



---

Junos<sup>®</sup> OS

# CoS Ingress Traffic Policing Feature Guide for Routing Devices

Release  
13.2



---

Published: 2013-07-31

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

*Junos® OS CoS Ingress Traffic Policing Feature Guide for Routing Devices*

13.2

Copyright © 2013, Juniper Networks, Inc.  
All rights reserved.

The information in this document is current as of the date on the title page.

## YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

## END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

	About the Documentation . . . . .	xi
	Documentation and Release Notes . . . . .	xi
	Supported Platforms . . . . .	xi
	Using the Examples in This Manual . . . . .	xi
	Merging a Full Example . . . . .	xii
	Merging a Snippet . . . . .	xii
	Documentation Conventions . . . . .	xiii
	Documentation Feedback . . . . .	xv
	Requesting Technical Support . . . . .	xv
	Self-Help Online Tools and Resources . . . . .	xv
	Opening a Case with JTAC . . . . .	xvi
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Tricolor Marking Policers . . . . .</b>	<b>3</b>
	Traffic Policing Overview . . . . .	3
	Congestion Management for IP Traffic Flows . . . . .	3
	Traffic Limits . . . . .	4
	Traffic Color Marking . . . . .	5
	Forwarding Classes and PLP Levels . . . . .	6
	Policer Application to Traffic . . . . .	7
	Policer Overview . . . . .	8
	Platform Support for Tricolor Marking . . . . .	10
	Tricolor Marking Architecture . . . . .	11
	Tricolor Marking Limitations . . . . .	12
	Policer Support for Aggregated Ethernet Bundle Overview . . . . .	13
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 2</b>	<b>Configuration Tasks for Tricolor Marking Policers . . . . .</b>	<b>17</b>
	Configuring Tricolor Marking . . . . .	17
	Configuring Single-Rate Tricolor Marking . . . . .	18
	Configuring Color-Blind Mode for Single-Rate Tricolor Marking . . . . .	19
	Configuring Color-Aware Mode for Single-Rate Tricolor Marking . . . . .	19
	Effect on Low PLP of Single-Rate Policer . . . . .	20
	Effect on Medium-Low PLP of Single-Rate Policer . . . . .	20
	Effect on Medium-High PLP of Single-Rate Policer . . . . .	21
	Effect on High PLP of Single-Rate Policer . . . . .	21

	Configuring Two-Rate Tricolor Marking . . . . .	21
	Configuring Color-Blind Mode for Two-Rate Tricolor Marking . . . . .	22
	Configuring Color-Aware Mode for Two-Rate Tricolor Marking . . . . .	22
	Effect on Low PLP of Two-Rate Policer . . . . .	23
	Effect on Medium-Low PLP of Two-Rate Policer . . . . .	23
	Effect on Medium-High PLP of Two-Rate Policer . . . . .	24
	Effect on High PLP of Two-Rate Policer . . . . .	24
	Enabling Tricolor Marking . . . . .	24
	Configuring Tricolor Marking Policers . . . . .	25
	Applying Tricolor Marking Policers to Firewall Filters . . . . .	26
	Example: Applying a Two-Rate Tricolor Marking Policer to a Firewall Filter . . . . .	27
	Applying Firewall Filter Tricolor Marking Policers to Interfaces . . . . .	28
	Example: Applying a Single-Rate Tricolor Marking Policer to an Interface . . . . .	28
	Applying Layer 2 Policers to Gigabit Ethernet Interfaces . . . . .	29
	Examples: Applying Layer 2 Policers to a Gigabit Ethernet Interface . . . . .	29
<b>Chapter 3</b>	<b>Configuration Tasks for Packet Loss Priority . . . . .</b>	<b>31</b>
	Using BA Classifiers to Set PLP . . . . .	31
	Using Multifield Classifiers to Set PLP . . . . .	32
	Configuring PLP for Drop-Profile Maps . . . . .	33
	Configuring Rewrite Rules Based on PLP . . . . .	34
<b>Chapter 4</b>	<b>Tricolor Marking Policers Example . . . . .</b>	<b>35</b>
	Example: Configuring and Verifying Two-Rate Tricolor Marking . . . . .	35
	Applying a Policer to the Input Interface . . . . .	35
	Applying Profiles to the Output Interface . . . . .	36
	Marking Packets with Medium-Low Loss Priority . . . . .	37
	Verifying Two-Rate Tricolor Marking Operation . . . . .	38
<b>Chapter 5</b>	<b>Configuration Statements for Tricolor Marking Policers . . . . .</b>	<b>39</b>
	action . . . . .	40
	classifiers (Definition) . . . . .	41
	code-points . . . . .	42
	drop-profile (Schedulers) . . . . .	43
	drop-profile-map (Schedulers) . . . . .	43
	dscp (Multifield Classifier) . . . . .	44
	dscp (Rewrite Rules) . . . . .	45
	dscp-ipv6 (Class-of-Service) . . . . .	46
	exp . . . . .	47
	family (Multifield Classifier) . . . . .	48
	filter (Applying to a Logical Interface) . . . . .	49
	filter (Configuring) . . . . .	50
	firewall . . . . .	51
	forwarding-class (BA Classifiers) . . . . .	52
	ieee-802.1 (Rewrite Rules on Logical Interface) . . . . .	53
	import (Classifiers) . . . . .	54
	import (Rewrite Rules) . . . . .	54
	inet-precedence . . . . .	55
	input-policer . . . . .	56

input-three-color .....	57
layer2-policer .....	58
logical-interface-policer .....	59
loss-priority (Normal Filter) .....	60
loss-priority (Simple Filter) .....	60
loss-priority (Scheduler Drop Profiles) .....	61
output-policer .....	62
output-three-color .....	63
policer (Configuring) .....	64
protocol (Schedulers) .....	66
rewrite-rules (Definition) .....	67
schedulers (Class of Service) .....	68
shared-bandwidth-policer .....	69
then .....	70
three-color-policer (Applying) .....	71
three-color-policer (Configuring) .....	72
tri-color .....	73

## Part 3

## Index

Index .....	77
-------------	----



# List of Figures

<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Tricolor Marking Policers .....</b>	<b>3</b>
	Figure 1: Network Traffic and Burst Rates .....	5
	Figure 2: Flow of Tricolor Marking Policer Operation .....	11
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 4</b>	<b>Tricolor Marking Policers Example .....</b>	<b>35</b>
	Figure 3: Tricolor Marking Sample Topology .....	35





# List of Tables

	<b>About the Documentation . . . . .</b>	<b>xi</b>
	Table 1: Notice Icons . . . . .	xiii
	Table 2: Text and Syntax Conventions . . . . .	xiii
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Tricolor Marking Policers . . . . .</b>	<b>3</b>
	Table 3: Policer Actions . . . . .	9
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 2</b>	<b>Configuration Tasks for Tricolor Marking Policers . . . . .</b>	<b>17</b>
	Table 4: Color-Blind Mode TCM Color-to-PLP Mapping . . . . .	19
	Table 5: Color-Aware Mode TCM PLP Mapping . . . . .	20
	Table 6: Color-Blind Mode TCM Color-to-PLP Mapping . . . . .	22
	Table 7: Color-Aware Mode TCM Mapping . . . . .	23
	Table 8: Tricolor Marking Policer Statements . . . . .	26



# About the Documentation

- Documentation and Release Notes on page xi
- Supported Platforms on page xi
- Using the Examples in This Manual on page xi
- Documentation Conventions on page xiii
- Documentation Feedback on page xv
- Requesting Technical Support on page xv

## Documentation and Release Notes

---

To obtain the most current version of all Juniper Networks<sup>®</sup> technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

## Supported Platforms

---

For the features described in this document, the following platforms are supported:

- T Series
- M Series
- MX Series
- PTX Series

## Using the Examples in This Manual

---

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

## Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

## Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the *CLI User Guide*.

## Documentation Conventions

Table 1 on page xiii defines notice icons used in this guide.

Table 1: Notice Icons





Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xiii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> <b>show chassis alarms</b> No alarms currently active

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces or emphasizes important new terms.</li> <li>Identifies book names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS System Basics Configuration Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name:  [edit] root@# <b>set system domain-name</b> <i>domain-name</i>
<b>Text like this</b>	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the [edit protocols ospf area area-id] hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul>
< > (angle brackets)	Enclose optional keywords or variables.	<b>stub</b> <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	<b>broadcast   multicast</b>  ( <i>string1</i>   <i>string2</i>   <i>string3</i> )
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	<b>community name members [</b> <i>community-ids</i> <b>]</b>
Indentation and braces ( { } )	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
<b>GUI Conventions</b>		
<b>Bold text like this</b>	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> <li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li> <li>To cancel the configuration, click <b>Cancel</b>.</li> </ul>
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

---

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

## Requesting Technical Support

---

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>

- Join and participate in the Juniper Networks Community Forum:  
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

## Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.



## PART 1

# Overview

- [Tricolor Marking Policers on page 3](#)



## CHAPTER 1

# Tricolor Marking Policers

- [Traffic Policing Overview on page 3](#)
- [Policer Overview on page 8](#)
- [Platform Support for Tricolor Marking on page 10](#)
- [Tricolor Marking Architecture on page 11](#)
- [Tricolor Marking Limitations on page 12](#)
- [Policer Support for Aggregated Ethernet Bundle Overview on page 13](#)

## Traffic Policing Overview

---

This topic covers the following information:

- [Congestion Management for IP Traffic Flows on page 3](#)
- [Traffic Limits on page 4](#)
- [Traffic Color Marking on page 5](#)
- [Forwarding Classes and PLP Levels on page 6](#)
- [Policer Application to Traffic on page 7](#)

## Congestion Management for IP Traffic Flows

Traffic policing, also known *rate limiting*, is an essential component of network access security that is designed to thwart denial-of-service (DoS) attacks. Traffic policing enables you to control the maximum rate of IP traffic sent or received on an interface and also to partition network traffic into multiple priority levels, also known as *classes of service*. A policer defines a set of traffic rate limits and sets consequences for traffic that does not conform to the configured limits. Packets in a traffic flow that does not conform to traffic limits are either discarded or marked with a different forwarding class or packet loss priority (PLP) level.

With the exception of policers configured to rate-limit aggregate traffic (all protocol families and logical interfaces configured on a physical interface), you can apply a policer to all IP packets in a Layer 2 or Layer 3 traffic flow at a logical interface.

With the exception of policers configured to rate-limit based on physical interface media rate, you can apply a policer to specific IP packets in a Layer 3 traffic flow at a logical interface by using a stateless firewall filter.

You can apply a policer to inbound or outbound interface traffic. Policers applied to inbound traffic help to conserve resources by dropping traffic that does not need to be routed through a network. Dropping inbound traffic also helps to thwart denial-of-service (DoS) attacks. Policers applied to outbound traffic control the bandwidth used.



**NOTE:** Traffic policers are instantiated on a per-PIC basis. Traffic policing does not work when the traffic for one local policy decision function (L-PDF) subscriber is distributed over multiple Multiservices PICs in an AMS group.

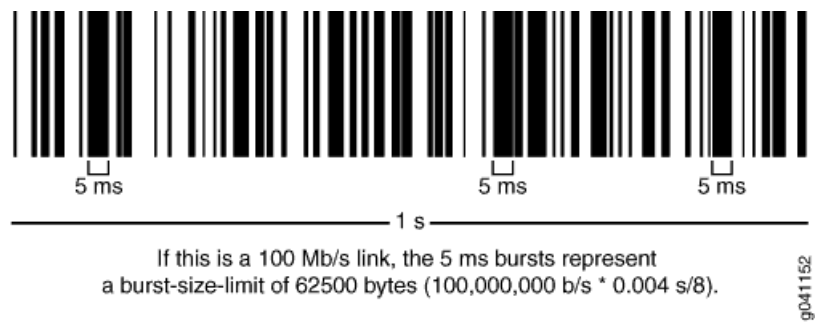
## Traffic Limits

Junos<sup>®</sup> operating system (Junos OS) policers use the *token-bucket* algorithm to enforce a limit on average transmit or receive rate of IP traffic at an interface while allowing bursts of traffic up to a maximum value based on the overall traffic load. The token-bucket algorithm offers more flexibility than the *leaky-bucket* algorithm in that you can allow a specified amount of bursting before starting to discard packets or apply a penalty to packet output-queuing priority or packet drop priority.

In the token-bucket model, the bucket represents the policing function. Tokens are added to the bucket at a fixed rate, but only up to the specified depth of the bucket. Each token represents a “credit” for some number of bits, and tokens in the bucket are “cashed in” for the ability to transmit or receive traffic at the interface. When sufficient tokens are present in the bucket, a traffic flow continues unrestricted. Otherwise, packets might be dropped or else re-marked with a lower forwarding class, a higher packet loss priority (PLP) level, or both.

- The rate at which tokens are added to the bucket represents the highest average transmit or receive rate in bits per second allowed for a given service level. You specify this highest average traffic rate as the *bandwidth limit* of the policer. If the traffic arrival rate is so high that at some point insufficient tokens are present in the bucket, then the traffic flow is no longer conforming to the traffic limit.
- The depth of the bucket in bytes controls the amount of back-to-back bursting allowed. You specify this factor as the *burst-size limit* of the policer. This second limit affects the average transmit or receive rate by limiting the number of bytes permitted in a transmission burst for a given interval of time. Bursts exceeding the current burst-size limit are dropped until there are sufficient tokens available to permit the burst to proceed.

Figure 1: Network Traffic and Burst Rates



As shown in the figure above, a UPC bar code is a good facsimile of what traffic looks like on the line; an interface is either transmitting (bursting at full rate) or it is not. The black lines represent periods of data transmission and the white space represents periods of silence when the token bucket can replenish.

Depending on the type of policer used, packets in a policed traffic flow that surpasses the defined limits might be implicitly set to a higher PLP level, assigned to a configured forwarding class or set to a configured PLP level (or both), or simply discarded. If packets encounter downstream congestion, packets with a **low** PLP level are less likely to be discarded than those with a **medium-low**, **medium-high**, or **high** PLP level.

## Traffic Color Marking

Based on the particular set of traffic limits configured, a policer identifies a traffic flow as belonging to one of either two or three categories that are similar to the colors of a traffic light used to control automobile traffic.

