QoS: Color-Aware Policer

The QoS: Color-Aware Policer enables a “color-aware” method of traffic policing. This feature allows you to police traffic according to the color classification of a packet. The packet color classification is based on packet matching criteria defined for two user-specified traffic classes—the conform-color class and the exceed-color class. These two traffic classes are created using the **conform-color** command and the metering rates are defined using the **police** command.

Feature History for QoS: Color-Aware Policerr

Release	Modification
12.0(26)S	This feature was introduced.
12.2(27)SBA	This feature was integrated into Cisco IOS Release 12.2(27)SBA.

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

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

Information About the Color-Aware Policer

To configure the Color-Aware Policer, you should understand the following concepts:

Benefits

Extended Traffic Policing Functionality

The Color-Aware Policer extends the functionality of the quality of service (QoS) traffic policing feature. It allows you to police traffic on the basis of the packet color classification in color-aware mode.

Improved SLA Provisioning

The Color-Aware Policer allows you to provision enhanced Service Level Agreements (SLAs) across the DiffServ domain.

Full Compliance with Industry-Standard RFCs

This feature fully complies with the following two industry-standard RFCs:

- RFC 2697: *A Single Rate Three Color Marker*
- RFC 2698: *A Two Rate Three Color Marker*

Use of Preexisting Packet Marking from Other Traffic Policers

Cisco IOS software includes a number of traffic policing features, including the Two-Rate Policer. The Color-Aware Policer takes into account any preexisting markings that may be set for a packet by another traffic policer (for example, the Two-Rate Policer) configured at a previous network node. At the node where color-aware policing is configured, these preexisting markings are then used in determining the appropriate color-aware policing action for the packet.

For example, two-rate policing may be configured on a node upstream in the network. The Two-Rate Policer has marked a packet as violate-color. The Color-Aware Policer takes this violate-color marking into account when determining the appropriate policing action. In color-aware policing, the violate-color packet would never receive the action associated with either the conform-color packets or exceed-color packets. This way, tokens for violating packets are never taken from the metering token buckets at the color-aware policing node.

Color-Aware Mode

The Cisco IOS traffic policing software polices traffic on the basis of metering rates such as the committed information rate (CIR), the peak information rate (PIR), their associated burst sizes, and any policing actions (such as transmit or drop) configured for the traffic. These metering rates, sizes, and policing actions are specified using the **police** command.

This feature allows you to police traffic in color-aware mode. In the color-aware mode, packet matching criteria will first be specified using the **class-map** command. Then a policy map will be configured to create classes, enable color-aware traffic policing, and create two classes used specifically for color-aware policing—the conform-color class and the exceed-color class.

The conform-color class and the exceed-class are created by using the **conform-color** command (described later in this document). The **police** command is used in conjunction with the **conform-color** command to specify the policing actions to be taken on packets in the conform-color class and the exceed-color class.

With color-aware policing, packets are classified as either conform-color packets, exceed-color packets, or violate-color packets. The metering treatment the packet receives varies by the classification, as described below:

- Packets belonging to the conform-color class are metered against both the CIR and the PIR.
- Packets belonging to the exceed-color class are metered against the PIR only.
- Packets belonging to the violate-color class are not metered against either the CIR or the PIR.

The **police** command is then used to specify the following items:

- The CIR and PIR
- The conform burst (bc) size
- The excess burst (be) size
- The policing actions to be taken on the packet.

Color-aware mode can be used with either single-rate traffic policing or two-rate traffic policing.

Color-Aware Mode of Single-Rate Traffic Policing

Networks police traffic by limiting the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Policing traffic allows you to control the maximum rate of traffic sent or received on an interface and to partition a network into multiple priority levels or class of service (CoS).

