



---

Junos<sup>®</sup> OS

## Traffic Policer Configuration

Release

11.3



Published: 2011-09-20

Revision 1

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408-745-2000  
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 Traffic Policer Configuration*  
Copyright © 2011, Juniper Networks, Inc.  
All rights reserved.

Revision History  
September 2011—R1 Junos OS 11.3

The information in this document is current as of the date listed in the revision history.

## 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.



# Abbreviated Table of Contents

Part 1	Overview	
Chapter 1	Introduction to Traffic Policing .....	3
Chapter 2	Introduction to Policer Configuration .....	13
Chapter 3	Policer Rate Limits and Actions .....	25
Chapter 4	Best Practices for Policer Configuration .....	33
Part 2	Configuration	
Chapter 5	Single-Rate Two-Color Policers .....	39
Chapter 6	Three-Color Policers .....	109
Chapter 7	Logical and Physical Interface Policers .....	125
Chapter 8	Layer 2 Policers .....	147
Chapter 9	Policer Configuration Statements .....	165
Part 3	Administration	
Chapter 10	Traffic Policing Standards .....	213
Chapter 11	Traffic Policing Reference .....	215
Chapter 12	Firewall Filter and Policer Operational Mode Commands .....	219
Part 4	Index	
	Index .....	233
	Index of Statements and Commands .....	239



# Table of Contents

<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Introduction to Traffic Policing</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	6
	Traffic Policer Types	7
	Single-Rate Two-Color Policers	7
	Basic Single-Rate Two-Color Policer	7
	Bandwidth Policer	8
	Logical Bandwidth Policer	8
	Three-Color Policers	8
	Single-Rate Three-Color Policers	8
	Two-Rate Three-Color Policers	8
	Hierarchical Policers	9
	Two-Color and Three-Color Policer Options	9
	Logical Interface (Aggregate) Policers	9
	Physical Interface Policers	9
	Policers Applied to Layer 2 Traffic	10
	Multifield Classification	10
	Order of Policer and Firewall Filter Operations	10
<b>Chapter 2</b>	<b>Introduction to Policer Configuration</b>	<b>13</b>
	Statement Hierarchy for Configuring Policers	13
	Two-Color Policer Configuration Overview	15
	Three-Color Policer Configuration Overview	19
	Hierarchical Policer Configuration Overview	22
	Guidelines for Applying Traffic Policers	24
<b>Chapter 3</b>	<b>Policer Rate Limits and Actions</b>	<b>25</b>
	Policer Bandwidth and Burst-Size Limits	25
	Policer Color-Marking and Actions	26
	Single Token Bucket Algorithm	28
	Token Bucket Concepts	28
	Single Token Bucket Algorithm	29
	Conformance Measurement for Two-Color Marking	29
	Dual Token Bucket Algorithms	30
	Token Bucket Concepts	30
	Guaranteed Bandwidth for Three-Color Marking	31

	Nonconformance Measurement for Single-Rate Three-Color Marking . . . . .	31
	Nonconformance Measurement for Two-Rate Three-Color Marking . . . . .	31
<b>Chapter 4</b>	<b>Best Practices for Policer Configuration . . . . .</b>	<b>33</b>
	Calculation of Policer Burst-Size Limit . . . . .	33
	Guidelines for Choosing a Burst-Size Limit . . . . .	33
	Burst-Size Limit Based on the Line Rate of the Interface . . . . .	34
	Burst-Size Limit Based on the MTU of Traffic on the Interface . . . . .	35
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 5</b>	<b>Single-Rate Two-Color Policers . . . . .</b>	<b>39</b>
	Basic Single-Rate Two-Color Policers . . . . .	39
	Single-Rate Two-Color Policer Overview . . . . .	39
	Example: Configuring a Single-Rate Two-Color Policer . . . . .	40
	Example: Configuring Interface and Firewall Filter Policers at the Same Interface . . . . .	46
	Bandwidth Policers . . . . .	55
	Bandwidth Policer Overview . . . . .	56
	Guidelines for Configuring a Bandwidth Policer . . . . .	56
	Guidelines for Applying a Bandwidth Policer . . . . .	56
	Example: Configuring a Logical Bandwidth Policer . . . . .	57
	Filter-Specific Counters and Policers . . . . .	64
	Filter-Specific Policer Overview . . . . .	64
	Example: Configuring a Stateless Firewall Filter to Protect Against TCP and ICMP Floods . . . . .	65
	Prefix-Specific Counting and Policing Actions . . . . .	71
	Prefix-Specific Counting and Policing Overview . . . . .	71
	Separate Counting and Policing for Each IPv4 Address Range . . . . .	71
	Prefix-Specific Action Configuration . . . . .	72
	Counter and Policer Set Size and Indexing . . . . .	73
	Filter-Specific Counter and Policer Set Overview . . . . .	74
	Example: Configuring Prefix-Specific Counting and Policing . . . . .	74
	Prefix-Specific Counting and Policing Configuration Scenarios . . . . .	81
	Prefix Length of the Action and Prefix Length of Addresses in Filtered Packets . . . . .	81
	Scenario 1: Firewall Filter Term Matches on Multiple Addresses . . . . .	82
	Scenario 2: Subnet Prefix Is Longer Than the Prefix in the Filter Match Condition . . . . .	84
	Scenario 3: Subnet Prefix Is Shorter Than the Prefix in the Firewall Filter Match Condition . . . . .	85
	Multifield Classification . . . . .	87
	Multifield Classification Overview . . . . .	87
	Forwarding Classes and PLP Levels . . . . .	87
	Multifield Classification and BA Classification . . . . .	88
	Multifield Classification Used In Conjunction with Policers . . . . .	88
	Multifield Classification Requirements and Restrictions . . . . .	89
	Supported Platforms . . . . .	89
	CoS Tricolor Marking Requirement . . . . .	90
	Restrictions . . . . .	90



	Multifield Classification Limitations on M Series Routers . . . . .	90
	Problem: Output-Filter Matching on Input-Filter Classification . . . . .	90
	Workaround: Configure All Actions in the Ingress Filter . . . . .	91
	Example: Configuring Multifield Classification . . . . .	92
	Policer Overhead to Account for Rate Shaping in the Traffic Manager . . . . .	99
	Policer Overhead to Account for Rate Shaping Overview . . . . .	99
	Example: Configuring Policer Overhead to Account for Rate Shaping . . . . .	99
<b>Chapter 6</b>	<b>Three-Color Policers . . . . .</b>	<b>109</b>
	Three-Color Policer Configuration Guidelines . . . . .	109
	Platforms Supported for Three-Color Policers . . . . .	109
	Color Modes for Three-Color Policers . . . . .	109
	Color-Blind Mode . . . . .	110
	Color-Aware Mode . . . . .	110
	Naming Conventions for Three-Color Policers . . . . .	110
	Basic Single-Rate Three-Color Policers . . . . .	111
	Single-Rate Three-Color Policer Overview . . . . .	111
	Example: Configuring a Single-Rate Three-Color Policer . . . . .	112
	Basic Two-Rate Three-Color Policers . . . . .	117
	Two-Rate Three-Color Policer Overview . . . . .	117
	Example: Configuring a Two-Rate Three-Color Policer . . . . .	118
<b>Chapter 7</b>	<b>Logical and Physical Interface Policers . . . . .</b>	<b>125</b>
	Two-Color and Three-Color Logical Interface Policers . . . . .	125
	Logical Interface (Aggregate) Policer Overview . . . . .	125
	Example: Configuring a Two-Color Logical Interface (Aggregate) Policer . . . . .	126
	Example: Configuring a Three-Color Logical Interface (Aggregate) Policer . . . . .	131
	Two-Color and Three-Color Physical Interface Policers . . . . .	137
	Physical Interface Policer Overview . . . . .	137
	Example: Configuring a Physical Interface Policer for Aggregate Traffic at a Physical Interface . . . . .	139
<b>Chapter 8</b>	<b>Layer 2 Policers . . . . .</b>	<b>147</b>
	Hierarchical Policers . . . . .	147
	Hierarchical Policer Overview . . . . .	147
	Example: Configuring a Hierarchical Policer . . . . .	149
	Two-Color and Three-Color Policers at Layer 2 . . . . .	154
	Two-Color Policing at Layer 2 Overview . . . . .	154
	Guidelines for Configuring Two-Color Policing of Layer 2 Traffic . . . . .	155
	Statement Hierarchy for Configuring a Two-Color Policer for Layer 2 Traffic . . . . .	155
	Statement Hierarchy for Applying a Two-Color Policer to Layer 2 Traffic . . . . .	155
	Three-Color Policing at Layer 2 Overview . . . . .	156
	Guidelines for Configuring Three-Color Policing of Layer 2 Traffic . . . . .	156
	Statement Hierarchy for Configuring a Three-Color Policer for Layer 2 Traffic . . . . .	156

	Statement Hierarchy for Applying a Three-Color Policer to Layer 2	
	Traffic	157
	Example: Configuring a Three-Color Logical Interface (Aggregate)	
	Policer	157
<b>Chapter 9</b>	<b>Policer Configuration Statements</b>	<b>165</b>
	action	165
	aggregate (Hierarchical Policer)	166
	bandwidth-limit (Hierarchical Policer)	167
	bandwidth-limit (Policer)	168
	bandwidth-percent	170
	burst-size-limit (Hierarchical Policer)	172
	burst-size-limit (Policer)	173
	color-aware	175
	color-blind	176
	committed-burst-size	177
	committed-information-rate	179
	excess-burst-size	181
	filter-specific	182
	forwarding-class (Firewall Filter Action)	183
	hierarchical-policer	184
	if-exceeding (Hierarchical Policer)	185
	if-exceeding (Policer)	186
	input-hierarchical-policer	187
	input-policer	187
	input-three-color	188
	layer2-policer	189
	logical-bandwidth-policer	190
	logical-interface-policer	190
	loss-priority (Firewall Filter Action)	191
	loss-priority high then discard (Three-Color Policer)	192
	output-policer	193
	output-three-color	194
	peak-burst-size	195
	peak-information-rate	197
	physical-interface-filter	198
	physical-interface-policer	199
	policer (Applying to a Logical Interface)	200
	policer (Configuring)	201
	policer (Firewall Filter Action)	202
	prefix-action (Configuring)	203
	prefix-action (Firewall Filter Action)	204
	premium (Hierarchical Policer)	205
	single-rate	206
	three-color-policer (Configuring)	207
	three-color-policer (Firewall Filter Action)	208
	two-rate	209

<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 10</b>	<b>Traffic Policing Standards</b>	<b>213</b>
	Supported Standards for Policing	213
<b>Chapter 11</b>	<b>Traffic Policing Reference</b>	<b>215</b>
	Using the CLI Editor in Configuration Mode	215
<b>Chapter 12</b>	<b>Firewall Filter and Policer Operational Mode Commands</b>	<b>219</b>
	clear firewall	220
	show firewall	221
	show firewall filter version	224
	show firewall log	225
	show firewall prefix-action-stats	228
	show policer	229
<b>Part 4</b>	<b>Index</b>	
	Index	233
	Index of Statements and Commands	239



