bytes
    30 second offered rate 74000 bps, drop rate 14000 bps
    Match: any

    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 63/417/0
    (pkts output/bytes output) 2094/386300
```

Packets Matched on the Basis of VLAN ID Number: Example

Note As of Cisco IOS Release 12.2(31)SB2, matching packets on the basis of VLAN ID numbers is supported on the Catalyst 1000 platform only.

The following is a sample configuration in which packets are matched and classified on the basis of the VLAN ID number. In this sample configuration, packets that match VLAN ID number 150 are placed in a class called “class1.”

```
Router# show class-map

Class Map match-all class1 (id 3)
Match vlan 150
```

Class1 is then configured as part of the policy map called “policy1.” The policy map is attached to Fast Ethernet subinterface 0/0.1.

The following sample output of the **show policy-map interface** command displays the packet statistics for the policy maps attached to Fast Ethernet subinterface 0/0.1. It displays the statistics for policy1, in which class1 has been configured.

```
Router# show policy-map interface

FastEthernet0/0.1

! Policy-map name.
Service-policy input: policy1

! Class configured in the policy map.
Class-map: class1 (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps

! VLAN ID 150 is the match criterion for the class.
Match: vlan 150
police:
cir 8000000 bps, bc 512000000 bytes
```

```
conformed 0 packets, 0 bytes; actions:
transmit
exceeded 0 packets, 0 bytes; actions:
drop
conformed 0 bps, exceed 0 bps

Class-map: class-default (match-any)
10 packets, 1140 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: any
10 packets, 1140 bytes
5 minute rate 0 bps
```

Table 16 describes the significant fields shown in the display.

Table 16 show policy-map interface Field Descriptions—Packets Matched on the Basis of VLAN ID Number[1]

Field	Description
Service-policy input	Name of the input service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of the packets coming into the class.
Match	Match criteria specified for the class of traffic. Choices include criteria such as VLAN ID number, precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) group (set). For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

1. A number in parentheses may appear next to the service-policy input name and the class-map name. The number is for Cisco internal use only and can be disregarded.

Cisco 7600 Series Routers: Example

The following example shows how to display the statistics and the configurations of all the input and output policies that are attached to an interface on a Cisco 7600 series router:

```
Router# show policy-map interface

 FastEthernet5/36
  service-policy input: max-pol-ipp5
    class-map: ipp5 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
  class ipp5
    police 2000000000 2000000 conform-action set-prec-transmit 6 exceed-action p
policed-dscp-transmit
```

The following example shows how to display the input-policy statistics and the configurations for a specific interface on a Cisco 7600 series router:

```
Router# show policy-map interface fastethernet 5/36 input
```

```
 FastEthernet5/36
  service-policy input: max-pol-ipp5
    class-map: ipp5 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
  class ipp5
    police 2000000000 2000000 conform-action set-prec-transmit 6 exceed-action p
policed-dscp-transmit
```

Table 17 describes the significant fields shown in the display.

Table 17 show policy-map interface Field Descriptions—Cisco 7600 Series Routers

Field	Description
service-policy input	Name of the input service policy applied to the specified interface.
class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
minute rate	Rate, in kbps, of the packets coming into the class.
match	Match criteria specified for the class of traffic. Choices include criteria such as VLAN ID number, precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) group (set). For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide*.
class	Precedence value.
police	Indicates that the **police** command has been configured to enable traffic policing.

Multiple Priority Queues on Serial Interface: Example

The following sample output from the **show policy-map interface** command shows the types of statistical information that displays when multiple priority queues are configured. Depending upon the interface in use and the options enabled, the output that you see may vary slightly from the output shown below.

```
Router# show policy-map interface

    Serial2/1/0
    Service-policy output: P1
    Queue statistics for all priority classes:
    .
    .
    .
    Class-map: Gold (match-all)
     0 packets, 0 bytes/*Updated for each priority level configured.*/
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 2
     Priority: 0 kbps, burst bytes 1500, b/w exceed drops: 0
    Priority Level 4:
     0 packets, 0 bytes
```

Bandwidth-Remaining Ratios: Example

The following sample output from the **show policy-map interface** command indicates that bandwidth-remaining ratios are configured for class queues. As shown in the example, the classes precedence_0, precedence_1, and precedence_2 have bandwidth-remaining ratios of 20, 40, and 60, respectively.