A *two-color-marking* policer categorizes traffic as either conforming to the traffic limits (green) or violating the traffic limits (red):

- **Green**—Two-color-marking policers implicitly set the packets in a green flow to the low PLP level, and you cannot configure any policer actions for conforming traffic.
- **Red**—Two-color-marking policers do not perform any implicit actions on packets in a red flow. Instead, those packets are handled according to the actions specified in the policer configuration. You can configure a two-color-marking policer to simply discard packets if the traffic flow is red. Alternatively, you can configure a two-color-marking policer to handle the packets in a red flow by setting the PLP level to either **low** or **high**, assigning the packets to any forwarding class already configured, or both.

On MX Series, M120, and M320 routers and M7i and M10i routers with the Enhanced CFEB (CFEB-E) and EX Series switches only, you can specify two additional PLP levels for packets in a red flow: **medium-low** or **medium-high**.

*Three-color-marking* policers categorize traffic as conforming to the traffic limits (green), violating the traffic limits (red), or exceeding the traffic limits but within an allowed range (yellow):

- Green—Like two-color-marking policers, three-color-marking policers implicitly set the packets in a green flow to the low PLP level, and you cannot configure any policer actions for conforming traffic.
- Yellow—Unlike two-color-marking policers, three-color-marking policers categorize a second type of nonconforming traffic: yellow.

Single-rate three-color policing categorizes as yellow traffic that exceeds the traffic limits while conforming to a second defined burst-size limit. Two-rate three-color policing categorizes as yellow traffic that exceeds the traffic limits while conforming to both a second defined burst-size limit and a second defined bandwidth limit.

Three-color-marking policers implicitly set the packets in a yellow flow to the medium-high PLP level so that the packets incur a less severe penalty than those in a red flow. You cannot configure any policer actions for yellow traffic.

- Red—Unlike two-color-marking policers, three-color-marking policers implicitly set the packets in a red flow to the high PLP level, which is the highest PLP value. You can also configure a three-color-marking policer to discard the packets in a red flow instead of forwarding them with a high PLP setting.

Two-color-marking policers allows bursts of traffic for short periods, whereas three-color-marking policers allow more sustained bursts of traffic.

## Forwarding Classes and PLP Levels

A packet's forwarding class assignment and PLP level are used by the Junos OS class of service (CoS) features. The Junos CoS features include a set of mechanisms that you can use to provide differentiated services when best-effort traffic delivery is insufficient. For router (and switch) interfaces that carry IPv4, IPv6, and MPLS traffic, you can configure CoS features to take in a single flow of traffic entering at the edge of your network and provide different levels of service across the network—internal forwarding and scheduling (queuing) for output—based on the forwarding class assignments and PLP levels of the individual packets.



**NOTE:** Forwarding-class or loss-priority assignments performed by a policer or a stateless firewall filter override any such assignments performed on the ingress by the CoS default IP precedence classification at all logical interfaces or by any configured behavior aggregate (BA) classifier that is explicitly mapped to a logical interface.

Based on CoS configurations, packets of a given forwarding class are transmitted through a specific output queue, and each output queue is associated with a transmission service level defined in a *scheduler*.

Based on other CoS configurations, when packets in an output queue encounter congestion, packets with higher loss-priority values are more likely to be dropped by the

random early detection (RED) algorithm. Packet loss priority values affect the scheduling of a packet without affecting the packet's relative ordering within the traffic flow.

## Policer Application to Traffic

After you have defined and named a policer, it is stored as a template. You can later use the same policer name to provide the same policer configuration each time you want to use it. This eliminates the need to define the same policer values more than once.

You can apply a policer to a traffic flow in either of two ways:

- You can configure a standard stateless firewall filter that specifies the **police** *police-name* nonterminating action or the **three-color-policer (single-rate | two-rate)** *police-name* nonterminating action. When you apply the standard filter to the input or output at a logical interface, the policer is applied to all packets of the filter-specific protocol family that match the conditions specified in the filter configuration.

With this method of applying a policer, you can define specific classes of traffic on an interface and apply traffic rate-limiting to each class.

- You can apply a policer directly to an interface so that traffic rate-limiting applies to all traffic on that interface, regardless of protocol family or any match conditions.

You can configure policers at the queue, logical interface, or Layer 2 (MAC) level. Only a single policer is applied to a packet at the egress queue, and the search for policers occurs in this order:

- Queue level
- Logical interface level
- Layer 2 (MAC) level

### Related Documentation

- *Stateless Firewall Filter Overview.*
- *Traffic Policer Types*
- *Order of Policer and Firewall Filter Operations*
- *Packet Flow Through the CoS Process Overview*

## Policer Overview

---

*Policing*, or rate limiting, enables you to limit the amount of traffic that passes into or out of an interface. It is an essential component of firewall filters that is designed to thwart denial-of-service (DoS) attacks. 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 classes of service.

Policers require you to apply limits to the traffic flow and set a consequence for packets that exceed these limits—usually a higher loss priority—so that if packets encounter downstream congestion, they are discarded first.

Policing uses the *token-bucket algorithm*, which enforces a limit on average bandwidth while allowing bursts up to a specified maximum value. It offers more flexibility than the *leaky bucket algorithm* (see the *Junos OS Class of Service Library for Routing Devices*) in allowing a certain amount of bursty traffic before it starts discarding packets.

You can define specific classes of traffic on an interface and apply a set of rate limits to each. You can use a policer in one of two ways: as part of a filter configuration or as part of a logical interface (where the policer is applied to all traffic on that interface).

After you have defined and named a policer, it is stored as a template. You can later use the same policer name to provide the same policer configuration each time you wish to use it. This eliminates the need to define the same policer values more than once.

Juniper Networks routing platform architectures can support three types of policer:

- **Single-rate two-color**—A two-color policer (or “policer” when used without qualification) meters the traffic stream and classifies packets into two categories of packet loss priority (PLP) according to a configured bandwidth and burst-size limit. You can mark packets that exceed the bandwidth and burst-size limit in some way, or simply discard them. A policer is most useful for metering traffic at the port (physical interface) level.
- **Single-rate three-color**—This type of policer is defined in RFC 2697, *A Single Rate Three Color Marker*, as part of an assured forwarding (AF) per-hop-behavior (PHB) classification system for a Differentiated Services (DiffServ) environment. This type of policer meters traffic based on the configured committed information rate (CIR), committed burst size (CBS), and the excess burst size (EBS). Traffic is marked as belonging to one of three categories (green, yellow, or red) based on whether the packets arriving are below the CBS (green), exceed the CBS (yellow) but not the EBS, or exceed the EBS (red). A single-rate three-color policer is most useful when a service is structured according to packet length and not peak arrival rate.
- **Two-rate three-color**—This type of policer is defined in RFC 2698, *A Two Rate Three Color Marker*, as part of an assured forwarding (AF) per-hop-behavior (PHB) classification system for a Differentiated Services (DiffServ) environment. This type of policer meters traffic based on the configured CIR and peak information rate (PIR), along with their associated burst sizes, the CBS and *peak burst size* (PBS). Traffic is marked as belonging to one of three categories (green, yellow, or red) based on whether the packets arriving are below the CIR (green), exceed the CIR (yellow) but not the



PIR, or exceed the PIR (red). A two-rate three-color policer is most useful when a service is structured according to arrival rates and not necessarily packet length.

Policer actions are implicit or explicit and vary by policer type. The term *Implicit* means that Junos assigns the loss-priority automatically. [Table 3 on page 9](#) describes the policer actions.

**Table 3: Policer Actions**

Policer	Marking	Implicit Action	Configurable Action
Single-rate two-color	Green (Conforming)	Assign low loss priority	None
	Red (Nonconforming)	None	Assign low or high loss priority, assign a forwarding class, or discard On some platforms, you can assign medium-low or medium-high loss priority
Single-rate three-color	Green (Conforming)	Assign low loss priority	None
	Yellow (Above the CIR and CBS)	Assign medium-high loss priority	None
	Red (Above the EBS)	Assign high loss priority	Discard
Two-rate three-color	Green (Conforming)	Assign low loss priority	None
	Yellow (Above the CIR and CBS)	Assign medium-high loss priority	None
	Red (Above the PIR and PBS)	Assign high loss priority	Discard

You can configure policers at the queue, logical interface, or Layer 2 (MAC) level. Only a single policer is applied to a packet at the egress queue, and the search for policers occurs in this order:

- Queue level
- Logical interface level
- Layer 2 (MAC) level

Three-color policers are not bound by a green-yellow-red coloring convention. Packets are marked with low, medium-high, or high PLP bit configurations based on color, so both three-color policer schemes extend the functionality of class-of-service (CoS) traffic

policing by providing three levels of drop precedence (loss priority) instead of the two normally available in port-level policers. Both single-rate and two-rate three-color policer schemes can operate in two modes:

- **Color-blind**—In color-blind mode, the three-color policer assumes that all packets examined have not been previously marked or metered. In other words, the three-color policer is “blind” to any previous coloring a packet might have had.
- **Color-aware**—In color-aware mode, the three-color policer assumes that all packets examined have been previously marked or metered. In other words, the three-color policer is “aware” of the previous coloring a packet might have had. In color-aware mode, the three-color policer can increase the PLP of a packet, but never decrease it. For example, if a color-aware three-color policer meters a packet with a medium PLP marking, it can raise the PLP level to high, but cannot reduce the PLP level to low.



**NOTE:** We recommend you use the naming convention ***policertypeTCM#-color type*** when configuring three-color policers and ***policer#*** when configuring two-color policers. TCM stands for three-color marker. Because policers can be numerous and must be applied correctly to work, a simple naming convention makes it easier to apply the policers properly.

---

For example, the first single-rate, color-aware three-color policer configured would be named **srTCM1-ca**. The second two-rate, color-blind three-color configured would be named **trTCM2-cb**.

## Platform Support for Tricolor Marking

---

Tricolor marking is supported on the following Juniper Networks routers:

- M120 Multiservice Edge Routers
- M320 Multiservice Edge Routers and T Series Core Routers with Enhanced II Flexible PIC Concentrators (FPCs)
- MX Series 3D Universal Edge Routers
- T640 Core Routers with Enhanced Scaling FPC4
- T640 and T1600 Core Routers with Enhanced Scaling FPC3
- T1600 Core Routers with T1600 Enhanced Scaling FPC4
- T4000 Core Routers



**NOTE:** On MX Series and M120 routers, you can apply three-color policers to aggregated interfaces.

---



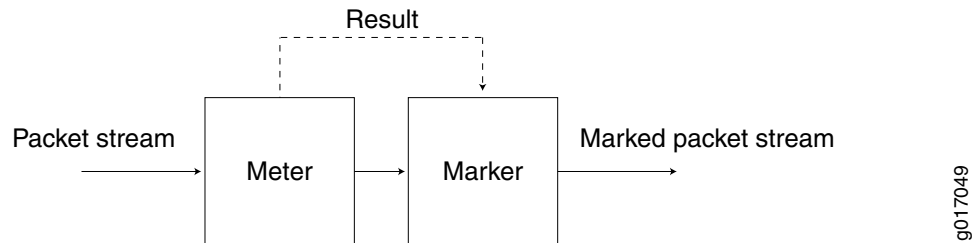
**NOTE:** On T Series routers, three-color policers and hierarchical policers are supported on aggregated interfaces if all child links are hosted on Enhanced Scaling FPCs.

## Tricolor Marking Architecture

Policers provide two functions: metering and marking.

The policer meters each packet and passes the packet and the metering result to the marker, as shown in [Figure 2 on page 11](#).

**Figure 2: Flow of Tricolor Marking Policer Operation**



The meter operates in two modes. In the color-blind mode, the meter treats the packet stream as uncolored. Any preset loss priorities are ignored. In the color-aware mode, the meter inspects the packet loss priority (PLP) field, which has been set by an upstream device as PLP high, medium-high, medium-low, or low; in other words, the PLP field has already been set by a behavior aggregate (BA) or multifield classifier. The marker changes the PLP of each incoming IP packet according to the results of the meter. For more information, see [“Configuring Two-Rate Tricolor Marking” on page 21](#).

This chapter emphasizes configuration and use of TCM policers. For more information about configuring and using two-color policers (“policers”), see the *Traffic Policers Feature Guide for Routing Devices*.

Single-rate TCM is so called because traffic is policed according to one rate—the CBR—and two burst sizes: the CBS and EBS. The CBS specifies the usual burst size in bytes and the EBS specifies the maximum burst size in bytes for packets that are admitted to the network. The EBS is greater than or equal to the CBS, and neither can be 0. As each packet enters the network, its bytes are counted. Packets that do not exceed the CBS are marked low PLP. Packets that exceed the CBS but are below the EBS are marked medium-high PLP. Packets that exceed the EBS are marked high PLP.

Two-rate TCM is so called because traffic is policed according to two rates: the CIR and the PIR. The PIR is greater than or equal to the CIR. The CIR specifies the average rate at which bits are admitted to the network and the PIR specifies the maximum rate at which bits are admitted to the network. As each packet enters the network, its bits are counted. Bits in packets that do not exceed the CIR have their packets marked low PLP. Bits in packets that exceed the CIR but are below the PIR have their packets marked medium-high PLP. Bits in packets that exceed the PIR have their packets marked high PLP.

For information about how to use marking policers with BA and multifield classifiers, see [“Using BA Classifiers to Set PLP” on page 31](#) and [“Using Multifield Classifiers to Set PLP” on page 32](#).

## Tricolor Marking Limitations

---

Tricolor Marking (TCM) has some limitations that must be kept in mind during configuration and operation.