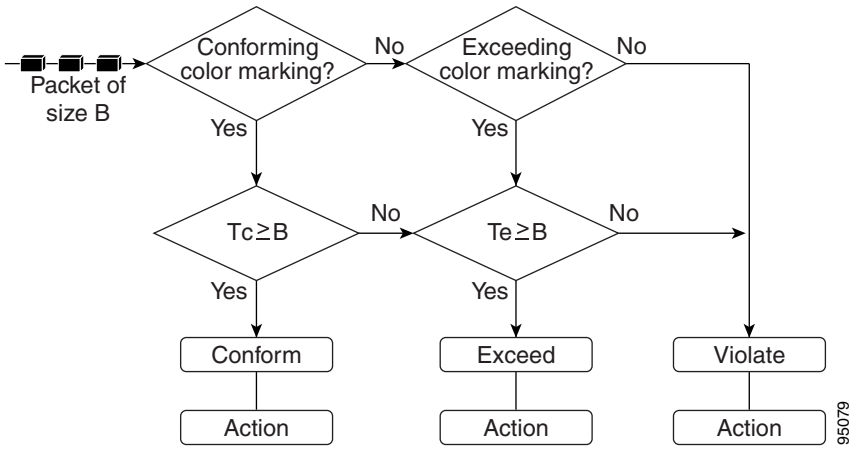
Single-rate traffic policing (often referred to simply as traffic policing) limits the input or output transmission rate of a class of traffic on the basis of user-defined criteria. It allows you to control the maximum rate of traffic transmitted or received on an interface.

Traffic policing works by using a token bucket algorithm. There are currently two types of token bucket algorithms: a single-token bucket algorithm and a two-token bucket algorithm. A single-token bucket system is used when the violate-action option is not specified, and a two-token bucket system is used when the violate-action option is specified.

Single-Rate Color-Aware Mode Functionality

The flow chart in Figure 1 illustrates the algorithm used for handling traffic in color-aware single-rate traffic policing.

Figure 1 Traffic Flow Algorithm Used in Color-Aware Single-Rate Traffic Policing



In the above flow chart, a packet of size B arrives at the interface. Tc indicates the number of tokens in the CIR token bucket, and Tb indicates the number of tokens in the excess token bucket.

When a packet of size B bytes arrives at the interface, the packet is evaluated as to whether it is marked as either a conform-color packet, an exceed-color packet, or a packet with no color marking. Then the following actions are performed on the packet in the order shown below:

1. If the packet is marked conform-color, and Tc is greater than or equal to B, the conform action is applied to the packet, and Tc is decremented by B.
2. Otherwise, if the packet is marked conform-color or exceed-color, and Te is greater than or equal to B, the exceed action is applied to the packet, and Te is decremented by B.
3. Otherwise, for all other packets, the violate action is applied to the packet.

Policing Actions

The algorithm provides users with three actions for each packet: a conform action, an exceed action, and an optional violate action. A conform action is applied to the conforming packets, an exceed action is applied to the exceeding packets, and an violate action is applied to the violating packets. Users can specify these actions. For instance, conforming packets can sent, exceeding packets can sent with a decreased priority, and violating packets can be dropped.

Color-Aware Mode of Two-Rate Traffic Policing

Networks police traffic by limiting the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Policing traffic allows you to control the maximum rate of traffic sent or received on an interface and to partition a network into multiple priority levels or CoS.

With the two-rate traffic policing, you can enforce traffic policing according to two separate rates—the CIR and the PIR. You can specify the use of these two rates, along with their corresponding values, by using the **cir** and **pir** keywords of the **police** command.

Two-rate traffic policing uses two token buckets—Tc and Tp—for policing traffic at two independent rates. The Tc token bucket contains the tokens in the CIR bucket. The Tp token bucket contains the tokens in the PIR bucket.

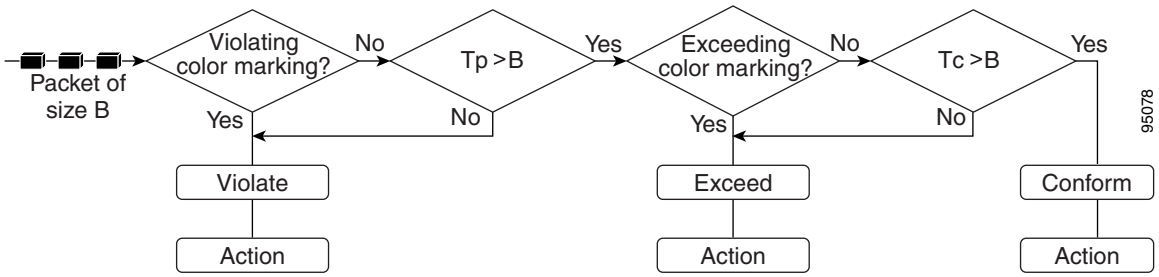
Note the following points about the two token buckets:

- The Tc token bucket is updated at the CIR value each time a packet arrives at the interface. The Tc token bucket can contain up to the confirm burst (Bc) value.
- The Tp token bucket is updated at the PIR value each time a packet arrives at the interface. The Tp token bucket can contain up to the peak burst (Be) value.