```
Router# show policy-map interface GigabitEthernet1/0/0.10

  Service-policy output: vlan10_policy

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
      Queueing
      queue limit 250 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 1000000, bc 4000, be 4000
      target shape rate 1000000
      bandwidth remaining ratio 10

      Service-policy : child_policy

        Class-map: precedence_0 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 0
          Queueing
          queue limit 62 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 20

        Class-map: precedence_1 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 1
          Queueing
          queue limit 62 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 40

        Class-map: precedence_2 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 2
          Queueing
          queue limit 62 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 60

        Class-map: class-default (match-any)
```

```
        0 packets, 0 bytes
        30 second offered rate 0 bps, drop rate 0 bps
        Match: any
          0 packets, 0 bytes
          30 second rate 0 bps

        queue limit 62 packets
        (queue depth/total drops/no-buffer drops) 0/0/0
        (pkts output/bytes output) 0/0
```

Tunnel Marking: Example

In this sample output of the **show policy-map interface** command, the character string "ip dscp tunnel 3" indicates that L2TPv3 tunnel marking has been configured to set the DSCP value to 3 in the header of a tunneled packet.

```
Router# show policy-map interface

 Serial0

  Service-policy input: tunnel

    Class-map: frde (match-all)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: fr-de
      QoS Set
        ip dscp tunnel 3
          Packets marked 0

    Class-map: class-default (match-any)
      13736 packets, 1714682 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
        13736 packets, 1714682 bytes
        30 second rate 0 bps
```

Table 18 describes the significant fields shown in the display.

Table 18 show policy-map interface Field Descriptions—Configured for Tunnel Marking

Field	Description
service-policy input	Name of the input service policy applied to the specified interface.
class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to 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.
match	Match criteria specified for the class of traffic. In this example, the Frame Relay Discard Eligible (DE) bit has been specified as the match criterion. For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide*.
ip dscp tunnel	Indicates that tunnel marking has been configured to set the DSCP in the header of a tunneled packet to a value of 3.

Related Commands

Command	Description
bandwidth remaining ratio	Specifies a bandwidth-remaining ratio for class queues and subinterface-level queues to determine the amount of unused (excess) bandwidth to allocate to the queue during congestion.
class-map	Creates a class map to be used for matching packets to a specified class.
compression header ip	Configures RTP or TCP IP header compression for a specific class.
drop	Configures a traffic class to discard packets belonging to a specific class.
match fr-dlci	Specifies the Frame Relay DLCI number as a match criterion in a class map.
match packet length (class-map)	Specifies the length of the Layer 3 packet in the IP header as a match criterion in a class map.
police	Configures traffic policing.
police (percent)	Configures traffic policing on the basis of a percentage of bandwidth available on an interface.
police (two rates)	Configures traffic policing using two rates, the CIR and the PIR.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
priority	Specifies that low-latency behavior must be given to a traffic class and configures multiple priority queues.
random-detect ecn	Enables ECN.
shape (percent)	Specifies average or peak rate traffic shaping on the basis of a percentage of bandwidth available on an interface.
show class-map	display all class maps and their matching criteria.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show interfaces	Displays statistics for all interfaces configured on a router or access server.
show mls qos	Displays MLS QoS information.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map class	Displays the configuration for the specified class of the specified policy map.
show table-map	Displays the configuration of a specified table map or of all table maps.
table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

show protocol phdf

To display protocol information from a specific protocol header description file (PHDF), use the **show protocol phdf** command in privileged EXEC mode.

show protocol phdf *protocol-name*

Syntax Description

protocol-name	Loaded PHDF.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced.

Examples

The following example shows how to define FPM traffic classes for slammer packets (UDP port 1434). The match criteria defined within the class maps is for slammer packets with an IP length not to exceed 404 bytes, UDP port 1434, and pattern 0x4011010 at 224 bytes from start of IP header. This example also shows how to define the service policy "fpm-policy" and apply it to the gigabitEthernet interface. Show commands have been issued to verify the FPM configuration. (Note that PHDFs are not displayed in show output because they are in XML format.)