The following limitations apply to TCM:

- When you enable TCM on a 10-port Gigabit Ethernet PIC or a 10-Gigabit Ethernet PIC, for queues 6 and 7 only, the output of the **show interfaces queue *interface-name*** command does not display the number of queued bytes and packets, or the number of bytes and packets dropped due to RED. If you do not configure tricolor marking on the interface, these statistics are available for all queues.
- When you enable TCM, Transmission Control Protocol (TCP)-based configurations for drop profiles are rejected. In other words, you cannot include the **protocol** statement at the **[edit class-of-service schedulers *scheduler-name* drop-profile-map]** hierarchy level. The result is that drop profiles are applied to packets with the specified PLP and any protocol type.
- On Gigabit Ethernet IQ PICs, for IEEE 802.1 rewrite rules, only two loss priorities are supported. Exiting packets with medium-high loss priority are treated as high, and packets with medium-low loss priority are treated as low. In other words rewrite rules corresponding to high and low apply instead of those corresponding to medium-high and medium-low. For IQ PICs, you can only configure one IEEE 802.1 rewrite rule on a physical port. All logical ports (units) on that physical port should apply the same IEEE 802.1 rewrite rule.
- When some PICs with Frame Relay encapsulation mark a packet with high loss priority, the packet is treated as having medium-high loss priority on M320 Multiservice Edge Routers and T Series Core Routers with Enhanced II FPCs and T640 Core Routers with Enhanced Scaling FPC4.
- TCM is not supported on aggregated Ethernet and aggregated SONET/SDH interfaces.
- In a single firewall filter term, you cannot configure both the **loss-priority** action modifier and the **three-color-policer** action modifier. These statements are mutually exclusive.

## Policer Support for Aggregated Ethernet Bundle Overview

Aggregated interfaces support single-rate policers, three-color marking policers, two-rate three-color marking policers, hierarchical policers, and percentage-based policers. By default, policer bandwidth and burst-size applied on aggregated bundles is not matched to the user-configured bandwidth and burst-size.

You can configure interface-specific policers applied on an aggregated Ethernet bundle or an aggregated SONET bundle to match the effective bandwidth and burst-size to user-configured values. The **shared-bandwidth-policer** statement is required to achieve this match behavior.

This capability applies to all interface-specific policers of the following types: single-rate policers, single-rate three-color marking policers, two-rate three-color marking policers, and hierarchical policers. Percentage-based policers match the bandwidth to the user-configured values by default, and do not require shared-bandwidth-policer configuration. The **shared-bandwidth-policer** statement causes a split in burst-size for percentage-based policers.



**NOTE:** This feature is supported on the following platforms: T Series routers, M120, M10i, M7i (CFEB-E only), M320 (SFPC only), MX240, MX480, and MX960 (DPC only), and EX Series switches.

The following usage scenarios are supported:

- Interface policers used by the following configuration:  

```
[edit] interfaces (aeX | asX) unit unit-num family family policer [input | output | arp]
```
- Policers and three-color policers (both single-rate three-color marking and two-rate three-color marking) used inside interface-specific filters; that is, filters that have an interface-specific keyword and are used by the following configuration:  

```
[edit] interfaces (aeX | asX) unit unit-num family family filter [input | output]
```
- Common-edge service filters, which are derived from CLI-configured filters and thus inherit interface-specific properties. All policers and three-color policers used by these filters are also affected.

The following usage scenarios are not supported:

- Policers and three-color policers used inside filters that are not interface specific; such a filter is meant to be shared across multiple interfaces.
- Any implicit policers or policers that are part of implicit filters; for example, the default ARP policer applied to an aggregate Ethernet interface. Such a policer is meant to be shared across multiple interfaces.
- Prefix-specific action policers.

To configure this feature, include the **shared-bandwidth-policer** statement at the following hierarchy levels: **[edit firewall policer *policer-name*]**, **[edit firewall three-color-policer *policer-name*]**, or **[edit firewall hierarchical-policer *policer-name*]**.

**Related Documentation**

- [shared-bandwidth-policer on page 69](#)

## PART 2

# Configuration

- [Configuration Tasks for Tricolor Marking Policers on page 17](#)
- [Configuration Tasks for Packet Loss Priority on page 31](#)
- [Tricolor Marking Policers Example on page 35](#)
- [Configuration Statements for Tricolor Marking Policers on page 39](#)





## CHAPTER 2

# Configuration Tasks for Tricolor Marking Policers

- [Configuring Tricolor Marking on page 17](#)
- [Configuring Single-Rate Tricolor Marking on page 18](#)
- [Configuring Two-Rate Tricolor Marking on page 21](#)
- [Enabling Tricolor Marking on page 24](#)
- [Configuring Tricolor Marking Policers on page 25](#)
- [Applying Tricolor Marking Policers to Firewall Filters on page 26](#)
- [Applying Firewall Filter Tricolor Marking Policers to Interfaces on page 28](#)
- [Applying Layer 2 Policers to Gigabit Ethernet Interfaces on page 29](#)

## Configuring Tricolor Marking

---

You configure marking policers by defining the policer and multiple levels of PLP for classifiers, rewrite rules, random early detection (RED) drop profiles, and firewall filters. To configure marking policers, include the following statements at the **[edit class-of-service]** hierarchy level:

```
[edit class-of-service]
tri-color;
classifiers {
  (dscp | dscp-ipv6 | exp | ieee-802.1 | inet-precedence) classifier-name {
    import classifier-name | default;
    forwarding-class class-name {
      loss-priority (low | medium-low | medium-high | high) code-points [ aliases ]
        [ bit-patterns ];
    }
  }
}
rewrite-rules {
  (dscp | dscp-ipv6 | exp | ieee-802.1 | inet-precedence) rewrite-name {
    import (rewrite-name | default);
    forwarding-class class-name {
      loss-priority (low | medium-low | medium-high | high) code-point (aliases |
        bit-patterns;
    }
  }
}
```

```
}
schedulers {
  scheduler-name {
    drop-profile-map loss-priority (any | low | medium-low | medium-high | high) protocol
    any drop-profile profile-name;
  }
}

[edit firewall]
policer name {
  then loss-priority (low | medium-low | medium-high | high);
}
three-color-policer policer-name {
  action {
    loss-priority high then discard; # Only for IQ2 PICs
  }
  logical-interface-policer;
  single-rate {
    (color-aware | color-blind);
    committed-information-rate bps;
    committed-burst-size bytes;
    excess-burst-size bytes;
  }
  two-rate {
    (color-aware | color-blind);
    committed-information-rate bps;
    committed-burst-size bytes;
    peak-information-rate bps;
    peak-burst-size bytes;
  }
}
filter filter-name {
  <family family> {
    term rule-name {
      then {
        three-color-policer (single-rate | two-rate) policer-name;
      }
    }
  }
}
```

**Related Documentation**

- [Traffic Policing Overview on page 3](#)

---

## Configuring Single-Rate Tricolor Marking

With TCM, you can configure traffic policing according to two separate modes—color-blind and color-aware. In color-blind mode, the current PLP value is ignored. In color-aware mode, the current PLP values are considered by the policer and can only be increased.

- [Configuring Color-Blind Mode for Single-Rate Tricolor Marking on page 19](#)
- [Configuring Color-Aware Mode for Single-Rate Tricolor Marking on page 19](#)

## Configuring Color-Blind Mode for Single-Rate Tricolor Marking

All packets are evaluated by the CBS. If a packet exceeds the CBS, it is evaluated by the EBS. In color-blind mode, the policer supports three loss priorities only: low, medium-high, and high.

In color-blind mode, packets that exceed the CBS but are below the EBS are marked yellow (medium-high). Packets that exceed the EBS are marked red (high), as shown in [Table 4 on page 19](#).

**Table 4: Color-Blind Mode TCM Color-to-PLP Mapping**

Color	PLP	Meaning
Green	low	Packet does not exceed the CBS.
Yellow	medium-high	Packet exceeds the CBS but does not exceed the EBS.
Red	high	Packet exceeds the EBS.

If you are using color-blind mode and you wish to configure an output policer that marks packets to have medium-low loss priority, you must configure a policer at the **[edit firewall policer *policer-name*]** hierarchy level. For example:

```
firewall {
  policer 4PLP {
    if-exceeding {
      bandwidth-limit 40k;
      burst-size-limit 4k;
    }
    then loss-priority medium-low;
  }
}
```

Apply this policer at one or both of the following hierarchy levels:

- **[edit firewall family *family* filter *filter-name* term *rule-name* then policer *policer-name*]**
- **[edit interfaces *interface-name* unit *logical-unit-number* family *family* filter *filter-name*]**

## Configuring Color-Aware Mode for Single-Rate Tricolor Marking

In color-aware mode, the metering treatment the packet receives depends on its classification. Metering can increase a packet's preassigned PLP, but cannot decrease it, as shown in [Table 5 on page 20](#).

Table 5: Color-Aware Mode TCM PLP Mapping

Incoming PLP	Packet Metered Against	Possible Cases	Outgoing PLP
<b>low</b>	CBS and EBS	Packet does not exceed the CBS.	<b>low</b>
		Packet exceeds the CBS but not the EBS.	<b>medium-high</b>
		Packet exceeds the EBS.	<b>high</b>
<b>medium-low</b>	EBS only	Packet does not exceed the CBS.	<b>medium-low</b>
		Packet does not exceed the EBS.	<b>medium-low</b>
		Packet exceeds the EBS.	<b>high</b>
<b>medium-high</b>	EBS only	Packet does not exceed the CBS.	<b>medium-high</b>
		Packet does not exceed the EBS.	<b>medium-high</b>
		Packet exceeds the EBS.	<b>high</b>
<b>high</b>	Not metered by the policer.	All cases.	<b>high</b>

The following sections describe single-rate color-aware PLP mapping in more detail.

#### Effect on Low PLP of Single-Rate Policer

Packets belonging to the green class have already been marked by a classifier with low PLP. The marking policer can leave the packet's PLP unchanged or increase the PLP to medium-high or high. Therefore, these packets are metered against both the CBS and the EBS.

For example, if a BA or multifield classifier marks a packet with low PLP according to the type-of-service (ToS) bits in the IP header, and the two-rate TCM policer is in color-aware mode, the output loss priority is as follows:

- If the rate of traffic flow is less than the CBS, packets remain marked as low PLP.
- If the rate of traffic flow is greater than the CBS but less than the EBS, some of the packets are marked as medium-high PLP, and some of the packets remain marked as low PLP.
- If the rate of traffic flow is greater than the EBS, some of the packets are marked as high PLP, and some of the packets remain marked as low PLP.

#### Effect on Medium-Low PLP of Single-Rate Policer

Packets belonging to the yellow class have already been marked by a classifier with medium-low or medium-high PLP. The marking policer can leave the packet's PLP

unchanged or increase the PLP to high. Therefore, these packets are metered against the EBS only.

For example, if a BA or multifield classifier marks a packet with medium-low PLP according to the ToS bits in the IP header, and the two-rate TCM policer is in color-aware mode, the output loss priority is as follows:

- If the rate of traffic flow is less than the CBS, packets remain marked as medium-low PLP.
- If the rate of traffic flow is greater than the CBS but less than the EBS, packets remain marked as medium-low PLP.
- If the rate of traffic flow is greater than the EBS, some of the packets are marked as high PLP, and some of the packets remain marked as medium-low PLP.

---

#### Effect on Medium-High PLP of Single-Rate Policer

Packets belonging to the yellow class have already been marked by a classifier with medium-low or medium-high PLP. The marking policer can leave the packet's PLP unchanged or increase the PLP to high. Therefore, these packets are metered against the EBS only.

For example, if a BA or multifield classifier marks a packet with medium-high PLP according to the ToS bits in the IP header, and the two-rate TCM policer is in color-aware mode, the output loss priority is as follows:

- If the rate of traffic flow is less than the CBS, packets remain marked as medium-high PLP.
- If the rate of traffic flow is greater than the CBS but less than the EBS, packets remain marked as medium-high PLP.
- If the rate of traffic flow is greater than the EBS, some of the packets are marked as high PLP, and some of the packets remain marked as medium-high PLP.

---

#### Effect on High PLP of Single-Rate Policer

Packets belonging to the red class have already been marked by a classifier with high PLP. The marking policer can only leave the packet's PLP unchanged. Therefore, these packets are not metered against the CBS or the EBS and all the packets remain marked as high PLP.

---

## Configuring Two-Rate Tricolor Marking

With TCM, you can configure traffic policing according to two separate modes—color-blind and color-aware. In color-blind mode, the current PLP value is ignored. In color-aware mode, the current PLP values are considered by the policer and can only be increased.

- [Configuring Color-Blind Mode for Two-Rate Tricolor Marking on page 22](#)
- [Configuring Color-Aware Mode for Two-Rate Tricolor Marking on page 22](#)

## Configuring Color-Blind Mode for Two-Rate Tricolor Marking

All packets are evaluated by the CIR. If a packet exceeds the CIR, it is evaluated by the PIR. In color-blind mode, the policer supports three loss priorities only: low, medium-high, and high.

In color-blind mode, packets that exceed the CIR but are below the PIR are marked yellow (medium-high). Packets that exceed the PIR are marked red (high), as shown in [Table 6 on page 22](#).

**Table 6: Color-Blind Mode TCM Color-to-PLP Mapping**

Color	PLP	Meaning
Green	low	Packet does not exceed the CIR.
Yellow	medium-high	Packet exceeds the CIR but does not exceed the PIR.
Red	high	Packet exceeds the PIR.

If you are using color-blind mode and you wish to configure an output policer that marks packets to have medium-low loss priority, you must configure a policer at the **[edit firewall policer *policer-name*]** hierarchy level. For example:

```
firewall {
  policer 4PLP {
    if-exceeding {
      bandwidth-limit 40k;
      burst-size-limit 4k;
    }
    then loss-priority medium-low;
  }
}
```

Apply this policer at one or both of the following hierarchy levels:

- **[edit firewall family *family* filter *filter-name* term *rule-name* then policer *policer-name*]**
- **[edit interfaces *interface-name* unit *logical-unit-number* family *family* filter *filter-name*]**

## Configuring Color-Aware Mode for Two-Rate Tricolor Marking

In color-aware mode, the metering treatment the packet receives depends on its classification. Metering can increase a packet's preassigned PLP, but cannot decrease it, as shown in [Table 7 on page 23](#).

Table 7: Color-Aware Mode TCM Mapping

Incoming PLP	Packet Metered Against	Possible Cases	Outgoing PLP
<b>low</b>	CIR and PIR	Packet does not exceed the CIR.	<b>low</b>
		Packet exceeds the CIR but not the PIR.	<b>medium-high</b>
		Packet exceeds the PIR.	<b>high</b>
<b>medium-low</b>	PIR only	Packet does not exceed the CIR.	<b>medium-low</b>
		Packet does not exceed the PIR.	<b>medium-low</b>
		Packet exceeds the PIR.	<b>high</b>
<b>medium-high</b>	PIR only	Packet does not exceed the CIR.	<b>medium-high</b>
		Packet does not exceed the PIR.	<b>medium-high</b>
		Packet exceeds the PIR.	<b>high</b>
<b>high</b>	Not metered by the policer.	All cases.	<b>high</b>

The following sections describe color-aware two-rate PLP mapping in more detail.