# List of Figures

Part 1	Overview	
Chapter 1	Introduction to Traffic Policing .....	3
	Figure 1: Network Traffic and Burst Rates .....	4
	Figure 2: Incoming and Outgoing Policers and Firewall Filters .....	11



# List of Tables

<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 2</b>	<b>Introduction to Policer Configuration . . . . .</b>	<b>13</b>
	Table 1: Two-Color Policer Configuration and Application Overview . . . . .	15
	Table 2: Three-Color Policer Configuration and Application Overview . . . . .	20
	Table 3: Hierarchical Policer Configuration and Application Summary . . . . .	23
<b>Chapter 3</b>	<b>Policer Rate Limits and Actions . . . . .</b>	<b>25</b>
	Table 4: Policer Bandwidth Limits and Burst-Size Limits . . . . .	25
	Table 5: Implicit and Configurable Policer Actions Based on Color Marking . . . . .	26
<b>Chapter 4</b>	<b>Best Practices for Policer Configuration . . . . .</b>	<b>33</b>
	Table 6: Example Calculations of Policer Burst-Size Limit . . . . .	34
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 5</b>	<b>Single-Rate Two-Color Policers . . . . .</b>	<b>39</b>
	Table 7: Examples of Counter and Policer Set Size and Indexing . . . . .	73
	Table 8: Summary of Prefix-Specific Action Scenarios . . . . .	81
<b>Chapter 6</b>	<b>Three-Color Policers . . . . .</b>	<b>109</b>
	Table 9: Recommended Naming Convention for Policers . . . . .	111
<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 12</b>	<b>Firewall Filter and Policer Operational Mode Commands . . . . .</b>	<b>219</b>
	Table 10: show firewall Output Fields . . . . .	222
	Table 11: show firewall filter version Output Fields . . . . .	224
	Table 12: show firewall log Output Fields . . . . .	225
	Table 13: show firewall prefix-action-stats Output Fields . . . . .	228
	Table 14: show policer Output Fields . . . . .	229





## PART 1

# Overview

- [Introduction to Traffic Policing on page 3](#)
- [Introduction to Policer Configuration on page 13](#)
- [Policer Rate Limits and Actions on page 25](#)
- [Best Practices for Policer Configuration on page 33](#)



## CHAPTER 1

# Introduction to Traffic Policing

- [Traffic Policing Overview on page 3](#)
- [Traffic Policer Types on page 7](#)
- [Order of Policer and Firewall Filter Operations on page 10](#)

## 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 6](#)

## 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.

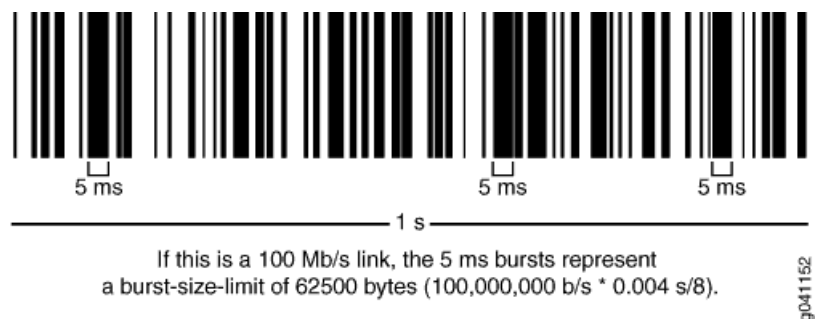
## Traffic Limits

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) 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 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 **policer *policer-name*** nonterminating action or the **three-color-policer (single-rate | two-rate) *policer-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” in the [Junos OS Firewall Filter and Policer Configuration Guide](#)
- [Traffic Policer Types on page 7](#)
- [Order of Policer and Firewall Filter Operations on page 10](#)
- [Packet Flow Through the CoS Process Overview](#)

---

## Traffic Policer Types

This topic covers the following information:

- [Single-Rate Two-Color Policers on page 7](#)
- [Three-Color Policers on page 8](#)
- [Hierarchical Policers on page 9](#)
- [Two-Color and Three-Color Policer Options on page 9](#)

### Single-Rate Two-Color Policers

You can use a single-rate two-color policer, or “policer” when used without qualification, to rate-limit a traffic flow to an average bits-per-second arrival rate (specified by the single specified bandwidth limit) while allowing bursts of traffic for short periods (controlled by the single specified burst-size limit). This type of policer categorizes a traffic flow as either green (conforming) or red (nonconforming). Packets in a green flow are implicitly set to a **low** loss priority and then transmitted. Packets in a red flow are handled according to actions specified in the policer configuration. Packets in a red flow can be marked—set to a specified forwarding class, set to a specified loss priority, or both—or they can be discarded.

A single-rate two-color policer is most useful for metering traffic at the port (physical interface) level.

---

#### Basic Single-Rate Two-Color Policer

You can apply a basic single-rate two-color policer to Layer 3 traffic in either of two ways: as an interface policer or as a firewall filter policer. You can apply the policer as an *interface policer*, meaning that you apply the policer directly to a logical interface at the protocol family level. If you want to apply the policer to selected packets only, you can apply the policer as a *firewall filter policer*, meaning that you reference the policer in a stateless firewall filter term and then apply the filter to a logical interface at the protocol family level.

### Bandwidth Policer

---

A bandwidth policer is simply a single-rate two-color policer that is defined using a bandwidth limit specified as a percentage value rather than as an absolute number of bits per second. When you apply the policer (as an interface policer or as a firewall filter policer) to a logical interface at the protocol family level, the effective bandwidth limit is calculated based on either the physical interface media rate or the logical interface configured shaping rate.

### Logical Bandwidth Policer

---

A logical bandwidth policer is a bandwidth policer for which the effective bandwidth limit is calculated based on the logical interface configured shaping rate. You can apply the policer as a firewall filter policer only, and the firewall filter must be configured as an interface-specific filter. When you apply an interface-specific filter to multiple logical interfaces on supported routing platforms, any **count** or **police** actions act on the traffic stream entering or exiting each individual interface, regardless of the sum of traffic on the multiple interfaces.

## Three-Color Policers

The Junos OS supports two types of three-color policers: single-rate and two-rate. The main difference between a single-rate and a two-rate policer is that the single-rate policer allows bursts of traffic for short periods, while the two-rate policer allows more sustained bursts of traffic. Single-rate policing is implemented using a single token-bucket model, so that periods of relatively low traffic must occur between traffic bursts to allow the token bucket to refill. Two-rate policing is implemented using a dual token-bucket model, which allows bursts of traffic for longer periods.

### Single-Rate Three-Color Policers

---

The single-rate three-color type of policer is defined in RFC 2697, *A Single Rate Three Color Marker*. You use this type of policer to rate-limit a traffic flow to a single rate and three traffic categories (green, yellow, and red). A single-rate three-color policer defines a *committed* bandwidth limit and burst-size limit plus an excess burst-size limit. Traffic that conforms to the committed traffic limits is categorized as green (conforming). Traffic that conforms to the bandwidth limit while allowing bursts of traffic as controlled by the excess burst-size limit is categorized as yellow. All other traffic is categorized as red.

A single-rate three-color policer is most useful when a service is structured according to packet length, not peak arrival rate.

### Two-Rate Three-Color Policers

---

The two-rate three-color type of policer is defined in RFC 2698, *A Two Rate Three Color Marker*. You use this type of policer to rate-limit a traffic flow to two rates and three traffic categories (green, yellow, and red). A two-rate three-color policer defines a *committed* bandwidth limit and burst-size limit plus a *peak* bandwidth limit and burst-size limit. Traffic that conforms to the committed traffic limits is categorized as green (conforming). Traffic that exceeds the committed traffic limits but remains below the peak traffic limits is categorized as yellow. Traffic that exceeds the peak traffic limits is categorized as red.



A two-rate three-color policer is most useful when a service is structured according to arrival rates and not necessarily packet length.

## Hierarchical Policers

You can use a hierarchical policer to rate-limit ingress Layer 2 traffic at a physical or logical interface and apply different policing actions based on whether the packets are classified for expedited forwarding (EF) or for a lower priority output queue. This feature is supported on SONET interfaces hosted on M40e, M120, and M320 edge routers with incoming Flexible PIC Concentrators (FPCs) as SFPC and outgoing FPCs as FFPC, and on T320, T640, and T1600 core routers with Enhanced Intelligent Queuing (IQE) PICs.

## Two-Color and Three-Color Policer Options

Both two-color and three-color policers can be configured with the following options:

- [Logical Interface \(Aggregate\) Policers on page 9](#)
- [Physical Interface Policers on page 9](#)
- [Policers Applied to Layer 2 Traffic on page 10](#)
- [Multifield Classification on page 10](#)

### Logical Interface (Aggregate) Policers

---

A logical interface policer—also called an aggregate policer—is a two-color or three-color policer that you can apply to multiple protocol families on the same logical interface without creating multiple instances of the policer. You apply a logical interface policer directly to a logical interface configuration (and not by referencing the policer in a stateless firewall filter and then applying the filter to the logical interface).

- You can apply the policer at the interface logical unit level to rate-limit all traffic types, regardless of the protocol family.
- You can also apply the policer at the logical interface protocol family level, to rate-limit traffic for a specific protocol family.

You can apply a logical interface policer to unicast traffic only. For information about configuring a stateless firewall filter for flooded traffic, see “Applying Filters to Forwarding Tables” in the “Traffic Sampling, Forwarding, and Monitoring” section of the [Junos OS Routing Policy Configuration Guide](#).

### Physical Interface Policers

---

A physical interface policer is a two-color or three-color policer that applies to all logical interfaces and protocol families configured on a physical interface, even if the logical interfaces belong to different routing instances. You apply a physical interface policer to a logical interface at the protocol level through a physical interface filter only, but rate limiting is performed aggregately for all logical interfaces and protocol families configured on the underlying physical interface.

This feature enables you to use a single policer instance to perform aggregate policing for different protocol families and different logical interfaces on the same physical interface.

### Policers Applied to Layer 2 Traffic

---

In addition to hierarchical policing, you can also apply single-rate two-color policers and three-color policers (both single-rate and two-rate) to Layer 2 input or output traffic. You must configure the two-color or three-color policer as a logical interface policer and reference the policer in the interface configuration at the logical unit level, and not at the protocol level. You cannot apply a two-color or three-color policer to Layer 2 traffic as a stateless firewall filter action.

### Multifield Classification

---

Like behavior aggregate (BA) classification, which is sometimes referred to as class-of-service (CoS) value traffic classification, multifield classification is a method of classifying incoming traffic by associating each packet with a forwarding class, a packet loss priority level, or both. The CoS scheduling configuration assigns packets to output queues based on forwarding class. The CoS random early detection (RED) process uses the drop probability configuration, output queue fullness percentage, and packet loss priority to drop packets as needed to control congestion at the output stage.

BA classification and multifield classification use different fields of a packet to perform traffic classification. BA classification is based on a *CoS value* in the IP packet header. Multifield classification can be based on *multiple fields* in the IP packet header, including CoS values. Multifield classification is used instead of BA classification when you need to classify packets based on information in the packet other than the CoS values only. Multifield classification is configured using a stateless firewall filter term that matches on any packet header fields and associates matched packets with a forwarding class, a loss priority, or both. The forwarding class or loss priority can be set by a firewall filter action or by a policer referenced as a firewall filter action.