Two-Rate Color-Aware Mode Functionality

The flow chart in Figure 2 illustrates the algorithm used for handling traffic in color-aware two-rate traffic policing.

Figure 2 Traffic Flow Algorithm Used in Color-Aware Two-Rate Traffic Policing



In the above illustration, a packet of size B arrives at the interface. Tc indicates the number of tokens in the CIR token bucket, and Tp indicates the number of tokens in PIR token bucket.

When a packet of size B bytes arrives at the interface, the packet is evaluated as to whether it is marked as either an exceed-color packet or a violate-color packet. Then the following actions are performed on the packet in the order shown below:

1. If the packet is marked violate-color, or Tp is less than B, the violate action is applied to the packet. Tp is not decremented.
2. Otherwise, if the packet is marked exceed-color, and Tc is less than B, the exceed action is applied to the packet, and Tc bucket is decremented by B.
3. Otherwise, for all other packets, the conform action is applied to the packet, and both the Tc and Tp are decremented by B.

Policing Actions

The algorithm provides users with three actions for each packet: a conform action, an exceed action, and an optional violate action. A conform action is applied to the conforming packets, an exceed action is applied to the exceeding packets, and an violate action is applied to the violating packets. Users can specify these actions. For instance, conforming packets can sent, exceeding packets can sent with a decreased priority, and violating packets can be dropped.

Packet Matching Criteria

The first process in configuring color-aware policing is to create a class map. The class map is used to specify packet matching criteria.For instance, you can configure the class map to match packets based on a precedence level, a CoS value, or a differentiated services code point (DSCP) value. The match criteria is set with a specific **match** command. For example, to match packets based on a precedence value, use the **match precedence** command.

The **match** commands that can be used in a class map to establish packet matching criteria include the commands listed in Table 1.

Table 1 match Commands Used to Establish Packet Matching Criteria

Command	Description
match cos	Matches a packet based on a Layer 2 CoS value.
match dscp	Identifies a specific DSCP value as a match criterion.
match fr-dlci	Specifies the Frame Relay data-link connection identifier (DLCI) number as a match criterion.
match mpls experimental	Specifies the value of the Multiprotocol Label Switching (MPLS) experimental (EXP) field as a match criterion.
match precedence	Identifies IP precedence values as match criterion.
match qos-group	Identifies a specific QoS group value as a match criterion.

The specific **match** commands that can be used to match packets vary from Cisco IOS release to Cisco IOS release. For more information about the **match** commands, refer to the documentation for your Cisco IOS release.

How to Configure Color-Aware Policing

This section contains the following procedures:

- Creating a Class Map, page 6 (required)
- Configuring a Policy Map, page 8 (required)
- Attaching the Policy Map, page 10 (required)
- Verifying the Configuration, page 11 (optional)

Creating a Class Map

A class map is used to specify packet matching criteria. To create a class map, use the commands in the following sections:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** [**match-all** | **match-any**] *class-map-name*

4. **match** [**ip**] **precedence** *ip-precedence-value*
5. **class-map** [**match-all** | **match-any**] *class-map-name*
6. **match** [**ip**] **precedence** *ip-precedence-value*
7. **exit**

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	**class-map** [**match-all** | **match-any**] *class-map-name* **Example:** `Router(config-if)# class-map conform_color_map`	Creates the conform-color class-map used for specifying packet matching criterion and enters class-map configuration mode. **Note** The optional **match-all** and **match-any** keywords determine how packets are evaluated when multiple match criteria exist. Packets must meet either all of the match criteria (**match-all**) or one of the match criteria (**match-any**) to be considered a member of the class. • Enter the class-map name.
Step 4	**match** [**ip**] **precedence** *ip-precedence-value* `Router(config-cmap)# match ip precedence 5`	(Optional) Specifies the IP precedence value as the match criterion. • Enter the IP precedence value. **Note** In this example, the IP precedence value was used as the match criterion. Other criteria (for example, the CoS value, the DSCP, or the MPLS EXP value) can be used. Match criteria are specified by using the various **match** commands. Use the **match** command that is appropriate for your network. For a list of match commands that are available, see Table 1.