#### Effect on Low PLP of Two-Rate Policer

Packets belonging to the green class have already been marked by a classifier with low PLP. The marking policer can leave the packet's PLP unchanged or increase the PLP to medium-high or high. Therefore, these packets are metered against both the CIR and the PIR.

For example, if a BA or multifield classifier marks a packet with low PLP according to the ToS bits in the IP header, and the two-rate TCM policer is in color-aware mode, the output loss priority is as follows:

- If the rate of traffic flow is less than the CIR, packets remain marked as low PLP.
- If the rate of traffic flow is greater than the CIR but less than the PIR, some of the packets are marked as medium-high PLP, and some of the packets remain marked as low PLP.
- If the rate of traffic flow is greater than the PIR, some of the packets are marked as high PLP, and some of the packets remain marked as low PLP.

#### Effect on Medium-Low PLP of Two-Rate Policer

Packets belonging to the yellow class have already been marked by a classifier with medium-low or medium-high PLP. The marking policer can leave the packet's PLP

unchanged or increase the PLP to high. Therefore, these packets are metered against the PIR only.

For example, if a BA or multifield classifier marks a packet with medium-low PLP according to the ToS bits in the IP header, and the two-rate TCM policer is in color-aware mode, the output loss priority is as follows:

- If the rate of traffic flow is less than the CIR, packets remain marked as medium-low PLP.
- If the rate of traffic flow is greater than the CIR/CBS but less than the PIR, packets remain marked as medium-low PLP.
- If the rate of traffic flow is greater than the PIR, some of the packets are marked as high PLP, and some of the packets remain marked as medium-low PLP.

---

#### Effect on Medium-High PLP of Two-Rate Policer

Packets belonging to the yellow class have already been marked by a classifier with medium-low or medium-high PLP. The marking policer can leave the packet's PLP unchanged or increase the PLP to high. Therefore, these packets are metered against the PIR only.

For example, if a BA or multifield classifier marks a packet with medium-high PLP according to the ToS bits in the IP header, and the two-rate TCM policer is in color-aware mode, the output loss priority is as follows:

- If the rate of traffic flow is less than the CIR, packets remain marked as medium-high PLP.
- If the rate of traffic flow is greater than the CIR but less than the PIR, packets remain marked as medium-high PLP.
- If the rate of traffic flow is greater than the PIR, some of the packets are marked as high PLP, and some of the packets remain marked as medium-high PLP.

---

#### Effect on High PLP of Two-Rate Policer

Packets belonging to the red class have already been marked by a classifier with high PLP. The marking policer can only leave the packet's PLP unchanged. Therefore, these packets are not metered against the CIR or the PIR and all the packets remain marked as high PLP.

---

## Enabling Tricolor Marking

By default, TCM is enabled on M120, MX Series, and T4000 routers, and EX Series switches. To enable TCM on other routers, include the **tri-color** statement at the **[edit class-of-service]** hierarchy level:

```
[edit class-of-service]
tri-color;
```



This statement is necessary on the following routers:

- M320 and T Series routers with Enhanced II FPCs
- T640 routers with Enhanced Scaling FPC4s

If you do not include this statement in the configuration on platforms that require it, you cannot configure medium-low or medium-high PLP for classifiers, rewrite rules, drop profiles, or firewall filters.

## Configuring Tricolor Marking Policers

A tricolor marking policer polices traffic on the basis of metering rates, including the CIR, the PIR, their associated burst sizes, and any policing actions configured for the traffic. To configure a tricolor marking policer, include the following statements at the **[edit firewall]** hierarchy level:

```
[edit firewall]
three-color-policer name {
  action {
    loss-priority high then discard; # Only for IQ2 PICs
  }
  logical-interface-policer;
  single-rate {
    (color-aware | color-blind);
    committed-information-rate bps;
    committed-burst-size bytes;
    excess-burst-size bytes;
  }
  two-rate {
    (color-aware | color-blind);
    committed-information-rate bps;
    committed-burst-size bytes;
    peak-information-rate bps;
    peak-burst-size bytes;
  }
}
```

You can configure a tricolor policer to discard high loss priority traffic on a logical interface in the ingress or egress direction. To configure a policer on a logical interface using tricolor marking policing to discard high loss priority traffic, include the **logical-interface-policer** statement and **action** statement.

In all cases, the range of allowable bits-per-second or byte values is 1500 to 100,000,000,000. You can specify the values for bps and bytes either as complete decimal numbers or as decimal numbers followed by the abbreviation **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

The color-aware policer implicitly marks packets into four loss priority categories:

- Low
- Medium-low

- Medium-high
- High

The color-blind policer implicitly marks packets into three loss priority categories:

- Low
- Medium-high
- High

Table 8 on page 26 describes all the configurable TCM statements.

**Table 8: Tricolor Marking Policer Statements**

Statement	Meaning	Configurable Values
<b>single-rate</b>	Marking is based on the CIR, CBS, and EBS.	—
<b>two-rate</b>	Marking is based on the CIR, PIR, and rated burst sizes.	—
<b>color-aware</b>	Metering depends on the packet's preclassification. Metering can increase a packet's assigned PLP, but cannot decrease it.	—
<b>color-blind</b>	All packets are evaluated by the CIR or CBS. If a packet exceeds the CIR or CBS, it is evaluated by the PIR or EBS.	—
<b>committed-information-rate</b>	Guaranteed bandwidth under normal line conditions and the average rate up to which packets are marked green.	1500 through 100,000,000,000 bps
<b>committed-burst-size</b>	Maximum number of bytes allowed for incoming packets to burst above the CIR, but still be marked green.	1500 through 100,000,000,000 bytes
<b>excess-burst-size</b>	Maximum number of bytes allowed for incoming packets to burst above the CIR, but still be marked yellow.	1500 through 100,000,000,000 bytes
<b>peak-information-rate</b>	Maximum achievable rate. Packets that exceed the CIR but are below the PIR are marked yellow. Packets that exceed the PIR are marked red.	1500 through 100,000,000,000 bps
<b>peak-burst-size</b>	Maximum number of bytes allowed for incoming packets to burst above the PIR, but still be marked yellow.	1500 through 100,000,000,000 bytes

## Applying Tricolor Marking Policers to Firewall Filters

To rate-limit traffic by applying a tricolor marking policer to a firewall filter, include the **three-color-policer** statement:

```
three-color-policer {
  (single-rate | two-rate) policer-name;
}
```

You can include this statement at the following hierarchy levels:

- [edit firewall family *family* filter *filter-name* term *rule-name* then]
- [edit firewall filter *filter-name* term *rule-name* then]

In the **family** statement, the protocol family can be **any**, **ccc**, **inet**, **inet6**, **mpls**, or **vpls**.

You must identify the referenced policer as a **single-rate** or **two-rate** policer, and this statement must match the configured TCM policer. Otherwise, an error message appears in the configuration listing.

For example, if you configure **srTCM** as a single-rate TCM policer and try to apply it as a two-rate policer, the following message appears:

```
[edit firewall]
user@host# show three-color-policer srTCM
single-rate {
    color-aware;
    ...
}
user@host# show filter TESTER
term A {
    then {
        three-color-policer {
            ##
            ## Warning: Referenced two-rate policer does not exist
            ##
            two-rate srTCM;
        }
    }
}
```

### Example: Applying a Two-Rate Tricolor Marking Policer to a Firewall Filter

Apply the **trtcm1-cb** policer to a firewall filter:

```
firewall {
    three-color-policer trtcm1-cb { # Configure the trtcm1-cb policer.
        two-rate {
            color-blind;
            committed-information-rate 1048576;
            committed-burst-size 65536;
            peak-information-rate 10485760;
            peak-burst-size 131072;
        }
    }
}
filter fil { # Configure the fil firewall filter, applying the trtcm1-cb policer.
    term default {
        then {
            three-color-policer {
                two-rate trtcm1-cb;
            }
        }
    }
}
```

**Related Documentation**

- [Firewall Filters Feature Guide for Routing Devices](#)

## Applying Firewall Filter Tricolor Marking Policers to Interfaces

---

To apply a tricolor marking policer to an interface, you must reference the filter name in the interface configuration. To do this, include the **filter** statement:

```
filter {  
    input filter-name;  
    output filter-name;  
}
```

You can include these statements at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family *family*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family *family*]

The filter name that you reference should have an attached tricolor marking policer, as shown in [“Applying Tricolor Marking Policers to Firewall Filters”](#) on page 26.

### Example: Applying a Single-Rate Tricolor Marking Policer to an Interface

Apply the **trtcm1-cb** policer to an interface:

```
firewall {  
    three-color-policer srtcm1 { # Configure the srtcm1-cb policer.  
        single-rate {  
            color-blind;  
            committed-information-rate 1048576;  
            committed-burst-size 65536;  
            excess-burst-size 131072;  
        }  
    }  
    filter fil { # Configure the fil firewall filter, applying the srtcm1-cb policer.  
        term default {  
            then {  
                three-color-policer {  
                    single-rate srtcm1-cb; # The TCM policer must be single-rate.  
                }  
            }  
        }  
    }  
    interfaces { # Configure the interface, which attaches the fil firewall filter.  
        so-1/0/0 {  
            unit 0 {  
                family inet {  
                    filter {  
                        input fil;  
                    }  
                }  
            }  
        }  
    }  
}
```

## Applying Layer 2 Policers to Gigabit Ethernet Interfaces

To rate-limit traffic by applying a policer to a Gigabit Ethernet interface (or a 10-Gigabit Ethernet interface [*xe-fpc/pic/port*]), include the **layer2-policer** statement with the direction, type, and name of the policer:

```
[edit interfaces ge-fpc/pic/port unit 0]
layer2-policer {
  input-policer policer-name;
  input-three-color policer-name;
  output-policer policer-name;
  output-three-color policer-name;
}
```

The direction (input or output) and type (policer or three-color) are combined into one statement and the policer named must be properly configured.

One input or output policer of either type can be configured on the interface.

### Examples: Applying Layer 2 Policers to a Gigabit Ethernet Interface

Apply color-blind and color-aware two-rate TCM policers as input and output policers to a Gigabit Ethernet interface:

```
ge-1/0/0 {
  unit 0
  layer2-policer {
    input-three-color trTCM1-cb; # Apply the trTCM1-color-blind policer.
    output-three-color trTCM1-ca; # Apply the trTCM1-color-aware policer.
  }
}
```

Apply two-level and color-blind single-rate TCM policers as input and output policers to a Gigabit Ethernet interface:

```
ge-1/0/0 {
  unit 1
  layer2-policer {
    input-policer two-color-policer; # Apply a two-color policer.
    output-three-color srTCM2-cb; # Apply the srTCM1-color-blind policer.
  }
}
```

Apply a color-aware single-rate TCM policer as output policer on a Gigabit Ethernet interface:

```
ge-1/0/0 {
  unit 2
  layer2-policer {
    output-three-color srTCM3-ca { # Apply the srTCM3-color-aware policer.
  }
}
```



## CHAPTER 3

# Configuration Tasks for Packet Loss Priority

- [Using BA Classifiers to Set PLP on page 31](#)
- [Using Multifield Classifiers to Set PLP on page 32](#)
- [Configuring PLP for Drop-Profile Maps on page 33](#)
- [Configuring Rewrite Rules Based on PLP on page 34](#)

### Using BA Classifiers to Set PLP

---

Behavior aggregate (BA) classifiers take action on incoming packets. When TCM is enabled, Juniper Networks M320 Multiservice Edge Routers and T Series Core Routers support four classifier PLP designations: **low**, **medium-low**, **medium-high**, and **high**. To configure the PLP for a classifier, include the following statements at the **[edit class-of-service]** hierarchy level:

```
[edit class-of-service]
classifiers {
  (dscp | dscp-ipv6 | exp | ieee-802.1 | inet-precedence) classifier-name {
    import (classifier-name | default);
    forwarding-class class-name {
      loss-priority (low | medium-low | medium-high | high) code-points [ aliases ]
      [ bit-patterns ];
    }
  }
}
```

The inputs for a classifier are the CoS values. The outputs for a classifier are the forwarding class and the loss priority (PLP). A classifier sets the forwarding class and the PLP for each packet entering the interface with a specific set of CoS values.

For example, in the following configuration, the **assured-forwarding** forwarding class and **medium-low** PLP are assigned to all packets entering the interface with the **101110** CoS values:

```
class-of-service {
  classifiers {
    dscp dscp-cl {
      forwarding-class assured-forwarding {
        loss-priority medium-low {
```

```
        code-points 101110;
      }
    }
  }
}
```

To use this classifier, you must configure the settings for the **assured-forwarding** forwarding class at the **[edit class-of-service forwarding-classes queue *queue-number* assured-forwarding]** hierarchy level. For more information, see *Overview of Forwarding Classes*.

---

## Using Multifield Classifiers to Set PLP

Multifield classifiers take action on incoming or outgoing packets, depending whether the firewall rule is applied as an input filter or an output filter. When TCM is enabled, Juniper Networks M320 Multiservice Edge Routers and T Series Core Routers support four multifield classifier PLP designations: **low**, **medium-low**, **medium-high**, and **high**.

To configure the PLP for a multifield classifier, include the **loss-priority** statement in a policer or firewall filter that you configure at the **[edit firewall]** hierarchy level:

```
[edit firewall]
family family-name {
  filter filter-name {
    term term-name {
      from {
        match-conditions;
      }
      then {
        loss-priority (low | medium-low | medium-high | high);
        forwarding-class class-name;
      }
    }
  }
}
```

The inputs (match conditions) for a multifield classifier are one or more of the six packet header fields: destination address, source address, IP protocol, source port, destination port, and DSCP. The outputs for a multifield classifier are the forwarding class and the loss priority (PLP). In other words, a multifield classifier sets the forwarding class and the PLP for each packet entering or exiting the interface with a specific destination address, source address, IP protocol, source port, destination port, or DSCP.