#### Related Documentation

- [Traffic Policing Overview on page 3](#)
- [Order of Policer and Firewall Filter Operations on page 10](#)
- [Two-Color Policer Configuration Overview on page 15](#)
- [Three-Color Policer Configuration Overview on page 19](#)
- [Hierarchical Policer Configuration Overview on page 22](#)
- [Two-Color Policing at Layer 2 Overview on page 154](#)
- [Three-Color Policing at Layer 2 Overview on page 156](#)

### Order of Policer and Firewall Filter Operations

---

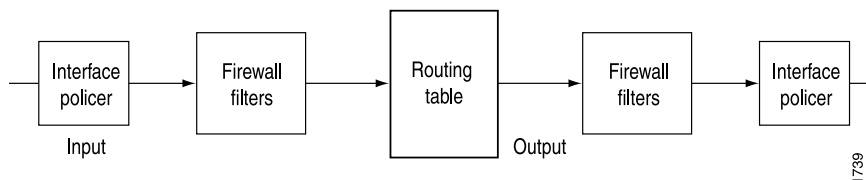
You can apply both a traffic policer and a stateless firewall filter (with or without policing actions) to a single logical interface at the same time. In this case, the order of precedence of operations is such that policers applied directly to the logical interface are evaluated before input filters but after output filters.

- If an input firewall filter is configured on the same logical interface as a policer, the policer is executed first.

- If an output firewall filter is configured on the same logical interface as a policer, the firewall filter is executed first.

Figure 2 on page 11 illustrates the order of policer and firewall filter processing at the same interface.

**Figure 2: Incoming and Outgoing Policers and Firewall Filters**



**Related  
Documentation**

- [Traffic Policing Overview on page 3](#)
- [Traffic Policer Types on page 7](#)
- [Statement Hierarchy for Configuring Policers on page 13](#)
- [Guidelines for Applying Traffic Policers on page 24](#)



## CHAPTER 2

# Introduction to Policer Configuration

- [Statement Hierarchy for Configuring Policers on page 13](#)
- [Two-Color Policer Configuration Overview on page 15](#)
- [Three-Color Policer Configuration Overview on page 19](#)
- [Hierarchical Policer Configuration Overview on page 22](#)
- [Guidelines for Applying Traffic Policers on page 24](#)

## Statement Hierarchy for Configuring Policers

---

```
firewall {
  family (any | bridge | ccc | inet | inet6 | mpls | vpls) {
    filter filter-name {
      ... protocol-family-specific-firewall-filter-configuration ...
      prefix-action name {
        count;
        destination-prefix-length prefix-length;
        policer policer-name;
        source-prefix-length prefix-length;
        subnet-prefix-length prefix-length;
      }
    }
  }
  filter filter-name {
    accounting-profile [ profile-names ];
    interface-specific;
    physical-interface-filter;
    term term-name {
      filter filter-name;
      from {
        ... ipv4-firewall-filter-match-conditions ...
      }
      then {
        ... ipv4-firewall-filter-terminating-actions ...
        ... ipv4-firewall-filter-nonterminating-actions ...
        next term;
      }
    }
  }
  hierarchical-policer policer-name {
    aggregate {
```

```

    if-exceeding {
        bandwidth-limit-limit bps;
        burst-size-limit bytes;
    }
    then {
        discard;
        forwarding-class class-name;
        loss-priority (high | low | medium-high | medium-low);
    }
}
premium {
    if-exceeding {
        bandwidth-limit bps;
        burst-size-limit bytes;
    }
    then {
        discard;
    }
}
}
interface-set interface-set-name {
    interface-name;
}
load-balance-group group-name {
    next-hop-group [ group-names ];
}
}
policer policer-name {
    filter-specific;
    if-exceeding {
        (bandwidth-limit bps | bandwidth-percent percentage);
        burst-size-limit bytes;
    }
    logical-bandwidth-policer;
    logical-interface-policer;
    physical-interface-policer;
    then {
        discard;
        forwarding-class class-name;
        loss-priority (high | low | medium-high | medium-low);
    }
}
}
three-color-policer policer-name {
    action {
        loss-priority high then discard;
    }
    logical-interface-policer;
    physical-interface-policer;
    single-rate {
        (color-aware | color-blind);
        committed-burst-size bytes;
        committed-information-rate bps;
        excess-burst-size bytes;
    }
    two-rate {
        (color-aware | color-blind);
        committed-burst-size bytes;

```

```

        committed-information-rate bps;
        peak-burst-size bytes;
        peak-information-rate bps;
    }
}

```

#### Related Documentation

- [Two-Color Policer Configuration Overview on page 15](#)
- [Three-Color Policer Configuration Overview on page 19](#)
- [Hierarchical Policer Configuration Overview on page 22](#)
- [Guidelines for Applying Traffic Policers on page 24](#)

## Two-Color Policer Configuration Overview

[Table 1 on page 15](#) describes the hierarchy levels at which you can configure and apply single-rate two-color policers to Layer 3 traffic. For information about applying single-rate two-color policers to Layer 2 traffic, see “[Two-Color Policing at Layer 2 Overview](#)” on [page 154](#).

**Table 1: Two-Color Policer Configuration and Application Overview**

Policer Configuration	Layer 3 Application	Key Points
<b>Single-Rate Two-Color Policer</b> <i>Defines traffic rate limiting that you can apply to Layer 3 protocol-specific traffic at a logical interface. Can be applied as an interface policer or as a firewall filter policer.</i>		
Basic policer configuration:  <pre> [edit firewall] policer <i>policer-name</i> {   if-exceeding {     bandwidth-limit <i>bps</i>;     burst-size-limit <i>bytes</i>;   }   then {     discard;     forwarding-class <i>class-name</i>;     loss-priority <i>supported-value</i>;   } } </pre>	Method A—Apply as an interface policer at the protocol family level:  <pre> [edit interfaces] interface-name {   unit <i>unit-number</i> {     family <i>family-name</i> {       policer {         input <i>policer-name</i>;         output <i>policer-name</i>;       }     }   } } </pre> Method B—Apply as a firewall filter policer at the protocol family level:  <pre> [edit firewall] family <i>family-name</i> {   filter <i>filter-name</i> {     interface-specific; # (*)     from {       ... <i>match-conditions</i> ...     }     then { </pre>	Policer configuration: <ul style="list-style-type: none"> <li>• Use <b>bandwidth-limit <i>bps</i></b> to specify an absolute value.</li> </ul> Firewall filter configuration (*): <ul style="list-style-type: none"> <li>• If applying to multiple interfaces, include the <b>interface-specific</b> statement to create unique policers and counters for each interface.</li> </ul> Interface policer verification: <ul style="list-style-type: none"> <li>• Use the <b>show interfaces (detail   extensive)</b> operational mode command.</li> <li>• Use the <b>show policer</b> operational mode command.</li> </ul> Firewall filter policer verification: <ul style="list-style-type: none"> <li>• Use the <b>show interfaces (detail   extensive)</b> operational mode command.</li> </ul>

Table 1: Two-Color Policer Configuration and Application Overview (*continued*)

Policer Configuration	Layer 3 Application	Key Points
	<pre>    policer <i>policer-name</i>;   } }  [edit interfaces] <i>interface-name</i> {   unit <i>unit-number</i> {     family <i>family-name</i> {       filter {         input <i>filter-name</i>;         output <i>filter-name</i>;       }       ... <i>protocol-configuration</i> ...     }   } }</pre>	<ul style="list-style-type: none"><li>• Use the <b>show firewall filter <i>filter-name</i></b> operational mode command.</li></ul>



Table 1: Two-Color Policer Configuration and Application Overview (*continued*)

Policy Configuration	Layer 3 Application	Key Points
<b>Bandwidth Policer</b> <i>Defines traffic rate limiting that you can apply to Layer 3 protocol-specific traffic at a logical interface, but the bandwidth limit is specified as a percentage value. Bandwidth can be based on physical interface line rate (the default) or the logical interface shaping rate. Can be applied as an interface policer or as a firewall filter policer where the filter is either interface-specific or a physical interface filter.</i>		
Bandwidth policer configuration:  <pre>[edit firewall] policer <i>policer-name</i> {   logical-bandwidth-policer;   if-exceeding {     bandwidth-percent (1..100);     burst-size-limit <i>bytes</i>;   }   then {     discard;     forwarding-class <i>class-name</i>;     loss-priority <i>supported-value</i>;   } }</pre>	Method A—Apply as an interface policer at the protocol family level:  <pre>[edit interfaces] interface-name {   unit <i>unit-number</i> {     family <i>family-name</i> {       policer {         input <i>policer-name</i>;         output <i>policer-name</i>;       }     }   } }</pre> Method B—Apply as a firewall filter policer at the protocol family level:  <pre>[edit firewall] family <i>family-name</i> {   filter <i>filter-name</i> {     interface-specific;     from {       ... <i>match-conditions</i> ...     }     then {       policer <i>policer-name</i>;     }   } }</pre> <pre>[edit interfaces] interface-name {   unit <i>unit-number</i> {     family <i>family-name</i> {       filter {         input <i>filter-name</i>;         output <i>filter-name</i>;       }       ... <i>protocol-configuration</i> ...     }   } }</pre>	Policer configuration:  <ul style="list-style-type: none"> <li>Use the <b>bandwidth-percent <i>percentage</i></b> statement instead of the <b>bandwidth-limit <i>bps</i></b> statement. By default, bandwidth policing rate-limits traffic based on a percentage of the physical interface media rate.</li> <li>To rate-limit traffic based on a percentage of the logical interface configured shaping rate, also include the <b>logical-bandwidth-policer</b> statement.</li> </ul> Firewall filter configuration:  <ul style="list-style-type: none"> <li>Percentage bandwidth policers can only be referenced by filters configured with the <b>interface-specific</b> statement.</li> </ul> Interface policer verification:  <ul style="list-style-type: none"> <li>Use the <b>show interfaces (detail   extensive)</b> operational mode command.</li> <li>Use the <b>show policer</b> operational mode command.</li> </ul> Firewall filter policer verification:  <ul style="list-style-type: none"> <li>Use the <b>show interfaces (detail   extensive)</b> operational mode command.</li> <li>Use the <b>show firewall filter <i>filter-name</i></b> operational mode command.</li> </ul>

Table 1: Two-Color Policer Configuration and Application Overview (*continued*)

Policer Configuration	Layer 3 Application	Key Points
<b>Logical Interface (Aggregate) Policer</b> <i>Defines traffic rate limiting that you can apply to multiple protocol families on the same logical interface without creating multiple instances of the policer. Can be applied directly to a logical interface configuration only.</i>		
Logical interface policer configuration: <pre>[edit firewall] policer <i>policer-name</i> {   logical-interface-policer;   if-exceeding {     bandwidth-limit <i>bps</i>;     burst-size-limit <i>bytes</i>;   }   then {     discard;     forwarding-class <i>class-name</i>;     loss-priority <i>supported-value</i>;   } }</pre>	Apply as an interface policer only: <pre>[edit interfaces] interface-name {   unit <i>unit-number</i> {     policer { # All protocols       input <i>policer-name</i>;       output <i>policer-name</i>;     }   }   family <i>family-name</i> {     policer { # One protocol       input <i>policer-name</i>;       output <i>policer-name</i>;     }   } }</pre>	Policer configuration: <ul style="list-style-type: none"> <li>• Include the <b>logical-interface-policer</b> statement.</li> </ul> Two options for interface policer application: <ul style="list-style-type: none"> <li>• To rate-limit all traffic types, regardless of the protocol family, apply the logical interface policer at the logical unit level.</li> <li>• To rate-limit traffic of a specific protocol family, apply the logical interface policer at the protocol family level.</li> </ul> Interface policer verification: <ul style="list-style-type: none"> <li>• Use the <b>show interfaces (detail   extensive)</b> operational mode command.</li> <li>• Use the <b>show policer</b> operational mode command.</li> </ul>