```
Router(config)# load protocol disk2:ip.phdf
Router(config)# load protocol disk2:udp.phdf

Router(config)# class-map type stack match-all ip-udp
Router(config-cmap)# description "match UDP over IP packets"
Router(config-cmap)# match field ip protocol eq 0x11 next udp

Router(config)# class-map type access-control match-all slammer
Router(config-cmap)# description "match on slammer packets"
Router(config-cmap)# match field udp dest-port eq 0x59A
Router(config-cmap)# match field ip length eq 0x194
Router(config-cmap)# match start 13-start offset 224 size 4 eq 0x4011010

Router(config)# policy-map type access-control fpm-udp-policy
Router(config-pmap)# description "policy for UDP based attacks"
Router(config-pmap)# class slammer
Router(config-pmap-c)# drop

Router(config)# policy-map type access-control fpm-policy
Router(config-pmap)# description "drop worms and malicious attacks"
Router(config-pmap)# class ip-udp
Router(config-pmap-c)# service-policy fpm-udp-policy

Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy type access-control input fpm-policy

Router# show protocols phdf ip

Protocol ID: 1
Protocol name: IP
Description: Definition-for-the-IP-protocol
```

```
Original file name: disk2:ip.phdf
Header length: 20
Constraint(s):
Total number of fields: 12
Field id: 0, version, IP-version
Fixed offset. offset 0
Constant length. Length: 4
Field id: 1, ihl, IP-Header-Length
Fixed offset. offset 4
Constant length. Length: 4
Field id: 2, tos, IP-Type-of-Service
Fixed offset. offset 8
Constant length. Length: 8
Field id: 3, length, IP-Total-Length
Fixed offset. offset 16
Constant length. Length: 16
Field id: 4, identification, IP-Identification
Fixed offset. offset 32
Constant length. Length: 16
Field id: 5, flags, IP-Fragmentation-Flags
Fixed offset. offset 48
Constant length. Length: 3
Field id: 6, fragment-offset, IP-Fragmentation-Offset
Fixed offset. offset 51
Constant length. Length: 13
Field id: 7, ttl, Definition-for-the-IP-TTL
Fixed offset. offset 64
Constant length. Length: 8
Field id: 8, protocol, IP-Protocol
Fixed offset. offset 72
Constant length. Length: 8
Field id: 9, checksum, IP-Header-Checksum
Fixed offset. offset 80
Constant length. Length: 16
Field id: 10, source-addr, IP-Source-Address
Fixed offset. offset 96
Constant length. Length: 32
Field id: 11, dest-addr, IP-Destination-Address
Fixed offset. offset 128
Constant length. Length: 32

Router# show protocols phdf udp

Protocol ID: 3
Protocol name: UDP
Description: UDP-Protocol
Original file name: disk2:udp.phdf
Header length: 8
Constraint(s):
Total number of fields: 4
Field id: 0, source-port, UDP-Source-Port
Fixed offset. offset 0
Constant length. Length: 16
Field id: 1, dest-port, UDP-Destination-Port
Fixed offset. offset 16
Constant length. Length: 16
Field id: 2, length, UDP-Length
Fixed offset. offset 32
Constant length. Length: 16
Field id: 3, checksum, UDP-Checksum
Fixed offset. offset 48
Constant length. Length: 16
```

Related Commands

Command	Description
load protocol	Loads a PHDF onto a router.

Feature Information for Flexible Packet Matching

Table 19 lists the release history for this feature.

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

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 19 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 19 Feature Information for Flexible Packet Matching

Feature Name	Releases	Feature Information
Flexible Packet Matching	12.4(4)T 12.2(18)ZY	FPM is a packet classification feature that allows users to define one or more classes of network traffic by pairing a rich set of standard matching operators with user-defined protocol header fields. In Cisco IOS Release 12.2(18)ZY, FPM was implemented on the Catalyst 6500 series of switches equipped with the PISA.
FPM Full Packet Filtering	12.4(15)T	In Cisco IOS Release 12.4(15)T, FPM now supports searching for patterns up to 56 bytes long anywhere within the entire packet. Prior to 12.4(15)T, FPM only supported searching for patterns up to 32 bytes long within the first 256 bytes of the packet.