For example, in the following configuration, the forwarding class **expedited-forwarding** and PLP **medium-high** are assigned to all IPv4 packets with the 10.1.1.0/24 or 10.1.2.0/24 source address:

```
firewall {
  family inet {
    filter classify-customers {
      term isp1-customers {
        from {
          source-address 10.1.1.0/24;
```



```

        source-address 10.1.2.0/24;
    }
    then {
        loss-priority medium-high;
        forwarding-class expedited-forwarding;
    }
}
}
}
}

```

To use this classifier, you must configure the settings for the **expedited-forwarding** forwarding class at the **[edit class-of-service forwarding-classes queue *queue-number* expedited-forwarding]** hierarchy level. For more information, see *Overview of Forwarding Classes*.

## Configuring PLP for Drop-Profile Maps

RED drop profiles take action on outgoing packets. When TCM is enabled, M320 and T Series routers support four drop-profile map PLP designations: **low**, **medium-low**, **medium-high**, and **high**.

To configure the PLP for the drop-profile map, include the **schedulers** statement at the **[edit class-of-service]** hierarchy level:

```

[edit class-of-service]
schedulers {
    scheduler-name {
        drop-profile-map loss-priority (any | low | medium-low | medium-high | high) protocol
        any drop-profile profile-name;
    }
}

```

When you configure TCM, the drop-profile map's protocol type must be **any**.

The inputs for a drop-profile map are the loss priority and the protocol type. The output for a drop-profile map is the drop profile name. In other words, the map sets the drop profile for each packet with a specific PLP and protocol type exiting the interface.

For example, in the following configuration, the **dp** drop profile is assigned to all packets exiting the interface with a medium-low PLP and belonging to any protocol:

```

class-of-service {
    schedulers {
        af {
            drop-profile-map loss-priority medium-low protocol any drop-profile dp;
        }
    }
}

```

To use this drop-profile map, you must configure the settings for the **dp** drop profile at the **[edit class-of-service drop-profiles dp]** hierarchy level. For more information, see *RED Drop Profiles Overview*.

## Configuring Rewrite Rules Based on PLP

---

Rewrite rules take action on outgoing packets. When TCM is enabled, M320 and T Series routers support four rewrite PLP designations: **low**, **medium-low**, **medium-high**, and **high**. To configure the PLP for a rewrite rule, include the following statements at the **[edit class-of-service]** hierarchy level:

```
[edit class-of-service]
rewrite-rules {
  (dscp | dscp-ipv6 | exp | ieee-802.1 | inet-precedence) rewrite-name {
    import (rewrite-name | default);
    forwarding-class class-name {
      loss-priority (low | medium-low | medium-high | high) code-point (alias | bits);
    }
  }
}
```

The inputs for a rewrite rule are the forwarding class and the loss priority (PLP). The output for a rewrite rule are the CoS values. In other words, a rewrite rule sets the CoS values for each packet exiting the interface with a specific forwarding class and PLP.

For example, if you configure the following, the **000000** CoS values are assigned to all packets exiting the interface with the **assured-forwarding** forwarding class and **medium-high** PLP:

```
class-of-service {
  rewrite-rules {
    dscp dscp-rw {
      forwarding-class assured-forwarding {
        loss-priority medium-high code-point 000000;
      }
    }
  }
}
```

To use this classifier, you must configure the settings for the **assured-forwarding** forwarding class at the **[edit class-of-service forwarding-classes queue queue-number assured-forwarding]** hierarchy level. For more information, see *Overview of Forwarding Classes*.

# Tricolor Marking Policers Example

- [Example: Configuring and Verifying Two-Rate Tricolor Marking on page 35](#)

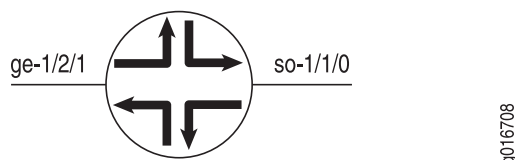
## Example: Configuring and Verifying Two-Rate Tricolor Marking

This example configures a two-rate tricolor marking policer on an input Gigabit Ethernet interface and shows commands to verify its operation.

Traffic enters the Gigabit Ethernet interface and exits a SONET/SDH OC12 interface. Oversubscription occurs when you send line-rate traffic from the Gigabit Ethernet interface out the OC12 interface.

[Figure 3 on page 35](#) shows the sample topology.

**Figure 3: Tricolor Marking Sample Topology**



- [Applying a Policer to the Input Interface on page 35](#)
- [Applying Profiles to the Output Interface on page 36](#)
- [Marking Packets with Medium-Low Loss Priority on page 37](#)
- [Verifying Two-Rate Tricolor Marking Operation on page 38](#)

## Applying a Policer to the Input Interface

The tricolor marking and policer are applied on the ingress Gigabit Ethernet interface. Incoming packets are metered. Packets that do not exceed the CIR are marked with low loss priority. Packets that exceed the CIR but do not exceed the PIR are marked with medium-high loss priority. Packets that exceed the PIR are marked with high loss priority.

```
[edit]
interfaces {
  ge-1/2/1 {
    unit 0 {
      family inet {
        filter {
          input trtcm-filter;
```

```
    }  
  }  
}  
}  
}  
firewall {  
  three-color-policer trtcm1 {  
    two-rate {  
      color-aware;  
      committed-information-rate 100m;  
      committed-burst-size 65536;  
      peak-information-rate 200m;  
      peak-burst-size 131072;  
    }  
  }  
  filter trtcm-filter {  
    term one {  
      then {  
        three-color-policer {  
          two-rate trtcm1;  
        }  
      }  
    }  
  }  
}
```

## Applying Profiles to the Output Interface

Transmission scheduling and weighted random early detection (WRED) profiles are applied on the output OC12 interface. The software drops traffic in the low, medium-high, and high drop priorities proportionally to the configured drop profiles.

```
[edit]  
class-of-service {  
  drop-profiles {  
    low-tcm {  
      fill-level 80 drop-probability 100;  
    }  
    med-tcm {  
      fill-level 40 drop-probability 100;  
    }  
    high-tcm {  
      fill-level 10 drop-probability 100;  
    }  
  }  
  tri-color;  
  interfaces {  
    so-1/1/0 {  
      scheduler-map tcm-sched;  
    }  
  }  
  scheduler-maps {  
    tcm-sched {  
      forwarding-class queue-0 scheduler q0-sched;  
      forwarding-class queue-3 scheduler q3-sched;  
    }  
  }  
}
```

```

}
schedulers {
  q0-sched {
    transmit-rate percent 50;
    buffer-size percent 50;
    drop-profile-map loss-priority low protocol any drop-profile low-tcm;
    drop-profile-map loss-priority medium-high protocol any drop-profile med-tcm;
    drop-profile-map loss-priority high protocol any drop-profile high-tcm;
  }
  q3-sched {
    transmit-rate percent 50;
    buffer-size percent 50;
  }
}
}

```

## Marking Packets with Medium-Low Loss Priority

In another example, the 4PLP filter and policer causes certain packets to be marked with medium-low loss priority.

```

interfaces {
  ge-7/2/0 {
    unit 0 {
      family inet {
        filter {
          input 4PLP;
        }
        policer {
          input 4PLP;
        }
        address 10.45.10.2/30;
      }
    }
  }
}

firewall {
  three-color-policer trTCM {
    two-rate {
      color-blind;
      committed-information-rate 400m;
      committed-burst-size 100m;
      peak-information-rate 1g;
      peak-burst-size 500m;
    }
  }
  policer 4PLP {
    if-exceeding {
      bandwidth-limit 40k;
      burst-size-limit 4k;
    }
    then loss-priority medium-low;
  }
  family inet {
    filter 4PLP {

```

```
term 0 {  
  from {  
    precedence 1;  
  }  
  then loss-priority medium-low;  
}  
}  
filter filter_trTCM {  
  term default {  
    then {  
      three-color-policer {  
        two-rate trTCM;  
      }  
    }  
  }  
}  
}
```

## Verifying Two-Rate Tricolor Marking Operation

The following operational mode commands are useful for checking the results of your configuration:

- **show class-of-service forwarding-table classifiers**
- **show interfaces *interface-name* extensive**
- **show interfaces queue *interface-name***

For information about these commands, see the *Junos OS Operational Mode Commands* and *Junos OS Operational Mode Commands*.

## CHAPTER 5

# Configuration Statements for Tricolor Marking Policers

## action

---

<b>Syntax</b>	<pre>action {     loss-priority high then discard; }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> <b>firewall three-color-policer</b> <i>name</i> ], [edit <b>firewall three-color-policer</b> <i>name</i> ], [edit logical-systems <i>logical-system-name</i> <b>firewall three-color-policer</b> <i>name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2. Logical systems support introduced in Junos OS Release 9.3. Support at the [edit dynamic-profiles ... <b>three-color-policer</b> ] hierarchy level introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
<b>Description</b>	Discard traffic on a logical interface using tricolor marking policing.



---

**NOTE:** This statement is supported only on IQ2 interfaces.

---


The remaining statement is explained separately.

<b>Required Privilege</b>	firewall—To view this statement in the configuration.
<b>Level</b>	firewall-control—To add this statement to the configuration.

<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Three-Color Policer Configuration Overview</i></li><li>• <i>Basic Single-Rate Three-Color Policers</i></li><li>• <i>Basic Two-Rate Three-Color Policers</i></li><li>• <i>Two-Color and Three-Color Logical Interface Policers</i></li><li>• <i>Two-Color and Three-Color Physical Interface Policers</i></li><li>• <i>Two-Color and Three-Color Policers at Layer 2</i></li><li>• <i>loss-priority high then discard</i></li></ul>
------------------------------	---



## classifiers (Definition)

<b>Syntax</b>	<pre> classifiers {     type classifier-name {         import (classifier-name   default);         forwarding-class class-name {             loss-priority level code-points [ aliases ] [ bit-patterns ];         }     } } </pre>
<b>Hierarchy Level</b>	[edit class-of-service], [edit class-of-service routing-instances <i>routing-instance-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. <b>ieee-802.1ad</b> option introduced in Junos OS Release 9.2.
<b>Description</b>	Define a CoS behavior aggregate (BA) classifier for classifying packets. You can associate the classifier with a forwarding class or code-point mapping, and import a default classifier or one that is previously defined.
	<div>  <p><b>NOTE:</b> The [edit class-of-service routing-instances <i>routing-instance-name</i>] hierarchy level and the <b>dscp-ipv6</b> and <b>ieee-802.1ad</b> classifier types are not supported on ACX Series routers.</p> </div>
<b>Options</b>	<p><b>classifier-name</b>—Name of the aggregate behavior classifier.</p> <p><b>type</b>—Traffic type: <b>dscp</b>, <b>dscp-ipv6</b>, <b>exp</b>, <b>ieee-802.1</b>, <b>ieee-802.1ad</b>, <b>inet-precedence</b>.</p>
<b>Required Privilege Level</b>	<p><b>interface</b>—To view this statement in the configuration.</p> <p><b>interface-control</b>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Overview of BA Classifier Types</i></li> <li>• <i>Example: Configuring CoS for a PBB Network on MX Series Routers</i></li> <li>• <i>Configuring CoS on ACX Series Universal Access Routers</i></li> </ul>

## code-points

---

<b>Syntax</b>	<code>code-points ([ <i>aliases</i> ]   [ <i>bit-patterns</i> ] );</code>
<b>Hierarchy Level</b>	[edit class-of-service classifiers <i>type classifier-name</i> forwarding-class <i>class-name</i> loss-priority <i>level</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 8.5 for J Series devices. Statement introduced in Junos OS Release 9.2 for SRX Series devices.
<b>Description</b>	Specify one or more DSCP code-point aliases or bit sets for association with a forwarding class.
<b>Options</b>	<b><i>aliases</i></b> —Name of the DSCP alias.  <b><i>bit-patterns</i></b> —Value of the code-point bits, in six-bit binary form.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Overview of BA Classifier Types</i></li><li>• <i>Example: Configuring CoS for a PBB Network on MX Series Routers</i></li><li>• <i>Example: Configuring Behavior Aggregate Classifiers</i></li><li>• <i>Example: Configuring Forwarding Classes</i></li></ul>

## drop-profile (Schedulers)

<b>Syntax</b>	<code>drop-profile <i>profile-name</i>;</code>
<b>Hierarchy Level</b>	[edit class-of-service <a href="#">schedulers</a> <i>scheduler-name</i> <a href="#">drop-profile-map</a> <a href="#">loss-priority</a> (any   low   medium-low   medium-high   high) <a href="#">protocol</a> (any   non-tcp   tcp)]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers. Statement introduced in Junos OS Release 12.2 for ACX Series Routers.
<b>Description</b>	Define drop profiles for RED. When a packet arrives, RED checks the queue fill level. If the fill level corresponds to a nonzero drop probability, the RED algorithm determines whether to drop the arriving packet.
<b>Options</b>	<i>profile-name</i> —Name of the drop profile.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Configuring Drop Profile Maps for Schedulers</i></li> <li><i>RED Drop Profiles Overview</i></li> </ul>

## drop-profile-map (Schedulers)

<b>Syntax</b>	<code>drop-profile-map <a href="#">loss-priority</a> (any   low   medium-low   medium-high   high) <a href="#">protocol</a>(any   non-tcp   tcp) <a href="#">drop-profile (Schedulers)</a> <i>profile-name</i>;</code>
<b>Hierarchy Level</b>	[edit class-of-service <a href="#">schedulers</a> <i>scheduler-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers. Statement introduced in Junos OS Release 12.2 for ACX Series Routers.
<b>Description</b>	Define the loss-priority value for a drop profile.  The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Default Schedulers Overview</i></li> <li><i>Configuring Drop Profile Maps for Schedulers</i></li> </ul>

## dscp (Multifield Classifier)

---

<b>Syntax</b>	<code>dscp [0   <i>value</i>];</code>
<b>Hierarchy Level</b>	<code>[edit firewall family <i>family-name</i> filter <i>filter-name</i> term <i>term-name</i> <b>then</b>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	<p>For M320 and T Series routers, set the DSCP field of incoming or outgoing packets to <b>000000</b>. On the same packets, you can use a behavior aggregate (BA) classifier and a rewrite rule to rewrite the MPLS EXP field.</p> <p>For MX Series routers with MPCs and EX Series switches, the DSCP field can be set from a numeric range.</p> <p>For MX Series routers and EX Series switches, if you configure a firewall filter with a DSCP action or traffic-class action on a DPC, the commit does not fail, but the filter is not applied to the interface, a warning displays, and an entry is made in the syslog.</p>
<b>Options</b>	<b><i>value</i></b> —For MX Series routers with MPCs, specify the field of incoming or outgoing packets in the range from <b>0</b> through <b>63</b> .
<b>Required Privilege Level</b>	<p>firewall—To view this statement in the configuration.</p> <p>firewall-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Applying Tricolor Marking Policers to Firewall Filters on page 26</a></li></ul>