Table 1: Two-Color Policer Configuration and Application Overview (*continued*)

Policy Configuration	Layer 3 Application	Key Points
<b>Physical Interface Policer</b> Defines traffic rate limiting that applies to all logical interfaces and protocol families configured on a physical interface, even if the interfaces belong to different routing instances. Can be applied as a firewall filter policer referenced from a physical interface filter only.		
Physical interface policer configuration:  <pre>[edit firewall] policer <i>policer-name</i> {   physical-interface-policer;   if-exceeding {     bandwidth-limit <i>bps</i>;     burst-size-limit <i>bytes</i>;   }   then {     discard;     forwarding-class <i>class-name</i>;     loss-priority <i>supported-value</i>;   } }</pre>	Apply as a firewall filter policer referenced from a physical interface filter that you apply at the protocol family level:  <pre>[edit firewall] family <i>family-name</i> {   filter <i>filter-name</i> {     physical-interface-filter;     from {       ... <i>match-conditions</i> ...     }     then {       policer <i>policer-name</i>;     }   } }</pre> <pre>[edit interfaces] interface-name {   unit <i>number</i> {     family <i>family-name</i> {       filter {         input <i>filter-name</i>;         output <i>filter-name</i>;       }       ... <i>protocol-configuration</i> ...     }   } }</pre>	Policer configuration: <ul style="list-style-type: none"> <li>• Include the <b>physical-interface-policer</b> statement.</li> </ul> Firewall filter configuration: <ul style="list-style-type: none"> <li>• Include the <b>physical-interface-filter</b> statement.</li> </ul> Application: <ul style="list-style-type: none"> <li>• Apply the filter to the input or output of a logical interface at the protocol family level.</li> </ul> Firewall filter policer verification: <ul style="list-style-type: none"> <li>• Use the <b>show interfaces (detail   extensive)</b> operational mode command.</li> <li>• Use the <b>show firewall filter <i>filter-name</i></b> operational mode command.</li> </ul>

**Related Documentation**

- [Basic Single-Rate Two-Color Policers on page 39](#)
- [Bandwidth Policers on page 55](#)
- [Filter-Specific Counters and Policers on page 64](#)
- [Prefix-Specific Counting and Policing Actions on page 71](#)
- [Multifield Classification on page 87](#)
- [Policer Overhead to Account for Rate Shaping in the Traffic Manager on page 99](#)
- [Two-Color and Three-Color Physical Interface Policers on page 137](#)

## Three-Color Policer Configuration Overview

Table 2 on page 20 describes the hierarchy levels at which you can configure and apply single-rate tricolor-marking (single-rate TCM) policers and two-rate tricolor-marking

(two-rate TCM) policers to Layer 3 traffic. For information about applying three-color policers to Layer 2 traffic, see [“Three-Color Policing at Layer 2 Overview”](#) on page 156.

**Table 2: Three-Color Policer Configuration and Application Overview**

Policer Configuration	Layer 3 Application	Key Points
<b>Single-Rate Three-Color Policer</b> Defines traffic rate limiting that you can apply to Layer 3 protocol-specific traffic at a logical interface. Can be applied as a firewall filter policer only. Provides moderate allowances for short periods of traffic that exceed the committed burst size.		
Basic single-rate TCM policer configuration:  <pre>[edit firewall] three-color-policer <i>policer-name</i> {   single-rate {     (color-aware   color-blind);     committed-information-rate       <i>bps</i>;     committed-burst-size <i>bytes</i>;     excess-burst-size <i>bytes</i>;   }   action {     loss-priority high then discard;   } }</pre>	Reference the policer from a firewall filter, and apply the filter to a protocol family on a logical interface:  <pre>[edit firewall] family <i>family-name</i> {   filter <i>filter-name</i> {     term <i>term-name</i> {       from {         ... <i>match-conditions</i> ...       }       then {         three-color-policer {           single-rate <i>policer-name</i>;         }       }     }   } }</pre> Apply the filter to a logical interface at the protocol family level:  <pre>[edit interfaces] interface <i>name</i> {   unit <i>unit-number</i> {     family <i>family-name</i> {       filter {         input <i>filter-name</i>;         output <i>filter-name</i>;       }     }   } }</pre>	Policer configuration: <ul style="list-style-type: none"> <li>Include the <b>single-rate (color-aware   color-blind)</b> statement.</li> </ul> Firewall filter configuration: <ul style="list-style-type: none"> <li>Include the <b>three-color-policer single-rate <i>policer-name</i></b> action.</li> </ul> Applying the firewall filter to the logical interface: <ul style="list-style-type: none"> <li>Include the <b>filter (input   output) <i>filter-name</i></b> statement.</li> </ul>

Table 2: Three-Color Policer Configuration and Application Overview (*continued*)

Policer Configuration	Layer 3 Application	Key Points
<b>Single-Rate Three-Color Physical Interface Policer</b> Defines traffic rate limiting that applies to all logical interfaces and protocol families configured on a physical interface, even if the interfaces belong to different routing instances. Can be applied as a firewall filter policer only.		
Physical interface single-rate TCM policer:  <pre>[edit firewall] three-color-policer <i>policer-name</i> {   physical-interface-policer;   single-rate {     (color-aware   color-blind);     committed-information-rate <i>bps</i>;     committed-burst-size <i>bytes</i>;     excess-burst-size <i>bytes</i>;   }   action {     loss-priority high then discard;   } }</pre>	Reference the policer from a physical interface filter only, and apply the filter to a protocol family on a logical interface:  <pre>[edit firewall] family <i>family-name</i> {   filter <i>filter-name</i> {     physical-interface-filter     term <i>term-name</i> {       from {         ... <i>match-conditions</i> ...       }       then {         three-color-policer {           single-rate <i>policer-name</i>;         }       }     }   } }</pre> <pre>[edit interfaces] interface-name {   unit <i>number</i> {     family <i>family-name</i> {       filter {         input <i>filter-name</i>;         output <i>filter-name</i>;       }     }   } }</pre>	Policer configuration: <ul style="list-style-type: none"> <li>• Include the <b>physical-interface-policer</b> statement.</li> </ul> Firewall filter configuration: <ul style="list-style-type: none"> <li>• Include the <b>physical-interface-filter</b> statement.</li> </ul> Application: <ul style="list-style-type: none"> <li>• Include the <b>filter (input   output) <i>filter-name</i></b> statement.</li> </ul> Verification <ul style="list-style-type: none"> <li>• To verify, use the <b>show firewall filter <i>filter-name</i></b> operational mode command.</li> </ul>

Table 2: Three-Color Policer Configuration and Application Overview (*continued*)

Policer Configuration	Layer 3 Application	Key Points
<b>Basic Two-Rate Three-Color Policer</b> Defines traffic rate limiting that you can apply to Layer 3 protocol-specific traffic at a logical interface. Can be applied as a firewall filter policer only. Provides moderate allowances for sustained periods of traffic that exceed the committed bandwidth limit or burst size.		
Basic two-rate TCM policer configuration:  <pre>[edit firewall] three-color-policer <i>policer-name</i> {   two-rate {     (color-aware   color-blind);     committed-information-rate <i>bps</i>;     committed-burst-size <i>bytes</i>;     peak-information-rate <i>bps</i>;     peak-burst-size <i>bytes</i>;   }   action {     loss-priority high then discard;   } }</pre>	Reference the policer from a firewall filter, and apply the filter to a protocol family on a logical interface:  <pre>[edit firewall] family <i>family-name</i> {   filter <i>filter-name</i> {     term <i>term-name</i> {       from {         ... <i>match-conditions</i> ...       }       then {         three-color-policer {           two-rate <i>policer-name</i>;         }       }     }   } }</pre> <pre>[edit interfaces] interface-name {   unit <i>unit-number</i> {     family <i>family-name</i> {       filter {         input <i>filter-name</i>;         output <i>filter-name</i>;       }     }   } }</pre>	Policer configuration: <ul style="list-style-type: none"> <li>Include the <b>two-rate (color-aware   color-blind)</b> statement.</li> </ul> Firewall filter configuration: <ul style="list-style-type: none"> <li>Include the <b>three-color-policer two-rate <i>policer-name</i></b> action.</li> </ul> Applying the firewall filter to the logical interface: <ul style="list-style-type: none"> <li>Include the <b>filter (input   output) <i>filter-name</i></b> statement.</li> </ul>

**Related Documentation**

- [Three-Color Policer Configuration Guidelines on page 109](#)
- [Basic Single-Rate Three-Color Policers on page 111](#)
- [Basic Two-Rate Three-Color Policers on page 117](#)
- [Two-Color and Three-Color Logical Interface Policers on page 125](#)
- [Two-Color and Three-Color Physical Interface Policers on page 137](#)

## Hierarchical Policer Configuration Overview

Table 3 on page 23 describes the hierarchy levels at which you can configure and apply hierarchical policers.

Table 3: Hierarchical Policer Configuration and Application Summary

Policer Configuration	Layer 2 Application	Key Points
<b>Hierarchical Policer</b> Hierarchically rate-limits Layer 2 ingress traffic for all protocol families. Cannot be applied to egress traffic, Layer 3 traffic, or at a specific protocol level of the interface hierarchy.		
Supported on the following interfaces:		
<ul style="list-style-type: none"> <li>• SONET interfaces hosted on M40e, M120, and M320 edge routers with incoming FPCs as SFPC and outgoing FPCs as FFPC.</li> <li>• SONET interfaces hosted on T320, T640, and T1600 core routers with Enhanced Intelligent Queuing (IQE) PICs.</li> <li>• Ethernet interfaces on Gigabit Ethernet Intelligent Queuing 2 (IQ2) and Ethernet Enhanced IQ2 (IQ2E) PICs.</li> <li>• Interfaces on DPCs in MX Series routers.</li> </ul>		
Aggregate and premium policing components of a hierarchical policer:	Option A—Apply directly to Layer 2 input traffic on a physical interface:	Hierarchically rate-limit Layer 2 ingress traffic for all protocol families and logical interfaces configured on a physical interface.
<pre>[edit firewall] hierarchical-policer <i>policer-name</i> {   aggregate {     if-exceeding {       bandwidth-limit <i>bps</i>;       burst-size-limit <i>bytes</i>;     }     then {       discard;       forwarding-class <i>class-name</i>;       loss-priority <i>supported-value</i>;     }   }   premium {     if-exceeding {       bandwidth-limit <i>bps</i>;       burst-size-limit <i>bytes</i>;     }     then {       discard;     }   } }</pre>	<pre>[edit interfaces] interface-name {   layer2-policer {     input-hierarchical-policer <i>policer-name</i>;   } }</pre>	Include the <b>layer2-policer</b> configuration statement at the <b>[edit interfaces <i>interface-name</i>]</b> hierarchy level.  <b>NOTE:</b> If you apply a hierarchical policer at a physical interface, you cannot also apply a hierarchical policer to any of the member logical interfaces.
	Option B—Apply directly to Layer 2 input traffic on a logical interface.	Hierarchically rate-limit Layer 2 ingress traffic for all protocol families configured on a specific logical interface.
	<pre>[edit interfaces] interface-name {   unit <i>unit-number</i> {     layer2-policer {       input-hierarchical-policer <i>policer-name</i>;     }   } }</pre>	Include the <b>layer2-policer</b> configuration statement at the <b>[edit interfaces <i>interface-name</i> unit <i>unit-number</i>]</b> hierarchy level.  <b>NOTE:</b> You must configure at least one protocol family for the logical interface.