	Command or Action	Purpose
Step 5	**class-map** [**match-all** | **match-any**] *class-map-name* **Example:** `Router(config-if)# class-map exceed_color_map`	Creates the exceed-color class-map used for specifying packet matching criterion and enters class-map configuration mode. **Note** The optional **match-all** and **match-any** keywords determine how packets are evaluated when multiple match criteria exist. Packets must meet either all of the match criteria (**match-all**) or one of the match criteria (**match-any**) to be considered a member of the class. • Enter the class-map name.
Step 6	**match** [**ip**] **precedence** *ip-precedence-value* `Router(config-cmap)# match ip precedence 3`	(Optional) Specifies the IP precedence value as the match criterion. • Enter the IP precedence value. **Note** In this example, the IP precedence value was used as the match criterion. Other criteria (for example, the CoS value, the DSCP, or the MPLS EXP value) can be used. Match criteria are specified by using the various **match** commands. Use the **match** command that is appropriate for your network. For a list of match commands that are available, see Table 1.
Step 7	**exit** **Example:** `Router(config-cmap)# exit`	(Optional) Exits class-map configuration mode.

Configuring a Policy Map

A policy map determines the specific QoS feature that will be applied to the packets in a specific class. For instance, a policy map can be used to configure traffic shaping, Weight Random Early Detection (WRED), or, as in this case, color-aware traffic policing.

To configure a policy map for color-aware traffic policing, use the commands in the following sections:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **police** {**cir** *cir*} [**bc** *conform-burst*] {**pir** *pir*} [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]
6. **conform-color** *class-map-name* [**exceed-color** *class-map-name*]
7. **exit**

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	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map color`	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. • Enter the policy map name.
Step 4	**class** {*class-name* | **class-default**} **Example:** `Router(config-pmap)# class ccolor`	Creates the specified class (or the default class) and enters policy-map class configuration mode. • Enter name of the class you want to create or type **class-default** (to specify the default class).
Step 5	**police** {**cir** *cir*} [**bc** *conform-burst*] {**pir** *pir*} [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]] **Example:** `Router(config-pmap-c)# police cir 8000 bc 5000 pir 8000 be 5000 conform-action transmit exceed-action set-prec-transmit 4 violate-action drop`	Configures traffic policing on the basis of the specified rates and optional actions, and enters policy-map class police configuration mode. • Enter the CIR and any optional values and actions, if applicable.
Step 6	**conform-color** *class-map-name* [**exceed-color** *class-map-name*] **Example:** `Router(config-pmap-c-police)# conform-color c1 exceed-color c2`	Enables color-aware traffic policing and creates the conform-color and exceed-color class-maps used for color-aware traffic policing. The **conform-color** *class-map-name* command creates the conform-color class. The **exceed-color** *class-map-name* option creates the exceed-color class. • Enter the class-map name or names.
Step 7	**exit** **Example:** `Router(config-pmap-c-police)# exit`	(Optional) Returns to global configuration mode.

Attaching the Policy Map

The policy map you have created must be attached to the appropriate interface or ATM permanent virtual circuit (PVC). For example, you may have to attach policy maps to either the input or the output interface on either the ingress or the egress router.

To attach a policy map to the appropriate interface or ATM PVC, use the commands in the following sections:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **pvc** [*name*] *vpi*/*vci* [**ilmi** | **qsaal** | **smds**]
5. **service-policy** {**input** | **output**} *policy-map-name*
6. **exit**

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	**interface** *type number* [*name-tag*] **Example:** `Router(config)# interface FastEthernet1/0.1`	Configures the interface type specified and enters interface configuration mode. • Enter interface type.
Step 4	**pvc** [*name*] *vpi*/*vci* [**ilmi** | **qsaal** | **smds**] **Example:** `Router(config-if)# pvc cisco 0/16 ilmi`	(Optional) Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters ATM VC configuration mode. **Note** This step is required only if you are attaching the policy map to an ATM PVC. If you are not attaching the policy map to an ATM PVC, skip this step and proceed with Step 5. • Enter the PVC name.