## dscp (Rewrite Rules)

<b>Syntax</b>	<code>dscp (rewrite-name   default) protocol mpls;</code>
<b>Hierarchy Level</b>	[edit class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i> rewrite-rules]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>For IPv4 traffic, apply a Differentiated Services (DiffServ) code point (DSCP) rewrite rule.</p> <p>Logical interfaces do not support multiple <b>dscp</b> rewrite rules for the same protocol.</p> <p>DSCP and DSCP IPv6 rewrite rules are supported on M Series and T Series routers when non-queuing PICs are installed, but are disabled when queuing PICs are installed with the following exceptions:</p> <ul style="list-style-type: none"> <li>On M320 routers, DSCP rewrite is supported on IQ, IQ2, IQE, and IQ2E PICs when used with the Enhanced III FPC.</li> <li>On M120 routers, DSCP rewrite is supported on IQ, IQ2, IQE, and IQ2E PICs.</li> </ul> <p>DSCP and DCSP IPv6 rewrite rules are supported on MIC and MPC interfaces on MX Series routers.</p> <p>DSCP rewrite rules are not supported on T Series routers when IQ, IQ2, IQE, IQ2E, SONET/SDH OC48/STM16 IQE, or PD-5-10XGE-SFPP PICs are installed.</p>
<b>Options</b>	<p><b>rewrite-name</b>—Name of a <b>rewrite-rules</b> mapping configured at the [edit class-of-service rewrite-rules dscp] hierarchy level.</p> <p><b>default</b>—The default mapping.</p> <p><b>protocol mpls</b>—(Optional for ingress MPLS tunnel nodes) For interfaces on MX Series routers or hosted on Enhanced III FPCs in M120 or M320 routers only, rewrite the MPLS EXP bits in the MPLS header independently of the IPv4 DSCP value for IPv4 packets entering an MPLS tunnel.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Configuring Rewrite Rules</i></li> <li><i>Applying Rewrite Rules to Output Logical Interfaces</i></li> <li><i>protocol (Rewrite Rules)</i></li> <li><i>Rewriting MPLS and IPv4 Packet Headers</i></li> <li><a href="#">rewrite-rules (Definition) on page 67</a></li> </ul>

## dscp-ipv6 (Class-of-Service)

---

<b>Syntax</b>	<code>dscp-ipv6 (rewrite-name   &lt;default&gt;) protocol mpls;</code>
<b>Hierarchy Level</b>	[edit class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i> rewrite-rules]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Support for <b>protocol mpls</b> option introduced in Junos OS Release 10.4R2.
<b>Description</b>	<p>For IPv6 traffic, apply a DSCP rewrite rule.</p> <p>Logical interfaces do not support multiple <b>dscp-ipv6</b> rewrite rules for the same protocol.</p> <p>DSCP and DSCP IPv6 rewrite rules are supported on M Series and T Series routers when non-queuing PICs are installed, but are disabled when queuing PICs are installed with the following exceptions:</p> <ul style="list-style-type: none"><li>• On M320 routers, DSCP rewrite is supported on IQ, IQ2, IQE, and IQ2E PICs when used with the Enhanced III FPC.</li><li>• On M120 routers, DSCP rewrite is supported on IQ, IQ2, IQE, and IQ2E PICs.</li></ul> <p>DSCP and DCSP IPv6 rewrite rules are supported on MIC and MPC interfaces on MX Series routers.</p> <p>DSCP rewrite rules are not supported on T Series routers when IQ, IQ2, IQE, IQ2E, SONET/SDH OC48/STM16 IQE, or PD-5-10XGE-SFPP PICs are installed.</p>
<b>Options</b>	<p><b>rewrite-name</b>—Name of a <b>rewrite-rules</b> mapping configured at the [edit class-of-service rewrite-rules dscp-ipv6] hierarchy level.</p> <p><b>default</b>—Default mapping.</p> <p><b>protocol mpls</b>—(Optional for ingress MPLS tunnel nodes) For interfaces on MX Series routers or hosted on Enhanced III FPCs in M120 or M320 routers only, rewrite the MPLS EXP bits in the MPLS header independently of the IPv6 DSCP value for IPv6 packets entering an MPLS tunnel.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Rewrite Rules</i></li><li>• <i>protocol</i></li><li>• <i>Setting IPv6 DSCP and MPLS EXP Values Independently</i></li><li>• <i>Configuring DSCP Values for IPv6 Packets Entering the MPLS Tunnel</i></li><li>• <i>Applying Rewrite Rules to Output Logical Interfaces</i></li><li>• <a href="#">rewrite-rules (Definition) on page 67</a></li></ul>

**exp**

<b>Syntax</b>	<code>exp (rewrite-name   default) protocol protocol-types;</code>
<b>Hierarchy Level</b>	<code>[edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced before Junos OS Release 12.2. for ACX series
<b>Description</b>	Apply an MPLS experimental (EXP) rewrite rule.
<b>Options</b>	<p><b>rewrite-name</b>—Name of a <b>rewrite-rules</b> mapping configured at the <code>[edit class-of-service rewrite-rules exp]</code> hierarchy level.</p> <p><b>default</b>—The default mapping.</p> <p>By default, IP precedence rewrite rules alter the first three bits on the type-of-service (ToS) byte while leaving the last three bits unchanged. This default behavior applies to rewrite rules you configure for MPLS packets with IPv4 payloads. You configure these types of rewrite rules by including the <b>mpls-inet-both</b> or <b>mpls-inet-both-non-vpn</b> option at the <code>[edit class-of-service interfaces interface interface-name unit logical-unit-number rewrite-rules exp rewrite-rule-name protocol]</code> hierarchy level. The IP precedence rewrite rules explanation does not apply to ACX Series Universal Access routers.</p> <p>On interfaces configured on Modular Port Concentrators (MPCs) and Modular Interface Cards (MICs) on MX Series 3D Universal Edge Routers and EX Series switches, we highly recommend that you configure the <b>default</b> option when you configure a behavior aggregate (BA) classifier that does not include a specific rewrite rule for MPLS packets. Doing so ensures that MPLS exp value is rewritten according to the BA classifier rules configured for forwarding or packet loss priority. This does not apply to ACX Series Universal Access routers.</p> <p><b>protocol-types</b>—Specify one or more protocol matching criteria:</p> <ul style="list-style-type: none"> <li>• <b>mpls-any</b>—Apply to MPLS packets, write MPLS header only.</li> <li>• <b>mpls-inet-both</b>—Apply to IPv4 MPLS packets, write MPLS and IPv4 header.</li> <li>• <b>mpls-inet-both-non-vpn</b>—Apply to IPv4 MPLS packets, write MPLS and IPv4 header for only non VPN traffic.</li> </ul>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Rewrite Rules</i></li> <li>• <i>Rewriting the EXP Bits of All Three Labels of an Outgoing Packet</i></li> <li>• <i>Applying Rewrite Rules to Output Logical Interfaces</i></li> <li>• <i>protocol (Rewrite Rules)</i></li> </ul>

- [rewrite-rules \(Definition\)](#) on page 67

---

## family (Multifield Classifier)

---

**Syntax**    `family family-name {  
              filter filter-name {  
                  term term-name {  
                      ... term_configuration ...  
                  }  
              }  
          }  
}`

**Hierarchy Level**    [edit [firewall](#)]

**Release Information**    Statement introduced before Junos OS Release 7.4.

**Description**    Configure a firewall filter for IP version 4 (IPv4) or IP version 6 (IPv6) traffic.

**Options**    *family-name*—Protocol family:

- **ccc**—Circuit cross-connect parameters
- **inet**—IPv4 parameters
- **inet6**—IPv6 protocol parameters
- **iso**—OSI ISO protocol parameters
- **mlppp**—Multilink PPP protocol parameters
- **mpls**—MPLS protocol parameters
- **tcc**—Translational cross-connect parameters
- **vpls**—Virtual private LAN service parameters.

The remaining statements are explained separately.

**Required Privilege Level**    interface—To view this statement in the configuration.  
                                  interface-control—To add this statement to the configuration.

**Related Documentation**    • *Configuring Multifield Classifiers*



## filter (Applying to a Logical Interface)

<b>Syntax</b>	<pre>filter {   group <i>filter-group-number</i>;   input <i>filter-name</i>;   input-list [ <i>filter-names</i> ];   output <i>filter-name</i>;   output-list [ <i>filter-names</i> ]; }</pre>
<b>Hierarchy Level</b>	<p>Protocol-independent firewall filter on MX Series router logical interface:</p> <pre>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]</pre> <p>All other standard firewall filters on all other devices:</p> <pre>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>]</pre>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Apply a stateless firewall filter to a logical interface at a specific protocol level.
<b>Options</b>	<p><b>group <i>filter-group-number</i></b>—Number of the group to which the interface belongs. Range: 1 through 255</p> <p><b>input <i>filter-name</i></b>—Name of one filter to evaluate when packets are received on the interface.</p> <p><b>input-list [ <i>filter-names</i> ]</b>—Names of filters to evaluate when packets are received on the interface. Up to 16 filters can be included in a filter input list.</p> <p><b>output <i>filter-name</i></b>—Name of one filter to evaluate when packets are transmitted on the interface.</p> <p><b>output-list [ <i>filter-names</i> ]</b>—Names of filters to evaluate when packets are transmitted on the interface. Up to 16 filters can be included in a filter output list.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Guidelines for Configuring Firewall Filters</i></li> <li>• <i>Guidelines for Applying Firewall Filters</i></li> </ul>

## filter (Configuring)

---

<b>Syntax</b>	<pre>filter <i>filter-name</i> {     accounting-profile <i>name</i>;     enhanced-mode;     interface-shared;     interface-specific;     physical-interface-filter;     term <i>term-name</i> {         ... term configuration ...     } }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> <b>firewall</b> family <i>family-name</i> ], [edit <b>firewall</b> family <i>family-name</i> ], [edit logical-systems <i>logical-system-name</i> <b>firewall</b> family <i>family-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Logical systems support introduced in Junos OS Release 9.3. <b>physical-interface-filter</b> statement introduced in Junos OS Release 9.6. Support at the [edit dynamic-profiles ... family <i>family-name</i> ] hierarchy level introduced in Junos OS Release 11.4. Support for the <b>interface-shared</b> > statement introduced in Junos OS Release 12.2. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
<b>Description</b>	Configure firewall filters.
<b>Options</b>	<p><b><i>filter-name</i></b>—Name that identifies the filter. This must be a non-reserved string of not more than 64 characters. To include spaces in the name, enclose it in quotation marks (" "). In Junos OS Release 9.0 and later, you can no longer use special characters within the name of a firewall filter. Firewall filter names are restricted from having the form <b>_.*</b> (beginning and ending with underscores) or <b>_.*</b> (beginning with an underscore).</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<b>firewall</b> —To view this statement in the configuration. <b>firewall-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Guidelines for Configuring Firewall Filters</i></li><li>• <i>Guidelines for Applying Firewall Filters</i></li><li>• <i>Configuring Multifield Classifiers</i></li><li>• <a href="#">Using Multifield Classifiers to Set PLP on page 32</a></li><li>• <i>simple-filter (Configuring)</i></li></ul>

## firewall

<b>Syntax</b>	<pre> firewall {     atm-policer <i>atm-policer-name</i> {         ... <i>atm-policer-configuration</i> ...     }     family <i>protocol-family-name</i> {         ... <i>protocol-family-configuration</i> ...     }     filter <i>ipv4-filter-name</i> {         ... <i>ipv4-filter-configuration</i> ...     }     hierarchical-policer <i>hierarchical-policer-name</i> {         ... <i>hierarchical-policer-configuration</i> ...     }     interface-set <i>interface-set-name</i> {         ... <i>interface-set-configuration</i> ...     }     policer <i>two-color-policer-name</i> {         ... <i>two-color-policer-configuration</i> ...     }     three-color-policer <i>three-color-policer-name</i> {         ... <i>three-color-policer-configuration</i> ...     } } </pre>
<b>Hierarchy Level</b>	[edit], [edit logical-systems <i>logical-system-name</i> ] [edit dynamic-profiles <i>profile-name</i> ],
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Logical systems support introduced in Junos OS Release 9.3.
<b>Description</b>	Configure firewall filters.  The statements are explained separately.
<b>Required Privilege Level</b>	firewall—To view this statement in the configuration. firewall-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Guidelines for Configuring Firewall Filters</i></li> <li>• <i>Guidelines for Configuring Service Filters</i></li> <li>• <i>Guidelines for Configuring Simple Filters</i></li> <li>• <i>Configuring Multifield Classifiers</i></li> <li>• <a href="#">Using Multifield Classifiers to Set PLP on page 32</a></li> </ul>

## forwarding-class (BA Classifiers)

---

<b>Syntax</b>	<code>forwarding-class class-name {     loss-priority level <b>code-points</b> [ <i>aliases</i> ] [ <i>bit-patterns</i> ]; }</code>
<b>Hierarchy Level</b>	[edit class-of-service classifiers <i>type classifier-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define forwarding class name and option values.
<b>Options</b>	<p><i>class-name</i>—Name of the forwarding class.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Defining Classifiers</i></li><li>• <i>Example: Configuring CoS for a PBB Network on MX Series Routers</i></li></ul>