Related Documentation • [Hierarchical Policers on page 147](#)

## Guidelines for Applying Traffic Policers

---

The following general guidelines pertain to applying traffic policers:

- Only one type of policer can be applied to the input or output of the same physical or logical interface. For example, you are not allowed to apply a policer and a hierarchical policer in the same direction at the same logical interface.
- Chaining of policers—that is, applying policers to both a port and the logical interfaces of that port—is not allowed.
- A maximum of 64 policers is supported per physical or logical interface, provided no behavior aggregate (BA) classification—traffic classification based on CoS values in the packet headers—is applied to the logical interface.
- The policer should be independent of BA classification. Without BA classification, all traffic on an interface is treated either as expedited forwarding (EF) or non-EF, based on the configuration. With BA classification, a physical or logical interface can support up to 64 policers. The interface might be a physical interface or logical interface.
- With BA classification, the miscellaneous traffic (the traffic *not* matching any of the BA classification DSCP/EXP bits) is policed as non-EF traffic. No separate policers are installed for this traffic.
- Policers can be applied to unicast packets only. For information about configuring a filter for flooded traffic, see “Applying Filters to Forwarding Tables” in the “Traffic Sampling, Forwarding, and Monitoring” section of the [Junos OS Routing Policy Configuration Guide](#).

### Related Documentation

- [Statement Hierarchy for Configuring Policers on page 13](#)
- [Two-Color Policer Configuration Overview on page 15](#)
- [Three-Color Policer Configuration Overview on page 19](#)
- [Hierarchical Policer Configuration Overview on page 22](#)



## CHAPTER 3

# Policer Rate Limits and Actions

- [Policer Bandwidth and Burst-Size Limits on page 25](#)
- [Policer Color-Marking and Actions on page 26](#)
- [Single Token Bucket Algorithm on page 28](#)
- [Dual Token Bucket Algorithms on page 30](#)

## Policer Bandwidth and Burst-Size Limits

[Table 4 on page 25](#) lists each of the Junos OS policer types supported. For each policer type, the table summarizes the bandwidth limits and burst-size limits used to rate-limit traffic.

Table 4: Policer Bandwidth Limits and Burst-Size Limits

Policer Type	Bandwidth Limits	Burst-Size Limits
<b>Single-Rate Two-Color Policer</b>		
Defines a single rate limit: a bandwidth limit and an allowed burst size for conforming traffic.	<b>bandwidth-limit <i>bps</i>;</b> M, MX, and T Series routers: 8000..500000000000	<b>burst-size-limit <i>bytes</i>;</b> M, MX, and T Series routers: 1500..100000000000
For a single-rate two-color policer only, you can specify the bandwidth limit as a percentage value from 1 through 100 instead of as an absolute number of bits per second. The effective bandwidth limit is calculated as a percentage of either the physical interface media rate or the logical interface configured shaping rate.	<b>bandwidth-percent</b> 1..100 percent	
<b>Single-Rate Three-Color Policer</b>		
Defines a single rate limit: a bandwidth limit and an allowed burst size for conforming traffic.	<b>committed-information-rate <i>bps</i>;</b> M, MX, and T Series routers: 1500..100000000000	<b>committed-burst-size <i>bytes</i>;</b> M, MX, and T Series routers: 1500..100000000000
Also defines a second, larger burst size. This second burst size is used to differentiate between two categories of nonconforming traffic (yellow or red).		<b>excess-burst-size <i>bytes</i>;</b> M, MX, and T Series routers: 1500..100000000000

Table 4: Policer Bandwidth Limits and Burst-Size Limits (*continued*)

Policer Type	Bandwidth Limits	Burst-Size Limits
<b>Two-Rate Three-Color Policer</b>		
Defines a committed rate limit: a bandwidth limit and an allowed burst size for conforming traffic.	<b>committed-information-rate <i>bps</i></b> ; M, MX, and T Series routers:	<b>committed-burst-size <i>bytes</i></b> ; M, MX, and T Series routers:
Also defines a peak rate limit: a second, larger burst size and a second, higher bandwidth limit. These additional rate-limit components are used to differentiate between two categories of nonconforming traffic (yellow or red).	1500..1000000000000  <b>peak-information-rate <i>bps</i></b> ; M, MX, and T Series routers:	1500..1000000000000  <b>peak-burst-size <i>bytes</i></b> ; M, MX, and T Series routers:
	1500..1000000000000	1500..1000000000000
<b>Hierarchical Policer</b>		
Defines two policers, each with a bandwidth limit and an allowed burst size for conforming traffic. Different policing actions are applied based on whether the packets are classified for expedited forwarding (EF) or for a lower priority.	<b>bandwidth-limit <i>bps</i></b> ; M40e, M120, and M320 (with FFPC and SFPC) edge routers and T320, T640, and T1600 core routers with Enhanced Intelligent Queuing (IQE) PICs:	<b>burst-size-limit <i>bytes</i></b> ; M40e, M120, and M320 (with FFPC and SFPC) edge routers and T320, T640, and T1600 core routers with Enhanced Intelligent Queuing (IQE) PICs:
Rate-limits ingress Layer 2 traffic at a SONET physical or logical interface hosted on supported routing platforms only.	32000..500000000000	1500..2147450880

- Related Documentation**
- [Policer Color-Marking and Actions on page 26](#)
  - [Calculation of Policer Burst-Size Limit on page 33](#)

## Policer Color-Marking and Actions

Table 5 on page 26 lists each of the Junos OS policer types supported. For each policer type, the table summarizes the color-marking criteria used to categorize a traffic flow and, for each color, the actions taken on packets in that type of traffic flow.

Table 5: Implicit and Configurable Policer Actions Based on Color Marking

Policer Rate Limits and Color Marking	Implicit Action	Configurable Actions
<b>Single-Rate Two-Color Policer</b>		
<ul style="list-style-type: none"> <li>• Bandwidth limit</li> <li>• Burst size</li> </ul>		

Table 5: Implicit and Configurable Policer Actions Based on Color Marking (*continued*)

Policer Rate Limits and Color Marking	Implicit Action	Configurable Actions
<b>Green</b> Conforms to rate and burst size limits	Set PLP to <b>low</b>	–
<b>Red</b> Exceeds rate and burst size limits	–	<ul style="list-style-type: none"> <li>Discard the packet.</li> <li>Assign to a forwarding class.</li> <li>Set PLP to <b>low</b> or <b>high</b>. On some platforms, you can also set the PLP to <b>medium-low</b> or <b>medium-high</b>.</li> </ul>
<b>Single-Rate Three-Color Policer</b> <ul style="list-style-type: none"> <li>Committed information rate (CIR)</li> <li>Committed burst size (CBS)</li> <li>Excess burst size (EBS)</li> </ul>		
<b>Green</b> Conforms to the CIR and CBS	Set PLP to <b>low</b>	–
<b>Yellow</b> Exceeds the CIR and CBS but conforms to the EBS	Set PLP to <b>medium-high</b>	–
<b>Red</b> Exceeds the EBS	Set PLP to <b>high</b>	<ul style="list-style-type: none"> <li>Discard the packet.</li> </ul>
<b>Two-Rate Three-Color Policer</b> <ul style="list-style-type: none"> <li>Committed information rate (CIR)</li> <li>Committed burst size (CBS)</li> <li>Peak information rate (PIR)</li> <li>Peak burst size (PBS)</li> </ul>		
<b>Green</b> Conforms to the CIR and CBS	Set PLP to <b>low</b>	–
<b>Yellow</b> Exceeds the CIR and CBS, but conforms to the PIR	Set PLP to <b>medium-high</b>	–
<b>Red</b> Exceeds the PIR and PBS	Set PLP to <b>high</b>	<ul style="list-style-type: none"> <li>Discard the packet.</li> </ul>
<b>Hierarchical Policer</b>		
<b>Aggregate policer</b> <ul style="list-style-type: none"> <li>Bandwidth limit</li> <li>Burst size</li> </ul>		

Table 5: Implicit and Configurable Policer Actions Based on Color Marking (*continued*)

Policer Rate Limits and Color Marking	Implicit Action	Configurable Actions
<b>Green</b> Conforms to rate limits	Set PLP to <b>low</b>	–
<b>Red</b> Exceeds rate limits	–	<ul style="list-style-type: none"> <li>Discard the packet.</li> <li>Assign to a forwarding class.</li> <li>Set PLP to <b>low</b> or <b>high</b>. On some platforms, you can also set the PLP to <b>medium-low</b> or <b>medium-high</b>.</li> </ul>
<b>Premium policer</b>		
<ul style="list-style-type: none"> <li>Bandwidth limit</li> <li>Burst size</li> </ul>		
<b>Green</b> Conforms to rate limits	Set PLP to <b>low</b>	–
<b>Red</b> Exceeds rate limits	–	<ul style="list-style-type: none"> <li>Discard the packet.</li> </ul>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Policer Bandwidth and Burst-Size Limits on page 25</a></li> <li><a href="#">Calculation of Policer Burst-Size Limit on page 33</a></li> </ul>	

## Single Token Bucket Algorithm

This topic covers the following information:

- [Token Bucket Concepts on page 28](#)
- [Single Token Bucket Algorithm on page 29](#)
- [Conformance Measurement for Two-Color Marking on page 29](#)

### Token Bucket Concepts

When you apply traffic policing to the input or output traffic at an interface, the rate limits and actions specified in the policer configuration are used to enforce a limit on the average throughput rate at the interface while also allowing bursts of traffic up to a maximum number of bytes based on the overall traffic load. Junos OS policers measure traffic-flow conformance to a policing rate limit by using a *token bucket algorithm*:

- The *bucket* represents a rate-limiting function of the policer on the interface input or output traffic.
- Each *token* in the bucket represents a “credit” for some number of *bits*, and tokens in the bucket are “cashed in” for the ability to receive or transmit traffic that conforms to a rate limit configured for the policer.

- The *token arrival rate* is the fixed *bits-per-second* rate at which tokens are added to the token bucket, but only up to the specified depth of the bucket.
- The *token bucket depth* defines the capacity of the bucket in *bytes*.

An algorithm based on a single token bucket allows burst of traffic for short periods, whereas an algorithm based dual token buckets allows more sustained bursts of traffic.