	Command or Action	Purpose
Step 5	**service-policy** {**input** | **output**} *policy-map-name* **Example:** `Router(config-if)# service-policy input policy1`	Specifies the name of the policy map to be attached to the *input or output* direction of the interface. **Note** Policy maps can be configured on ingress or egress routers. They can also be attached in the input or output direction of an interface. The direction (input or output) and the router (ingress or egress) to which the policy map should be attached varies according your network configuration. When using the **service-policy** command to attach the policy map to an interface, be sure to choose the router and the interface direction that are appropriate for your network configuration. • Enter the policy map name.
Step 6	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode.

Verifying the Configuration

This task allows you to verify that you created the configuration you intended and that the feature is functioning correctly. To verify the configuration, use the commands in the following sections:

SUMMARY STEPS

1. **enable**
2. **show policy-map**
3. **show policy-map interface** *interface-name*
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show policy-map** **Example:** `Router# show policy-map`	(Optional) Displays all configured policy maps.
Step 3	**show policy-map interface** *interface-name* **Example:** `Router# show policy-map interface s4/0`	(Optional) 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. • Enter the interface name.
Step 4	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode.

Troubleshooting Tips

The commands in the "Verifying the Configuration" section allow you to verify that you achieved the intended configuration and that the feature is functioning correctly. If after using the **show** commands listed above, the configuration is not correct or the feature is not functioning as expected, do the following.

If the configuration is not the one you intended, complete the following procedures:

- Use the **show running-config** command and analyze the output of the command.
- If the policy map does not appear in the output of the **show running-config** command, enable the **logging console** command.
- Attach the policy map to the interface again.

If the packets are not being matched correctly (for example, the packet counters are not incrementing correctly), complete the following procedures:

- Use the **show policy-map** command and analyze the output of the command.
- Use the **show running-config** command and analyze the output of the command.
- Run the **show policy-map interface** command and analyze the output of the command. Review the the following:
  - If a policy map applies queueing and the packets are matching the correct class, but you see unexpected results, compare the number of packets to the number of packets matched.
  - If the interface is congested and you are only seeing a small number of packets matched, check the tuning of the transmisson (tx) ring and evaluate whether the queueing is happening on the tx ring. To do this, use the **show controllers** command and look at the value of the tx count in the show output of the command.

Configuration Examples for Color-Aware Policing

This section provides the following configuration example:

Color-Aware Policing: Example

The following example shows color-aware policing configured in a policy map called "color." Before the feature was configured, the **class-map** command was used to create two classes called "c1" and "c2," respectively. These two classes were configured as shown below:

```
class-map c1
  match ip prec 5
class-map c2
  match ip prec 3
```

With the two classes created, color-aware policing is configured as shown below:

```
Router# enable
Router# configure terminal
Router(config)# policy-map color
Router(config-pmap)# class ccolor
Router(config-pmap-c)# police cir 8000 bc 5000 pir 8000 be 5000 conform-action transmit
exceed-action set-prec-transmit 4 violate-action drop
Router(config-pmap-c-police)# conform-color c1 exceed-color c2
```

Note The traffic class (in this example, ccolor) must still be created using the Modular QoS Command-Line Interface (CLI) (MQC).

With color-aware policing configured as shown, the following results occur based on the CIR, the PIR, and the conform actions, exceed actions, and violate actions specified by the **police** command:

- Packets that have metering rates less than or equal to the CIR and belong to class c1 (conform-color) are policed as conforming to the rate. These packets are also policed according to the conform action specified by the **police** command. In this instance, the packets will be transmitted.
- Packets that have metering rates between the CIR and the PIR and belong to either class c1 (conform-color) or class c2 (exceed-color) are policed as exceeding the CIR. These packets are also policed according to the exceed action specified by the **police** command. In this instance, the precedence value of the packets will be set and the packets transmitted.
- Packets that have metering rates higher than the PIR or belong to *neither* class c1 *or* class c2 are policed as violating the rate. These packets are also policed according to the violate action specified by the **police** command. In this instance, the packets will be dropped.