## ieee-802.1 (Rewrite Rules on Logical Interface)

<b>Syntax</b>	<code>ieee-802.1 (<i>rewrite-name</i>   default) vlan-tag (outer   outer-and-inner);</code>
<b>Hierarchy Level</b>	<code>[edit class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i> rewrite-rules]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. <b>vlan-tag</b> statement introduced in Junos OS Release 8.1.
<b>Description</b>	Apply an IEEE-802.1 rewrite rule. For IQ PICs, you can only configure one IEEE 802.1 rewrite rule on a physical port. All logical ports (units) on that physical port should apply the same IEEE 802.1 rewrite rule.
<b>Options</b>	<b><i>rewrite-name</i></b> —Name of a <b>rewrite-rules</b> mapping configured at the <code>[edit class-of-service rewrite-rules ieee-802.1]</code> hierarchy level.  <b>default</b> —The default mapping.
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Rewrite Rules</i></li> <li>• <i>Example: Configuring CoS for a PBB Network on MX Series Routers</i></li> <li>• <a href="#">dscp (Rewrite Rules) on page 45</a></li> <li>• <a href="#">dscp-ipv6 (Class-of-Service) on page 46</a></li> <li>• <a href="#">exp on page 47</a></li> <li>• <i>exp-push-push-push</i></li> <li>• <i>exp-swap-push-push</i></li> <li>• <i>ieee-802.1ad</i></li> <li>• <a href="#">inet-precedence on page 55</a></li> <li>• <a href="#">rewrite-rules (Definition) on page 67</a></li> </ul>

## import (Classifiers)

---

<b>Syntax</b>	<code>import (classifier-name   default);</code>
<b>Hierarchy Level</b>	<code>[edit class-of-service classifiers type classifier-name]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify a default or previously defined classifier.
<b>Options</b>	<b>classifier-name</b> —Name of the classifier mapping configured at the <code>[edit class-of-service classifiers]</code> hierarchy level.  <b>default</b> —The default classifier mapping.
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Overview of BA Classifier Types</i></li></ul>

## import (Rewrite Rules)

---

<b>Syntax</b>	<code>import (rewrite-name   default);</code>
<b>Hierarchy Level</b>	<code>[edit class-of-service rewrite-rules type rewrite-name]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify a default or previously defined <b>rewrite-rules</b> mapping to import.
<b>Options</b>	<b>rewrite-name</b> —Name of a rewrite-rules mapping configured at the <code>[edit class-of-service rewrite-rules]</code> hierarchy level.  <b>default</b> —The default <b>rewrite-rules</b> mapping.
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Rewrite Rules</i></li></ul>

## inet-precedence

---

<b>Syntax</b>	<code>inet-precedence (<i>rewrite-name</i>   default);</code>
<b>Hierarchy Level</b>	[edit class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i> rewrite-rules]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Apply a IPv4 precedence rewrite rule.
<b>Options</b>	<p><b><i>rewrite-name</i></b>—Name of a <b>rewrite-rules</b> mapping configured at the [edit class-of-service rewrite-rules <b>inet-precedence</b>] hierarchy level.</p> <p><b>default</b>—The default mapping. By default, IP precedence rewrite rules alter the first three bits on the type of service (ToS) byte while leaving the last three bits unchanged.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Rewrite Rules</i></li><li>• <i>Applying Rewrite Rules to Output Logical Interfaces</i></li><li>• <i>protocol (Rewrite Rules)</i></li><li>• <a href="#">rewrite-rules (Definition) on page 67</a></li></ul>

## input-policer

---

<b>Syntax</b>	<code>input-policer <i>policer-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> <a href="#">layer2-policer</a>]</code> <code>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> <a href="#">layer2-policer</a>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
<b>Description</b>	Apply a single-rate two-color policer to the Layer 2 input traffic at the logical interface. The <b>input-policer</b> and <b>input-three-color</b> statements are mutually exclusive.
<b>Options</b>	<b><i>policer-name</i></b> —Name of the single-rate two-color policer that you define at the <code>[edit firewall]</code> hierarchy level.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Two-Color and Three-Color Policers at Layer 2</i></li><li>• <a href="#">Applying Layer 2 Policers to Gigabit Ethernet Interfaces on page 29</a></li><li>• <i>Configuring a Gigabit Ethernet Policer</i></li><li>• <a href="#">input-three-color on page 57</a></li><li>• <a href="#">layer2-policer on page 58</a></li><li>• <a href="#">logical-interface-policer on page 59</a></li><li>• <a href="#">output-policer on page 62</a></li><li>• <a href="#">output-three-color on page 63</a></li></ul>



## input-three-color

---


<b>Syntax</b>	<code>input-three-color <i>policer-name</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> <a href="#">layer2-policer</a> ] [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> <a href="#">layer2-policer</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
<b>Description</b>	Apply a single-rate or two-rate three-color policer to the Layer 2 input traffic at the logical interface. The <b>input-three-color</b> and <b>input-policer</b> statements are mutually exclusive.
<b>Options</b>	<b><i>policer-name</i></b> —Name of the single-rate or two-rate three-color policer.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Two-Color and Three-Color Policers at Layer 2</i></li> <li>• <a href="#">Applying Layer 2 Policers to Gigabit Ethernet Interfaces on page 29</a></li> <li>• <i>Configuring a Gigabit Ethernet Policer</i></li> <li>• <a href="#">input-policer on page 56</a></li> <li>• <a href="#">layer2-policer on page 58</a></li> <li>• <a href="#">logical-interface-policer on page 59</a></li> <li>• <a href="#">output-policer on page 62</a></li> <li>• <a href="#">output-three-color on page 63</a></li> </ul>

## layer2-policer

---

<b>Syntax</b>	<pre>layer2-policer {     input-policer <i>policer-name</i>;     input-three-color <i>policer-name</i>;     output-policer <i>policer-name</i>;     output-three-color <i>policer-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ],
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
<b>Description</b>	<p>For 1-Gigabit Ethernet and 10-Gigabit Ethernet IQ2 and IQ2-E interfaces on M Series, MX Series, and T Series routers, and for aggregated Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces on EX Series switches, apply Layer 2 logical interface policers. The following policers are supported:</p> <ul style="list-style-type: none"><li>• Two-color</li><li>• Single-rate tricolor marking (srTCM)</li><li>• Two-rate tricolor marking (trTCM)</li></ul> <p>Two-color and tricolor policers are configured at the <b>[edit firewall]</b> hierarchy level.</p>
<b>Options</b>	<p><b>input-policer <i>policer-name</i></b>—Two-color input policer to associate with the interface. This statement is mutually exclusive with the <b>input-three-color</b> statement.</p> <p><b>input-three-color <i>policer-name</i></b>—Tricolor input policer to associate with the interface. This statement is mutually exclusive with the <b>input-policer</b> statement.</p> <p><b>output-policer <i>policer-name</i></b>—Two-color output policer to associate with the interface. This statement is mutually exclusive with the <b>output-three-color</b> statement.</p> <p><b>output-three-color <i>policer-name</i></b>—Tricolor output policer to associate with the interface. This statement is mutually exclusive with the <b>output-policer</b> statement.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Applying Layer 2 Policers to Gigabit Ethernet Interfaces on page 29</a></li><li>• <a href="#">Configuring Gigabit Ethernet Two-Color and Tricolor Policers</a></li></ul>

## logical-interface-policer

<b>Syntax</b>	logical-interface-policer;
<b>Hierarchy Level</b>	<p>[edit dynamic-profiles <i>profile-name</i> <b>firewall policer</b> <i>policer-name</i>],          [edit dynamic-profiles <i>profile-name</i> <b>firewall three-color-policer</b> <i>name</i>],          [edit firewall atm-policer <i>atm-policer-name</i>]          [edit <b>firewall policer</b> <i>policer-name</i>],          [edit firewall policer <i>policer-template-name</i>],          [edit <b>firewall three-color-policer</b> <i>policer-name</i>],          [edit logical-systems <i>logical-system-name</i> <b>firewall policer</b> <i>policer-name</i>],          [edit logical-systems <i>logical-system-name</i> <b>firewall three-color-policer</b> <i>name</i>]</p>
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Support at the [edit firewall three-color-policer <i>policer-name</i>] hierarchy level introduced in Junos OS Release 8.2.</p> <p>Logical systems support introduced in Junos OS Release 9.3.</p> <p>Support at the [edit dynamic-profiles ... policer <i>policer-name</i>] and [edit dynamic-profiles ... three-color-policer <i>name</i>] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
<b>Description</b>	Configure a logical interface policer.
	<div>  <p><b>NOTE:</b> Starting in Junos OS Release 12.2R2, on T Series Core Routers only, you can configure an MPLS LSP policer for a specific LSP to be shared across different protocol family types. You must include the logical-interface-policer statement to do so.</p> </div>
<b>Required Privilege Level</b>	<p>firewall—To view this statement in the configuration.</p> <p>firewall-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Two-Color and Three-Color Logical Interface Policers</i></li> <li>• <i>Traffic Policer Types</i></li> <li>• <a href="#">Configuring Tricolor Marking Policers on page 25</a></li> <li>• <a href="#">action on page 40</a></li> <li>• <i>Configuring Gigabit Ethernet Two-Color and Tricolor Policers</i></li> <li>• <i>action</i></li> </ul>

## loss-priority (Normal Filter)

---

<b>Syntax</b>	loss-priority (high   low);
<b>Hierarchy Level</b>	[edit firewall family <i>family-name</i> filter <i>filter-name</i> term <i>term-name</i> <b>then</b> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Set the loss priority of incoming packets.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Multifield Classifiers</i></li></ul>

## loss-priority (Simple Filter)

---

<b>Syntax</b>	loss-priority (high   low   medium);
<b>Hierarchy Level</b>	[edit firewall family <i>family-name</i> simple-filter <i>filter-name</i> term <i>term-name</i> <b>then</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.6.
<b>Description</b>	Set the loss priority of incoming packets.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Multifield Classifiers</i></li></ul>

## loss-priority (Scheduler Drop Profiles)

<b>Syntax</b>	loss-priority (any   high   low   medium-high   medium-low);
<b>Hierarchy Level</b>	[edit class-of-service <a href="#">schedulers</a> <i>scheduler-name</i> drop-profile-map]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers. Statement introduced in Junos OS Release 12.2 for ACX Series Routers.
<b>Description</b>	Specify a loss priority to which to apply a drop profile. The drop profile map sets the drop profile for a specific PLP and protocol type. The inputs for the map are the PLP designation and the protocol type. The output is the drop profile.
<b>Options</b>	<b>any</b> —The drop profile applies to packets with any PLP.



**NOTE:** On ACX Series Routers, only the **any** option is supported when you configure the **non-tcp** option for [protocol](#).

**high**—The drop profile applies to packets with high PLP.

**low**—The drop profile applies to packets with low PLP.

**medium-high**—The drop profile applies to packets with medium-high PLP.

**medium-low**—The drop profile applies to packets with medium-low PLP.

<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.

- Related Documentation**
- [Default Schedulers Overview](#)
  - [Configuring Drop Profile Maps for Schedulers](#)
  - [Configuring Schedulers for Priority Scheduling](#)
  - [Configuring Tricolor Marking on page 17](#)
  - [protocol \(Schedulers\) on page 66](#)

## output-policer

---

<b>Syntax</b>	<code>output-policer <i>policer-name</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> <a href="#">layer2-policer</a> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> <a href="#">layer2-policer</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
<b>Description</b>	Apply a single-rate two-color policer to the Layer 2 output traffic at the logical interface. The <b>output-policer</b> and <b>output-three-color</b> statements are mutually exclusive.
<b>Options</b>	<b><i>policer-name</i></b> —Name of the single-rate two-color policer that you define at the [edit <b>firewall</b> ] hierarchy level.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Two-Color and Three-Color Policers at Layer 2</i></li><li>• <a href="#">Applying Layer 2 Policers to Gigabit Ethernet Interfaces on page 29</a></li><li>• <i>Configuring a Gigabit Ethernet Policer</i></li><li>• <a href="#">input-policer on page 56</a></li><li>• <a href="#">input-three-color on page 57</a></li><li>• <a href="#">layer2-policer on page 58</a></li><li>• <a href="#">logical-interface-policer on page 59</a></li><li>• <a href="#">output-three-color on page 63</a></li></ul>

## output-three-color

---

<b>Syntax</b>	<code>output-three-color <i>policer-name</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> <a href="#">layer2-policer</a> ] [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> <a href="#">layer2-policer</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
<b>Description</b>	Apply a single-rate or two-rate three-color policer to the Layer 2 output traffic at the logical interface. The <b>output-three-color</b> and <b>output-policer</b> statements are mutually exclusive.
<b>Options</b>	<i>policer-name</i> —Name of the single-rate or two-rate three-color policer.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Two-Color and Three-Color Policers at Layer 2</i></li> <li>• <a href="#">Applying Layer 2 Policers to Gigabit Ethernet Interfaces on page 29</a></li> <li>• <i>Configuring a Gigabit Ethernet Policer</i></li> <li>• <a href="#">input-three-color on page 57</a></li> <li>• <a href="#">input-policer on page 56</a></li> <li>• <a href="#">layer2-policer on page 58</a></li> <li>• <a href="#">logical-interface-policer on page 59</a></li> <li>• <a href="#">output-policer on page 62</a></li> </ul>

## policer (Configuring)

---

Syntax	<pre>policer <i>policer-name</i> {     filter-specific;     if-exceeding {         bandwidth-limit <i>bps</i>;         bandwidth-percent <i>number</i>;         burst-size-limit <i>bytes</i>;     }     logical-bandwidth-policer;     logical-interface-policer;     physical-interface-policer;     shared-bandwidth-policer;     then {         <i>policer-action</i>;     } }</pre>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> <b>firewall</b> ], [edit <b>firewall</b> ], [edit logical-systems <i>logical-system-name</i> <b>firewall</b> ]
Release Information	Statement introduced before Junos OS Release 7.4. The <b>out-of-profile</b> policer action added in Junos OS Release 8.1. The <b>logical-bandwidth-policer</b> statement added in Junos OS Release 8.2. Logical systems support introduced in Junos OS Release 9.3. The <b>physical-interface-policer</b> statement introduced in Junos OS Release 9.6. The <b>shared-bandwidth-policer</b> statement added in Junos OS Release 11.2. Support at the [edit dynamic-profiles ... <b>firewall</b> ] hierarchy level introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Configure policer rate limits and actions. When included at the [edit <b>firewall</b> ] hierarchy level, the <b>policer</b> statement creates a template, and you do not have to configure a policer individually for every firewall filter or interface. To activate a policer, you must include the <b>policer-action</b> modifier in the <b>then</b> statement in a firewall filter term or on an interface.
Options	<b><i>policer-action</i></b> —One or more actions to take: <ul style="list-style-type: none"><li>• <b>discard</b>—Discard traffic that exceeds the rate limits.</li><li>• <b>forwarding-class <i>class-name</i></b>—Specify the particular forwarding class.</li><li>• <b>loss-priority</b>—Set the packet loss priority (PLP) to <b>low</b>, <b>medium-low</b>, <b>medium-high</b>, or <b>high</b>.</li><li>• <b>out-of-profile</b>—On J Series routers with strict priority queuing, prevent starvation of other queues by rate limiting the data stream entering the strict priority queue, marking the packets that exceed the rate limit as out-of-profile, and dropping the out-of-profile packets if the physical interface is congested.</li></ul>



***policer-name***—Name that identifies the policer. The name can contain letters, numbers, and hyphens (-), and can be up to 255 characters long. To include spaces in the name, enclose it in quotation marks (" "). Policer names cannot begin with an underscore in the form `_.*`.