## Single Token Bucket Algorithm

A single-rate two-color policer limits traffic throughput at an interface based on how the traffic conforms to rate-limit values specified in the policer configuration. Similarly, a hierarchical policer limits traffic throughput at an interface based on how aggregate and premium traffic subflows conform to aggregate and premium rate-limit values specified in the policer configuration. For both two-color policer types, packets in a conforming traffic flow are categorized as *green*, and packets in a non-conforming traffic flow are categorized as *red*.

The single token bucket algorithm measures traffic-flow conformance to a two-color policer rate limit as follows:

- The token arrival rate represents the single *bandwidth limit* configured for the policer. You can specify the bandwidth limit as an absolute number of bits per second by including the **bandwidth-limit *bps*** statement. Alternatively, for single-rate two-color policers only, you can use the **bandwidth-percent *percentage*** statement to specify the bandwidth limit as a percentage of either the physical interface port speed or the configured logical interface shaping rate.
- The token bucket depth represents the single *burst size* configured for the policer. You specify the burst size by including the **burst-size-limit *bytes*** statement.
- If the bucket is filled to capacity, arriving tokens “overflow” the bucket and are lost.

When the bucket contains insufficient tokens for receiving or transmitting the traffic at the interface, packets might be dropped or else re-marked with a lower forwarding class, a higher packet loss priority (PLP) level, or both.

## Conformance Measurement for Two-Color Marking

In two-color-marking policing, a traffic flow whose average arrival or departure rate does not exceed the token arrival rate (bandwidth limit) is considered *conforming traffic*. Packets in a conforming traffic flow (categorized as green traffic) are implicitly marked with a packet loss priority (PLP) level of **low** and then passed through the interface.

For a traffic flow whose average arrival or departure rate exceeds the token arrival rate, conformance to a two-color policer rate limit depends on the tokens in the bucket. If sufficient tokens remain in the bucket, the flow is considered conforming traffic. If the bucket does not contain sufficient tokens, the flow is considered *non-conforming traffic*. Packets in a non-conforming traffic flow (categorized as red traffic) are handled according to policing actions. Depending on the configuration of the two-color policer, packets might be implicitly discarded; or the packets might be re-marked with a specified forwarding class, a specified PLP, or both, and then passed through the interface.



**NOTE:** The number of tokens remaining in the bucket at any given time is a function of the token bucket depth and the overall traffic load.

The token bucket is initially filled to capacity, and so the policer allows an initial traffic burst (back-to-back traffic at average rates that exceed the token arrival rate) up to the size of the token bucket depth.

During periods of relatively low traffic (traffic that arrives at or departs from the interface at average rates below the token arrival rate), unused tokens accumulate in the bucket, but only up to the configured token bucket depth.

#### Related Documentation

- [Two-Color Policer Configuration Overview on page 15](#)
- [Hierarchical Policer Configuration Overview on page 22](#)
- [Policer Color-Marking and Actions on page 26](#)
- [bandwidth-limit \(Hierarchical Policer\) on page 167](#)
- [bandwidth-limit \(Policer\) on page 168](#)
- [bandwidth-percent on page 170](#)
- [burst-size-limit \(Hierarchical Policer\) on page 172](#)
- [burst-size-limit \(Policer\) on page 173](#)

## Dual Token Bucket Algorithms

---

This topic covers the following information:

- [Token Bucket Concepts on page 30](#)
- [Guaranteed Bandwidth for Three-Color Marking on page 31](#)
- [Nonconformance Measurement for Single-Rate Three-Color Marking on page 31](#)
- [Nonconformance Measurement for Two-Rate Three-Color Marking on page 31](#)

### Token Bucket Concepts

When you apply traffic policing to the input or output traffic at an interface, the rate limits and actions specified in the policer configuration are used to enforce a limit on the average throughput rate at the interface while also allowing bursts of traffic up to a maximum number of bytes based on the overall traffic load. Junos OS policers measure traffic-flow conformance to a policing rate limit by using a *token bucket algorithm*:

- The *bucket* represents a rate-limiting function of the policer on the interface input or output traffic.
- Each *token* in the bucket represents a “credit” for some number of *bits*, and tokens in the bucket are “cashed in” for the ability to receive or transmit traffic that conforms to a rate limit configured for the policer.

- The *token arrival rate* is the fixed *bits-per-second* rate at which tokens are added to the token bucket, but only up to the specified depth of the bucket.
- The *token bucket depth* defines the capacity of the bucket in *bytes*.

An algorithm based on a single token bucket allows burst of traffic for short periods, whereas an algorithm based dual token buckets allows more sustained bursts of traffic.

## Guaranteed Bandwidth for Three-Color Marking

A committed information rate (CIR) defines the guaranteed bandwidth for traffic arriving at or departing from the interface under normal line conditions. A flow of traffic at an average rate that conforms to the CIR is categorized green, and packets in a green flow are implicitly marked with **low** packet loss priority (PLP) and then passed through the interface. During periods of relatively low traffic (traffic that arrives at or departs from the interface at average rates below the CIR), any unused bandwidth capacity accumulates in the first token bucket, but only up to a configured number of bytes. If any unused bandwidth capacity overflows the first bucket, the excess accumulates in a second token bucket.

The committed burst size (CBS) defines the maximum number of bytes for which unused amounts of the guaranteed bandwidth can be accumulated in the first token bucket. A burst of traffic at an average rate that exceeds the CIR is also categorized as green provided that sufficient unused bandwidth capacity is available in the first token bucket.

## Nonconformance Measurement for Single-Rate Three-Color Marking

Single-rate three-color policer configurations specify a second burst size—the excess burst size (EBS)—that defines the maximum number of bytes for which the second token bucket can accumulate unused bandwidth that overflows from the first bucket.

A traffic flow is categorized yellow if its average rate exceeds the CIR and the available bandwidth capacity accumulated in the first bucket if sufficient unused bandwidth capacity is available in the second token bucket. Packets in a yellow flow are implicitly marked with **medium-high** PLP and then passed through the interface.

A traffic flow is categorized red its average rate exceeds the CIR and the available bandwidth capacity accumulated in the second bucket. Packets in a red flow are implicitly marked with **high** PLP and then either passed through the interface or optionally discarded.

## Nonconformance Measurement for Two-Rate Three-Color Marking

Two-rate three-color policer configurations include a second rate limit—the peak-information-rate (PIR)—that you set to the expected average data rate for traffic arriving at or departing from the interface under peak conditions.

Two-rate three-color policer configurations also include a second burst size—the peak burst size (PBS)—that defines the maximum number of bytes for which the second token bucket can accumulate unused peak bandwidth capacity. During periods of relatively little peak traffic (traffic that arrives at or departs from the interface at average rates that exceed the PIR), any unused peak bandwidth capacity accumulates in the second token bucket, but only up to the maximum number of bytes specified by the PBS.

A traffic flow is categorized yellow if it exceeds the CIR and the available committed bandwidth capacity accumulated in the first token bucket but conforms to the PIR. Packets in a yellow flow are implicitly marked with **medium-high** PLP and then passed through the interface.

A traffic flow is categorized red if it exceeds the PIR and the available peak bandwidth capacity accumulated in the second token bucket. Packets in a red flow are implicitly marked with **high** PLP and then either passed through the interface or optionally discarded.

**Related  
Documentation**

- [Three-Color Policer Configuration Overview on page 19](#)
- [Policer Color-Marking and Actions on page 26](#)
- [committed-burst-size on page 177](#)
- [committed-information-rate on page 179](#)
- [excess-burst-size on page 181](#)
- [peak-burst-size on page 195](#)
- [peak-information-rate on page 197](#)



# Best Practices for Policer Configuration

- [Calculation of Policer Burst-Size Limit on page 33](#)

## Calculation of Policer Burst-Size Limit

---

This topic covers the following information:

- [Guidelines for Choosing a Burst-Size Limit on page 33](#)
- [Burst-Size Limit Based on the Line Rate of the Interface on page 34](#)
- [Burst-Size Limit Based on the MTU of Traffic on the Interface on page 35](#)

## Guidelines for Choosing a Burst-Size Limit

A policer burst-size limit controls the number of bytes of traffic that can pass through a policed interface unrestricted when a burst of traffic pushes the average transmit or receive rate above the configured bandwidth limit. The actual number of bytes of bursty traffic allowed to pass through a policed interface can vary from zero to the configured burst-size limit, depending on the overall traffic load.

Junos OS implements two-color policers using a *single token bucket* algorithm and implements three-color policers using a *dual token bucket* algorithm. In both of these models, the bits-per-second rate configured as a bandwidth limit is conceptualized the *token arrival rate* for a token bucket, and the number of bytes configured as a policer burst-size limit is conceptualized as the *bucket depth* for the corresponding bucket. The number of tokens remaining in the bucket at any given time is a function of the token bucket depth and the overall traffic load. The token bucket is initially filled to capacity, and so the policer allows an initial traffic burst (back-to-back traffic at average rates that exceed the token arrival rate) up to the size of the token bucket depth. During periods of relatively low traffic (traffic that arrives at or departs from the interface at average rates below the token arrival rate), unused tokens accumulate in the bucket, but only up to the configured token bucket depth.



**NOTE:** If you set the burst-size limit too low, too many packets will be subjected to rate-limiting. If you set the burst-size limit too high, too few packets will be rate-limited.

The following general guidelines apply to choosing a policer burst-size limit:

- A burst-size limit should not be set lower than 10 times the maximum transmission unit (MTU) of the traffic on the interface to be policed.
- The amount of time to allow a burst of traffic at the full line rate of a policed interface should not be lower than 5 milliseconds.
- The minimum and maximum values you can specify for a policer burst-size limit depends on the policer type (two-color, three-color, or hierarchical). For more information, see [“Policer Bandwidth and Burst-Size Limits” on page 25](#).



**BEST PRACTICE:** The preferred method for choosing a burst-size limit is based on the line rate of the interface on which you apply the policer and the amount of time you want to allow a burst of traffic at the full line rate.

In cases where the line rate of the target interface is unknown, you can choose a burst-size limit based on the MTU of the traffic on the target interface.

### Burst-Size Limit Based on the Line Rate of the Interface

To calculate the burst-size limit based on the line rate of the interface:

- Multiply the interface line rate (in bits per second) by the amount of time (in seconds) to allow a burst of traffic at the full line rate, and then divide by 8 bits to convert from bits to bytes.

$$\text{burst-size limit in bytes} = \frac{\text{interface media rate} \times \text{allowable time for bursty traffic}}{8 \text{ bits}}$$

We recommend that you use a value of 5 ms (0.005 seconds) as the starting point for the allowable amount of time for a burst of traffic.

[Table 6 on page 34](#) shows example calculations of burst-size limits for various physical interface types.