Additional References

The following sections provide references related to Color-Aware Policing:

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*, Release 12.3 T
Additional information about configuring traffic policing	"Policing and Shaping" section of the *Cisco IOS Quality of Service Solutions Configuration Guide* *http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/index.htm*
MQC	"Configuring the Modular Quality of Service Command-Line Interface" section in the *Cisco IOS Quality of Service Solutions Configuration Guide* *http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/index.htm*
Other traffic policing-related features, such as:	
• Two-rate traffic policing	*Two-Rate Policer*, Cisco IOS Release 12.2(4)T feature module
• Traffic policing using multiple policer actions	*Policer Enhancement — Multiple Actions*, Cisco IOS Release 12.2(8)T feature module
• Percentage-based traffic policing and shaping	*Percentage-Based Policing and Shaping*, Cisco IOS Release 12.2(13)T feature module
• Three-level hierarchical policing	*Modular QoS CLI (MQC) Three-Level Hierarchical Policer*, Cisco IOS Release 12.2(13)T feature module

Standards

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

MIBs

MIBs	MIBs Link
• CISCO-CLASS-BASED-QOS-MIB • CISCO-CLASS-BASED-QOS-CAPABILITY-MIB	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
• RFC 2697	*A Single Rate Three Color Marker*
• RFC 2698	*A Two Rate Three Color Marker*

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3 T command reference publications.

New Commands

- **conform-color**

Modified Commands

- **show policy-map**
- **show policy-map interface**

conform-color

To enable color-aware traffic policing and create the conform-color and exceed-color class maps used for color-aware traffic policing, use the **conform-color** command in policy-map class police configuration mode. To disable the color-aware mode of traffic policing, use the **no** form of this command.

conform-color *class-map-name* [**exceed-color** *class-map-name*]

no conform-color

Syntax Description

class-map-name	Specifies the name of the conform-color class map. This is the class map in which packets conforming to the traffic policing color will be placed. The class-map name can be a maximum of 40 alphanumeric characters.
exceed-color	(Optional) Indicates that an exceed-color class-map name will be specified.
class-map-name	(Optional) Specifies the name of the exceed-color class map. This is the class map in which packets exceeding the traffic policing color will be placed. The name can be a maximum of 40 alphanumeric characters.

Defaults

No default behavior or values

Command Modes

Policy-map class police configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

The **conform-color** command is used in conjunction with the **police** command to configure color-aware policing. The **police** command specifies the committed information rate (CIR), conform burst (bc) size, peak information rate (PIR), and excess burst (be) size used to police packets. The **police** command is also used to specify any optional policing actions (such as transmit, set-clp-transmit, or drop) that can be performed on packets conforming to, exceeding, or violating the specified rates.

When using the **conform-color** command, note the following points:

- If the **exceed-color** keyword and corresponding *class-map-name* argument are not specified, all packets not belonging to the specified conform-color class will belong to the exceed-color class.
- If *both* the conform-color and exceed-color class-map names are specified, packets not belonging to *either* the conform-color class or the exceed-color class will belong to the violate-color class.

Examples

The following example shows color-aware policing configured in a policy map called "color." Before the feature was configured, the **class-map** command was used to create two classes called "c1" and "c2," respectively. These two classes were configured as shown below:

```
class-map c1
  match ip prec 5
class-map c2
  match ip prec 3
```

With the two classes created, color-aware policing is configured as shown below:

```
Router# enable
Router# configure terminal
Router(config)# policy-map color
Router(config-pmap)# class ccolor
Router(config-pmap-c)# police cir 8000 bc 5000 pir 8000 be 5000 conform-action transmit
exceed-action set-prec-transmit 4 violate-action drop
Router(config-pmap-c-police)# conform-color c1 exceed-color c2
```

With color-aware policing configured as shown, the following results occur on the basis of the CIR, the PIR, and the conform actions, exceed actions, and violate actions specified by the **police** command:

- Packets that have metering rates less than or equal to the CIR and belong to class c1 are policed as conforming to the rate. These packets are also policed according to the conform action specified by the **police** command. In this instance, the packets will be transmitted.
- Packets that have metering rates between the CIR and the PIR and belong to class c1 or c2 are policed as exceeding the CIR. These packets are also policed according to the exceed action specified by the **police** command. In this instance, the precedence value of the packets will be set and the packets transmitted.
- Packets that have metering rates higher than the PIR, or belong to *neither* class c1 *or* c2 are policed as violating the rate. These packets are also policed according to the violate action specified by the **police** command. In this instance, the packets will be dropped.