**then**—Actions to take on matching packets.

The remaining statements are explained separately.

<b>Required Privilege</b>	firewall—To view this statement in the configuration.
<b>Level</b>	firewall-control—To add this statement to the configuration.

**Related  
Documentation**

- *Bandwidth Policer Overview*
- *Configuring Firewall Filters and Policers for VPLS*
- *Configuring Multifield Classifiers*
- *Logical Interface (Aggregate) Policer Overview*
- *Physical Interface Policer Overview*
- *Statement Hierarchy for Configuring Policers*
- *Single-Rate Two-Color Policer Overview*
- [Using Multifield Classifiers to Set PLP on page 32](#)
- [filter \(Configuring\) on page 50](#)
- *priority (Schedulers)*

## protocol (Schedulers)

---

<b>Syntax</b>	protocol (any   non-tcp   tcp);
<b>Hierarchy Level</b>	[edit class-of-service <a href="#">schedulers</a> <i>scheduler-name</i> <a href="#">drop-profile-map</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers. Statement introduced in Junos OS Release 12.2 for ACX Series Routers.
<b>Description</b>	Specify the protocol type for the specified scheduler.
<b>Options</b>	<b>any</b> —Accept any protocol type.  <b>non-tcp</b> —(ACX Series Routers, M Series and T Series (except T4000) routers only) Accept any protocol type other than TCP/IP.



**NOTE:** On ACX Series Routers, when you configure the **non-tcp** option, only the **any** option is supported for [loss-priority](#).

---

	<b>tcp</b> —(ACX Series Routers, M Series and T Series (except T4000) routers only) Accept TCP/IP protocol type.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Schedulers</i></li></ul>

## rewrite-rules (Definition)


<b>Syntax</b>	<pre>rewrite-rules {     type <i>rewrite-name</i>{         import (<i>rewrite-name</i>   default);         forwarding-class <i>class-name</i> {             loss-priority <i>level</i> code-point [ <i>aliases</i> ] [ <i>bit-patterns</i> ];         }     } }</pre>
<b>Hierarchy Level</b>	[edit class-of-service]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. <b>ieee-802.1ad</b> option introduced in Junos OS Release 9.2.
<b>Description</b>	Specify a rewrite-rules mapping for the traffic that passes through all queues on the interface.
<b>Options</b>	<p><b><i>rewrite-name</i></b>—Name of a <b>rewrite-rules</b> mapping.</p> <p><b><i>type</i></b>—Traffic type.</p> <p><b>Values:</b> <b>dscp</b>, <b>dscp-ipv6</b>, <b>exp</b>, <b>frame-relay-de</b> (J Series routers only), <b>ieee-802.1</b>, <b>ieee-802.1ad</b>, <b>inet-precedence</b></p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Rewrite Rules</i></li> <li>• <i>Example: Configuring CoS for a PBB Network on MX Series Routers</i></li> <li>• J Series router documentation</li> </ul>

## schedulers (Class of Service)

---

<b>Syntax</b>	<pre>schedulers {   scheduler-name {     adjust-minimum <i>rate</i>;     adjust-percent <i>percentage</i>;     buffer-size (<i>seconds</i>   percent <i>percentage</i>   remainder   temporal <i>microseconds</i>);     drop-profile-map loss-priority (any   low   medium-low   medium-high   high) <i>protocol</i>       (any   non-tcp   tcp) drop-profile <i>profile-name</i>;     excess-priority [ low   medium-low   medium-high   high   none];     excess-rate (percent <i>percentage</i>   proportion <i>value</i>);     priority <i>priority-level</i>;     shaping-rate (percent <i>percentage</i>   <i>rate</i>);     transmit-rate (percent <i>percentage</i>   <i>rate</i>   remainder) &lt;exact   rate-limit&gt;;   } }</pre>
<b>Hierarchy Level</b>	[edit class-of-service]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1X48 for PTX Series routers.
<b>Description</b>	Specify the scheduler name and parameter values.
<b>Options</b>	<p><i>scheduler-name</i>—Name of the scheduler to be configured.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Schedulers Overview</i></li><li>• <i>Default Schedulers Overview</i></li><li>• <i>Configuring Schedulers</i></li><li>• <i>Configuring a Scheduler</i></li><li>• <i>Example: Configuring CoS for a PBB Network on MX Series Routers</i></li></ul>

## shared-bandwidth-policer

<b>Syntax</b>	shared-bandwidth-policer;
<b>Hierarchy Level</b>	<p>[edit firewall <b>policer</b> <i>policer-name</i>]</p> <p>[edit firewall <b>three-color-policer</b> <i>policer-name</i>]</p> <p>[edit <b>firewall</b> hierarchical-policer <i>policer-name</i>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 11.2.</p> <p>Support for MX Series MPC and MIC interfaces added in Junos OS Release 12.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
<b>Description</b>	<p>Policer instances share bandwidth. This enables configuration of interface-specific policers applied on an aggregated Ethernet bundle or an aggregated SONET bundle to match the effective bandwidth and burst-size to user-configured values. This feature is supported on the following platforms: T Series routers, M120, M10i, M7i (CFEB-E only), M320 (SFPC only), MX240, MX480, and MX960 with DPC, MIC, and MPC interfaces and EX Series switches.</p>
<div>  <p><b>NOTE:</b> This statement is not supported on T4000 Type 5 FPCs.</p> </div>	
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Policer Support for Aggregated Ethernet Bundle Overview on page 13</a></li> </ul>

## then

---

**Syntax**    then {  
              application-profile *profile-name*;  
              dscp (*alias* | *bits*);  
              forwarding-class *class-name*;  
              syslog;  
              (reflexive | reverse) {  
                  application-profile *profile-name*;  
                  dscp (*alias* | *bits*);  
                  forwarding-class *class-name*;  
                  syslog;  
              }  
          }

**Hierarchy Level**    [edit services cos rule *rule-name* term *term-name*]

**Release Information**    Statement introduced in Junos OS Release 8.1.

**Description**    Define the CoS term actions.

The remaining statements are explained separately.

**Required Privilege Level**    interface—To view this statement in the configuration.  
                                  interface-control—To add this statement to the configuration.

**Related Documentation**    • *Configuring Actions in a CoS Rule*  
                                  • *Configuring Actions in CoS Rules*

## three-color-policer (Applying)

<b>Syntax</b>	three-color-policer { (single-rate   two-rate) <i>policer-name</i> ; }
<b>Hierarchy Level</b>	[edit firewall family <i>family-name</i> filter <i>filter-name</i> term <i>term-name</i> then] [edit logical-systems <i>logical-system-name</i> <b>firewall</b> family <i>family-name</i> <b>filter</b> <i>filter-name</i> term <i>term-name</i> then]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4. <b>single-rate</b> statement added in Junos OS Release 8.2. Logical systems support introduced in Junos OS Release 9.3. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
<b>Description</b>	For M320 and T Series routers with Enhanced II Flexible PIC Concentrators (FPCs) and the T640 router with Enhanced Scaling FPC4, apply a tricolor marking policer.
<b>Options</b>	<b>single-rate</b> —Named tricolor policer is a single-rate policer.  <b>two-rate</b> —Named tricolor policer is a two-rate policer.  <b><i>policer-name</i></b> —Name of a tricolor policer.
<b>Required Privilege Level</b>	firewall—To view this statement in the configuration. firewall-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Applying Tricolor Marking Policers to Firewall Filters on page 26</a></li> <li>• <i>Firewall Filter Nonterminating Actions</i></li> <li>• <i>Three-Color Policer Configuration Overview</i></li> </ul>

## three-color-policer (Configuring)

---

Syntax	<pre>three-color-policer <i>policer-name</i> {     action {         loss-priority high then discard;     }     filter-specific;     logical-interface-policer;     physical-interface-policer;     shared-bandwidth-policer;     single-rate {         (color-aware   color-blind);         committed-burst-size <i>bytes</i>;         committed-information-rate <i>bps</i>;         excess-burst-size <i>bytes</i>;     }     two-rate {         (color-aware   color-blind);         committed-burst-size <i>bytes</i>;         committed-information-rate <i>bps</i>;         peak-burst-size <i>bytes</i>;         peak-information-rate <i>bps</i>;     } }</pre>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> <b>firewall</b> ], [edit <b>firewall</b> ], [edit logical-systems <i>logical-system-name</i> <b>firewall</b> ]
Release Information	Statement introduced before Junos OS Release 7.4. The <b>action</b> and <b>single-rate</b> statements added in Junos OS Release 8.2. Logical systems support introduced in Junos OS Release 9.3. Support at the [edit dynamic-profiles ... <b>firewall</b> ] hierarchy level introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Configure a three-color policer.
Options	<b><i>policer-name</i></b> —Name of the three-color policer. Reference this name when you apply the policer to an interface.  The remaining statements are explained separately.
Required Privilege Level	<b>firewall</b> —To view this statement in the configuration. <b>firewall-control</b> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <i>Statement Hierarchy for Configuring Policers</i></li><li>• <a href="#">Configuring Tricolor Marking Policers on page 25</a></li><li>• <i>Three-Color Policer Configuration Guidelines</i></li><li>• <i>Basic Single-Rate Three-Color Policers</i></li></ul>



- *Basic Two-Rate Three-Color Policers*
- *Two-Color and Three-Color Logical Interface Policers*
- *Two-Color and Three-Color Physical Interface Policers*
- *Two-Color and Three-Color Policers at Layer 2*

---

## tri-color

---

<b>Syntax</b>	tri-color;
<b>Hierarchy Level</b>	[edit class-of-service]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	For IPv4 packets on M320, MX Series, T Series routers with Enhanced II Flexible PIC Concentrators (FPCs), and EX Series switches, enable two-rate tricolor marking (TCM), as defined in RFC 2698.
<b>Default</b>	If you do not include this statement, tricolor marking is not enabled and the medium packet loss priority (PLP) is not configurable.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Tricolor Marking on page 17</a></li></ul>



## PART 3

# Index

- [Index on page 77](#)



# Index

## Symbols

#, comments in configuration statements.....	xiv
( ), in syntax descriptions.....	xiv
< >, in syntax descriptions.....	xiv
[ ], in configuration statements.....	xiv
{ }, in configuration statements.....	xiv
(pipe), in syntax descriptions.....	xiv

## A

action statement.....	40
usage guidelines.....	25
aggregate (logical interface) policer configuration statement for.....	59
architecture tricolor marking.....	11

## B

braces, in configuration statements.....	xiv
brackets angle, in syntax descriptions.....	xiv
square, in configuration statements.....	xiv

## C

code-points statement.....	42
color-aware single-rate.....	18
two-rate.....	21
color-blind single-rate.....	18
two-rate.....	21
comments, in configuration statements.....	xiv
conventions text and syntax.....	xiii
CoS policer actions, overview.....	3
curly braces, in configuration statements.....	xiv
customer support.....	xv
contacting JTAC.....	xv

## D

documentation comments on.....	xv
drop-profile statement.....	43
RED.....	43
<i>See also</i> RED	
drop-profile-map statement.....	43
dscp-ipv6 statement.....	46

## E

exp statement.....	47
--------------------	----

## F

family statement multifield classifiers.....	48
filter statement firewall.....	50
usage guidelines.....	28
firewall statement.....	51
font conventions.....	xiii
forwarding class policer actions overview.....	3
four loss priorities.....	8

## I

ieee-802.1 statement rewrite rules on logical interface.....	53
inet-precedence statement.....	55
input-policer statement.....	56
input-three-color statement.....	57

## L

Layer 2 policer applying to interface.....	29
example configurations.....	29
layer2-policer statement.....	58
usage guidelines.....	29
limitations tricolor marking.....	12
logical interface (aggregate) policer configuration statement for.....	59
logical interface-policer statement.....	59
logical-interface-policer statement usage guidelines.....	25

## M

manuals comments on.....	xv
-----------------------------	----

**O**

one-rate four-color marking.....	8
output-policer statement.....	62
output-three-color statement.....	63

**P**

packet loss priority	
policer actions	
overview.....	3
parentheses, in syntax descriptions.....	xiv
platform support	
tricolor marking.....	10
policer	
Layer 2	
applying to interface.....	29
example configurations.....	29
overview.....	3
policer actions	
forwarding class	
overview.....	3
packet loss-priority	
overview.....	3
policer statement	
configuring.....	64

**R**

RFC 2698.....	8
---------------	---

**S**

shared-bandwidth-policer statement.....	69
support, technical See technical support	
syntax conventions.....	xiii

**T**

technical support	
contacting JTAC.....	xv
term statement	
firewall	
usage guidelines.....	26
then statement	
CoS.....	70
three-color-policer statement.....	72
usage guidelines.....	25
tri-color statement.....	73
usage guidelines.....	24
tricolor marking	
architecture.....	11
filter, applying to.....	26
limitations.....	12

platform support.....	10
single-rate	
color-aware mode.....	18
color-blind mode.....	18
two-rate	
color-aware mode.....	21
color-blind mode.....	21
tricolor marking policer.....	8
configuring.....	25
enabling.....	24
example configuration.....	27, 28, 35
filter, applying to.....	26
interface, applying to.....	28
verifying your configuration.....	35
with BA classifier.....	31
with drop-profile map.....	33
with multifield classifier.....	32
with rewrite rule.....	34
two-rate tricolor marking.....	8
configuring the policer.....	25
enabling.....	24
example configuration.....	27, 28, 35
interface, applying to.....	28
verifying your configuration.....	35
with BA classifier.....	31
with drop-profile map.....	33
with multifield classifier.....	32
with rewrite rule.....	34