**Table 6: Example Calculations of Policer Burst-Size Limit**

Target Interface		Allowed Burst Period	Calculation of Policer Burst-Size Limit Based on a Target Interface Line Rate and an Allowed Burst Period
Type	Line Rate		
DS3	45 Mbps	5 ms	45,000,000 bps x 0.005 seconds x 1 byte / 8 bits = 28,125 bytes
Fast Ethernet	100 Mbps	5 ms	100,000,000 bps x 0.005 seconds x 1 byte / 8 bits = 62,500 bytes
Gigabit Ethernet	1000 Mbps	5 ms	1,000,000,000 bps x 0.005 seconds x 1 byte / 8 bits = 625,000 bytes

Table 6: Example Calculations of Policer Burst-Size Limit (*continued*)

Target Interface		Allowed Burst Period	Calculation of Policer Burst-Size Limit Based on a Target Interface Line Rate and an Allowed Burst Period
Type	Line Rate		
10-Gigabit Ethernet	10,000Mbps	5 ms	10,000,000,000 bpsm x 0.005 seconds x 1 byte / 8 bits = 6,250,000 bytes

Burst-Size Limit Based on the MTU of Traffic on the Interface

To calculate the burst-size limit based on the MTU of traffic on the interface:

- Multiply the interface traffic MTU by a factor of 10 or greater. At the minimum, the burst size should be at least one interface MTU.

burst-size limit in bytes = interface traffic MTU x 10

For example, suppose that you are configuring a policer for an interface that carries traffic with an MTU of 4700 bytes. The recommended burst-size limit is 47,000 bytes or greater.

Related Documentation

- [Policer Bandwidth and Burst-Size Limits on page 25](#)
- [Policer Color-Marking and Actions on page 26](#)
- [Single Token Bucket Algorithm on page 28](#)
- [Dual Token Bucket Algorithms on page 30](#)



## PART 2

# Configuration

- [Single-Rate Two-Color Policers on page 39](#)
- [Three-Color Policers on page 109](#)
- [Logical and Physical Interface Policers on page 125](#)
- [Layer 2 Policers on page 147](#)
- [Policer Configuration Statements on page 165](#)



## CHAPTER 5

# Single-Rate Two-Color Policers

- [Basic Single-Rate Two-Color Policers on page 39](#)
- [Bandwidth Policers on page 55](#)
- [Filter-Specific Counters and Policers on page 64](#)
- [Prefix-Specific Counting and Policing Actions on page 71](#)
- [Multifield Classification on page 87](#)
- [Policer Overhead to Account for Rate Shaping in the Traffic Manager on page 99](#)

## Basic Single-Rate Two-Color Policers

---

- [Single-Rate Two-Color Policer Overview on page 39](#)
- [Example: Configuring a Single-Rate Two-Color Policer on page 40](#)
- [Example: Configuring Interface and Firewall Filter Policers at the Same Interface on page 46](#)

## Single-Rate Two-Color Policer Overview

Single-rate two color policing enforces a configured rate of traffic flow for a particular service level by applying implicit or configured actions to traffic that does not conform to the limits. When you apply a single-rate two-color policer to the input or output traffic at an interface, the policer meters the traffic flow to the rate limit defined by the following components:

- **Bandwidth limit**—The average number of bits per second permitted for packets received or transmitted at the interface. You can specify the bandwidth limit as an absolute number of bits per second or as a percentage value from 1 through 100. If a percentage value is specified, the effective bandwidth limit is calculated as a percentage of either the physical interface media rate or the logical interface configured shaping rate.
- **Burst-size limit**—The maximum size permitted for bursts of data.

For a traffic flow that conforms to the configured limits (categorized as green traffic), packets are implicitly marked with a packet loss priority (PLP) level of **low** and are allowed to pass through the interface unrestricted.

For a traffic flow that exceeds the configured limits (categorized as red traffic), packets are handled according to the traffic-policing actions configured for the policer. The action

might be to discard the packet, or the action might be to re-mark the packet with a specified forwarding class, a specified PLP, or both, and then transmit the packet.

To rate-limit Layer 3 traffic, you can apply a two-color policer in the following ways:

- Directly to a logical interface, at a specific protocol level.
- As the action of a standard stateless firewall filter that is applied to a logical interface, at a specific protocol level.

To rate-limit Layer 2 traffic, you can apply a two-color policer as a *logical interface policer* only. You cannot apply a two-color policer to Layer 2 traffic through a firewall filter.

## Example: Configuring a Single-Rate Two-Color Policer

This example shows how to configure a single-rate two-color policer that you apply to a logical interface as a firewall filter action.

- [Requirements on page 40](#)
- [Overview on page 40](#)
- [Configuration on page 40](#)
- [Verification on page 45](#)

---

### Requirements

No special configuration beyond device initialization is required before configuring this example.

To set the maximum burst size of the policer, you should know the line rate of the interface (preferred) or else the maximum transmission unit (MTU) of the traffic on the target interface.

---

### Overview

In this example, you configure a single-rate two-color policer and then use an IPv4 firewall filter to apply the policer to all traffic except for BGP messages. You apply the firewall filter to the input and output of the same logical interface.

### Topology

Assume that you know the traffic flow needs to be rate-limited to an average bandwidth of 9 Mbps. Also assume that you do not know the line rate of the target interface, but you do know that the MTU of traffic on the interface is 4700 bytes. As described in [“Calculation of Policer Burst-Size Limit” on page 33](#), you can estimate a starting value of 10 times the MTU.

---

### Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see [“Using the CLI Editor in Configuration Mode” on page 215](#).



To configure this example, perform the following tasks:

- [Configuring the Logical Interface and Monitoring the Traffic Rate Without Policing on page 41](#)
- [Configuring the Basic Single-Rate Two-Color Policer on page 42](#)
- [Referencing the Policer from a Term in a Stateless Firewall Filter on page 43](#)
- [Applying the Firewall Filter to the Input and Output of the Logical Interface on page 44](#)

#### CLI Quick Configuration

To quickly configure this example, copy the following configuration commands into a text file, remove any line breaks, and then paste the commands into the CLI at the **[edit]** hierarchy level.

```
set interfaces so-1/3/0 unit 0 family inet address 10.39.1.1/16
set firewall policer p-9m-47k-discard if-exceeding bandwidth-limit 9m
set firewall policer p-9m-47k-discard if-exceeding burst-size-limit 47k
set firewall policer p-9m-47k-discard then discard
set firewall family inet filter rate-limit-in term t1 from protocol tcp
set firewall family inet filter rate-limit-in term t1 from port bgp
set firewall family inet filter rate-limit-in term t1 then accept
set firewall family inet filter rate-limit-in term t2 then policer p-9m-47k-discard
set firewall family inet filter rate-limit-in term t2 then accept
set interfaces so-1/3/0 unit 0 family inet filter input rate-limit-in
set interfaces so-1/3/0 unit 0 family inet filter output rate-limit-in
```

#### *Configuring the Logical Interface and Monitoring the Traffic Rate Without Policing*

#### Step-by-Step Procedure

To configure the logical interface and monitor the traffic rate:

1. Configure IPv4 on the logical interface.

```
[edit]
user@host# edit interfaces so-1/3/0 unit 0 family inet address 10.39.1.1/16
```

2. Commit the configuration.

```
[edit]
user@host# commit
```

3. Monitor the traffic flow at the interface (press 'q' to terminate monitoring).

```
[edit]
user@host# run monitor interface so-1/3/0.0
```

The traffic statistics report the input and output rates before applying interface rate limiting.

#### Results

Confirm the configuration of the logical interface by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show interfaces
so-3/3/0 {
  unit 0 {
    family inet {
      address 10.39.1.1/16
```

```

    }
  }
}

```

### Configuring the Basic Single-Rate Two-Color Policer

#### Step-by-Step Procedure

To configure the basic single-rate two-color policer:

1. Enable configuration of a single-rate two-color policer.

[edit]

user@host# edit firewall **policer** p-9m-47k-discard



#### NOTE:

This example illustrates a basic two-color policer, which does not require any of the following statements:

- **filter-specific**—You can include this statement so that, when this policer is applied as a firewall filter policer, a single instance of the policer is used by all terms within the same firewall filter.
- **logical-bandwidth-policer**—Include this statement only if the policer bandwidth limit is specified as a percentage value (using the **bandwidth-percent percent** statement) and you want the bandwidth limit to be based on the configured shaping rate for the target logical interface.
- **logical-interface-policer**—Include this statement only if you apply the policer directly to a physical or logical interface to rate-limit traffic for any configured protocol family based on the physical interface media rate.
- **physical-interface-policer**—Include this statement if you apply the policer to packets filtered by a standard stateless firewall filter term and you want the policer to meter the aggregate traffic (all protocol families and logical interfaces configured on the underlying physical interface).

2. Configure the policer to rate-limit to an average bandwidth of 9 Mbps and a burst size of 47 KB.

[edit firewall policer p-9m-47k-discard]

user@host# set if-exceeding **bandwidth-limit** 9m

user@host# set if-exceeding **burst-size-limit** 47k

For information about configuring the burst size, see [“Calculation of Policer Burst-Size Limit” on page 33](#).

When the traffic flow conforms to these limits, the flow is categorized as green. For a single-rate two-color policer, packets in a green flow are implicitly set to a **low** packet loss priority (PLP) level.

3. Configure the policer to discard packets in a red traffic flow.

```
[edit firewall policer p-9m-47k-discard]
user@host# set then discard
```

Instead of discarding the traffic that exceeds the traffic limits, you can set the PLP level, the forwarding class assignment, or both.

**Results** Confirm the configuration of the policer by entering the **show firewall** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show firewall
policer p-9m-47k-discard {
  if-exceeding {
    bandwidth-limit 9m;
    burst-size-limit 47k;
  }
  then discard;
}
```

#### *Referencing the Policer from a Term in a Stateless Firewall Filter*

**Step-by-Step Procedure** To reference the policer from a term in a stateless firewall filter:

1. Enable configuration of the stateless firewall filter.

```
[edit]
user@host# edit firewall family inet filter rate-limit-in
```

2. Configure the first term to accept all BGP traffic.

BGP messages are transported over TCP port 179.

```
[edit firewall family inet filter rate-limit-in]
user@host# set term t1 from protocol tcp
user@host# set term t1 from port bgp
user@host# set term t1 then accept
```

The BGP traffic is not rate-limited to avoid having the BGP session time out because the packet is discarded by the policer.

3. Configure the second term to rate-limit all other traffic using the policer.

```
[edit firewall family inet filter rate-limit-in]
user@host# set term t2 then policer p-9m-47k-discard
user@host# set term t2 then accept
```

**Results** Confirm the configuration of the firewall filter by entering the **show firewall** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show firewall
family inet {
  filter rate-limit-in {
```

```
term t1 {
  from {
    protocol tcp;
    port bgp;
  }
  then accept;
}
term t2 {
  then {
    policer p-9m-47k-discard;
    accept;
  }
}
}
}
policer p-9m-47k-discard {
  if-exceeding {
    bandwidth-limit 9m;
    burst-size-limit 47k;
  }
  then discard;
}
```

### *Applying the Firewall Filter to the Input and Output of the Logical Interface*

#### **Step-by-Step Procedure**

To apply the stateless firewall filter to the input and output of the logical interface:

1. Enable configuration of IPv4 on the logical interface.

```
[edit]
user@host# edit interfaces so-1/3/0 unit 0 family inet
```

2. Apply the stateless firewall filter.