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match precedence	Identifies IP precedence values as match criteria.
police	Configures traffic policing.
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.

show policy-map

To display the configuration of all classes for a specified service policy map or all classes for all existing policy maps, use the **show policy-map** command in EXEC mode.

show policy-map [*policy-map*]

Syntax Description

policy-map	(Optional) Name of the service policy map whose complete configuration is to be displayed.

Defaults

All existing policy map configurations are displayed.

Command Modes

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.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.2(13)T	The output of this command was modified for the Percentage-Based Policing and Shaping feature and includes the bandwidth percentage used when calculating traffic policing and shaping.
12.0(28)S	The output of this command was modified for the QoS: Percentage-Based Policing feature to display the committed (conform) burst (bc) and excess (peak) burst (be) sizes in milliseconds (ms).
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

The **show policy-map** command displays the configuration of a service policy map created using the **policy-map** command. You can use the **show policy-map** command to display all class configurations comprising any existing service policy map, whether or not that service policy map has been attached to an interface.

Examples

The following is sample output from the **show policy-map** command. This sample output displays the contents of a policy map called "policy1." In policy 1, traffic policing on the basis of a committed information rate (CIR) of 20 percent has been configured, and the bc and be have been specified in milliseconds. As part of the traffic policing configuration, optional conform, exceed, and violate actions have been specified.

```
Router# show policy-map policy1
  Policy Map policy1
    Class class1
     police cir percent 20 bc 300 ms pir percent 40 be 400 ms
```

```
conform-action transmit
exceed-action drop
violate-action drop
```

Table 2 describes the significant fields shown in the display.

Table 2 show policy-map Field Descriptions

Field	Description
Policy Map	Name of policy map displayed.
Class	Name of class configured in policy map displayed.
police	Indicates that traffic policing on the basis of specified percentage of bandwidth has been enabled. The committed burst (bc) and excess burst (be) sizes have been specified in milliseconds (ms), and optional conform, exceed, and violate actions have been specified.

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
show policy-map class	Displays the configuration for the specified class of the specified policy map.
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 packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific permanent virtual circuit (PVC) on the interface, use the **show policy-map interface** command in EXEC mode.

show policy-map interface *interface-name* [**vc** [*vpi/*] *vci*][**dlci** *dlci*] [**input** | **output**]

Syntax Description

interface-name	Name of the interface or subinterface whose policy configuration is to be displayed.
vc	(Optional) For ATM interfaces only, shows the policy configuration for a specified PVC. The name can be up to 16 characters long.
vpi/	(Optional) ATM network virtual path identifier (VPI) for this PVC. On the Cisco 7200 and 7500 series routers, this value ranges from 0 to 255. 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. The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0.
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) 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.

Defaults

No default behavior or values

Command Modes

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.
12.1(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 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 to display burst parameters and associated actions.
12.2(8)T	This command was modified to display the multiple actions configured for packets conforming to, exceeding, or violating a specific rate.
12.0(28)S	The output of 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.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

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

Examples

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 s2/0
 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

When calculating the CIR, the following formula is used:

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

According to the output of 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

When calculating the PIR, the following formula is used:

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

According to the output of 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 PIR:

40 % * 2048 kbps = 819200 bps

Note Discrepancies between this total and the total shown in the output of 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)

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)

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 3 describes the significant fields shown in the display.

Table 3 show policy-map interface Field Descriptions[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 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 options that are available, refer to the "Configuring the Modular Quality of Service Command-Line Interface" chapter of 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.

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.

Related Commands

Command	Description
police (percent)	Configures traffic policing on the basis of a percentage of bandwidth available on an interfaces.
shape (percent)	Specifies average or peak rate traffic shaping on the basis of a percentage of bandwidth available on an interface.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
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.