```
[edit interfaces so-1/3/0 unit 0 family inet]
user@host# set filter input rate-limit-in
user@host# set filter output rate-limit-in
```

#### **Results**

Confirm the configuration of the logical interface by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show interfaces
so-3/3/0 {
  unit 0 {
    family inet {
      filter {
        input rate-limit-in;
        output rate-limit-in;
      }
      address 10.39.1.1/16;
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

Confirm that the configuration is working properly.

- [Monitoring and Adjusting Policing of the Logical Interface on page 45](#)
- [Displaying the Number of Packets Processed by the Policer at the Logical Interface on page 45](#)

### *Monitoring and Adjusting Policing of the Logical Interface*

**Purpose** Ensure that the traffic limits configured in the policer are throttling the input and output rate as you intended.

**Action** To ensure that the configured traffic limits are throttling the traffic rate as intended:

1. Monitor the traffic flow at the interface (press 'q' to terminate monitoring).

[edit]

```
user@host# run monitor interface so-1/3/0.0
```

The traffic statistics report the input and output rate after applying interface rate limiting.

2. Adjust the burst-size limit if necessary.

If the policer appears to be throttling the input and output rate more than you intended, increase the burst size (possibly doubling it) and then check again.

### *Displaying the Number of Packets Processed by the Policer at the Logical Interface*

**Purpose** Verify the traffic flow through the logical interface and that the policer is evaluated when packets are received on the logical interface.

**Action** Use the **show firewall** operational mode command for the filter you applied to the logical interface:

[edit]

```
user@host# run show firewall filter rate-limit-in
```

```
Filter: rate-limit-in
```

```
Policers:
```

Name	Packets
p-9m-47k-discard-t2	32863

The command output displays the name of policer (**p-9m-47k-discard**), the name of the filter term (**t2**) under which the policer action is specified, and the number of packets that matched the filter term. This is only the number of out-of-specification (out-of-spec) packet counts, not all packets policed by the policer.

## Example: Configuring Interface and Firewall Filter Policers at the Same Interface

This example shows how to configure three single-rate two-color policers and apply the policers to the IPv4 input traffic at the same single-tag virtual LAN (VLAN) logical interface.

- [Requirements on page 46](#)
- [Overview on page 46](#)
- [Configuration on page 47](#)
- [Verification on page 53](#)

---

### Requirements

No special configuration beyond device initialization is required before configuring this example.

---

### Overview

In this example, you configure three single-rate two-color policers and apply the policers to the IPv4 input traffic at the same single-tag VLAN logical interface. Two policers are applied to the interface through a firewall filter, and one policer is applied directly to the interface.

You configure one policer, named **p-all-1m-5k-discard**, to rate-limit traffic to 1 Mbps with a burst size of 5000 bytes. You apply this policer directly to IPv4 input traffic at the logical interface. When you apply a policer directly to protocol-specific traffic at a logical interface, the policer is said to be applied as an *interface policer*.

You configure the other two policers to allow burst sizes of 500 KB, and you apply these policers to IPv4 input traffic at the logical interface by using an IPv4 standard stateless firewall filter. When you apply a policer to protocol-specific traffic at a logical interface through a firewall filter action, the policer is said to be applied as a *firewall-filter policer*.

- You configure the policer named **p-icmp-500k-500k-discard** to rate-limit traffic to 500 Kbps with a burst size of 500 K bytes by discarding packets that do not conform to these limits. You configure one of the firewall filter terms to apply this policer to Internet Control Message Protocol (ICMP) packets.
- You configure the policer named **p-ftp-10p-500k-discard** to rate-limit traffic to a 10 percent bandwidth with a burst size of 500 KB by discarding packets that do not conform to these limits. You configure another firewall-filter term to apply this policer to File Transfer Protocol (FTP) packets.

A policer that you configure with a bandwidth limit expressed as a percentage value (rather than as an absolute bandwidth value) is called a *bandwidth policer*. Only single-rate two-color policers can be configured with a percentage bandwidth specification. By default, a bandwidth policer rate-limits traffic to the specified percentage of the line rate of the physical interface underlying the target logical interface.

### Topology

You configure the target logical interface as a single-tag VLAN logical interface on a Fast Ethernet interface operating at 100 Mbps. This means that the policer you configure with the 10-percent bandwidth-limit (the policer that you apply to FTP packets) rate-limits the FTP traffic on this interface to 10 Mbps.



**NOTE:** In this example, you do not configure the bandwidth policer as a *logical-bandwidth policer*. Therefore, the percentage is based on the physical media rate rather than on the configured shaping rate of the logical interface.

The firewall filter that you configure to reference two of the policers must be configured as an *interface-specific filter*. Because the policer that is used to rate-limit FTP packets specifies the bandwidth limit as a percentage value, the firewall filter that references this policer must be configured as an interface-specific filter. Thus, if this firewall filter were to be applied to multiple interfaces instead of just the Fast Ethernet interface in this example, unique policers and counters would be created for each interface to which the filter is applied.

### Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see [“Using the CLI Editor in Configuration Mode” on page 215](#).

To configure this example, perform the following tasks:

- [Configuring the Single-Tag VLAN Logical Interface on page 48](#)
- [Configuring the Three Policers on page 49](#)
- [Configuring the IPv4 Firewall Filter on page 51](#)
- [Applying the Interface Policer and Firewall Filter Policers to the Logical Interface on page 52](#)

#### CLI Quick Configuration

To quickly configure this example, copy the following configuration commands into a text file, remove any line breaks, and then paste the commands into the CLI at the **[edit]** hierarchy level.

```
set interfaces fe-0/1/1 vlan-tagging
set interfaces fe-0/1/1 unit 0 vlan-id 100
set interfaces fe-0/1/1 unit 0 family inet address 10.20.15.1/24
set interfaces fe-0/1/1 unit 1 vlan-id 101
set interfaces fe-0/1/1 unit 1 family inet address 10.20.240.1/24
set firewall policer p-all-1m-5k-discard if-exceeding bandwidth-limit 1m
set firewall policer p-all-1m-5k-discard if-exceeding burst-size-limit 5k
set firewall policer p-all-1m-5k-discard then discard
set firewall policer p-ftp-10p-500k-discard if-exceeding bandwidth-percent 10
set firewall policer p-ftp-10p-500k-discard if-exceeding burst-size-limit 500k
set firewall policer p-ftp-10p-500k-discard then discard
set firewall policer p-icmp-500k-500k-discard if-exceeding bandwidth-limit 500k
set firewall policer p-icmp-500k-500k-discard if-exceeding burst-size-limit 500k
set firewall policer p-icmp-500k-500k-discard then discard
```

```

set firewall family inet filter filter-ipv4-with-limits interface-specific
set firewall family inet filter filter-ipv4-with-limits term t-ftp from protocol tcp
set firewall family inet filter filter-ipv4-with-limits term t-ftp from port ftp
set firewall family inet filter filter-ipv4-with-limits term t-ftp from port ftp-data
set firewall family inet filter filter-ipv4-with-limits term t-ftp then policer
  p-ftp-10p-500k-discard
set firewall family inet filter filter-ipv4-with-limits term t-icmp from protocol icmp
set firewall family inet filter filter-ipv4-with-limits term t-icmp then policer
  p-icmp-500k-500k-discard
set firewall family inet filter filter-ipv4-with-limits term catch-all then accept
set interfaces fe-0/1/1 unit 1 family inet filter input filter-ipv4-with-limits
set interfaces fe-0/1/1 unit 1 family inet policer input p-all-1m-5k-discard

```

### *Configuring the Single-Tag VLAN Logical Interface*

#### **Step-by-Step Procedure**

To configure the single-tag VLAN logical interface:

1. Enable configuration of the Fast Ethernet interface.

```

[edit]
user@host# edit interfaces fe-0/1/1

```

2. Enable single-tag VLAN framing.

```

[edit interfaces fe-0/1/1]
user@host# set vlan-tagging

```

3. Bind VLAN IDs to the logical interfaces.

```

[edit interfaces fe-0/1/1]
user@host# set unit 0 vlan-id 100
user@host# set unit 1 vlan-id 101

```

4. Configure IPv4 on the single-tag VLAN logical interfaces.

```

[edit interfaces fe-0/1/1]
user@host# set unit 0 family inet address 10.20.15.1/24
user@host# set unit 1 family inet address 10.20.240.1/24

```

**Results** Confirm the configuration of the VLAN by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```

[edit]
user@host# show interfaces
fe-0/1/1 {
  vlan-tagging;
  unit 0 {
    vlan-id 100;
    family inet {
      address 10.20.15.1/24;
    }
  }
  unit 1 {
    vlan-id 101;
    family inet {
      address 10.20.240.1/24;
    }
  }
}

```



```

    }
  }
}

```

### Configuring the Three Policers

#### Step-by-Step Procedure

To configure the three policers:

1. Enable configuration of a two-color policer that discards packets that do not conform to a bandwidth of 1 Mbps and a burst size of 5000 bytes.



**NOTE:** You apply this policer directly to all IPv4 input traffic at the single-tag VLAN logical interface, so the packets will not be filtered before being subjected to rate limiting.

```

[edit]
user@host# edit firewall policer p-all-1m-5k-discard

```

2. Configure the first policer.

```

[edit firewall policer p-all-1m-5k-discard]
user@host# set if-exceeding bandwidth-limit 1m
user@host# set if-exceeding burst-size-limit 5k
user@host# set then discard

```

3. Enable configuration of a two-color policer that discards packets that do not conform to a bandwidth specified as "10 percent" and a burst size of 500,000 bytes.

You apply this policer only to the FTP traffic at the single-tag VLAN logical interface.

You apply this policer as the action of an IPv4 firewall filter term that matches FTP packets from TCP.

```

[edit firewall policer p-all-1m-5k-discard]
user@host# up

```

```

[edit]
user@host# edit firewall policer p-ftp-10p-500k-discard

```

4. Configure policing limits and actions.

```

[edit firewall policer p-ftp-10p-500k-discard]
user@host# set if-exceeding bandwidth-percent 10
user@host# set if-exceeding burst-size-limit 500k
user@host# set then discard

```

Because the bandwidth limit is specified as a percentage, the firewall filter that references this policer must be configured as an interface-specific filter.



**NOTE:** If you wanted this policer to rate-limit to 10 percent of the logical interface configured shaping rate (rather than to 10 percent of the physical interface media rate), you would need to include the `logical-bandwidth-policer` statement at the [edit firewall policer p-all-1m-5k-discard] hierarchy level. This type of policer is called a *logical-bandwidth policer*.

5. Enable configuration of the IPv4 firewall filter policer for ICMP packets.

```
[edit firewall policer p-ftp-10p-500k-discard]
user@host# up
```

```
[edit]
user@host# edit firewall policer p-icmp-500k-500k-discard
```

6. Configure policing limits and actions.

```
[edit firewall policer p-icmp-500k-500k-discard]
user@host# set if-exceeding bandwidth-limit 500k
user@host# set if-exceeding burst-size-limit 500k
user@host# set then discard
```

**Results** Confirm the configuration of the policers by entering the `show firewall` configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show firewall
policer p-all-1m-5k-discard {
  if-exceeding {
    bandwidth-limit 1m;
    burst-size-limit 5k;
  }
  then discard;
}
policer p-ftp-10p-500k-discard {
  if-exceeding {
    bandwidth-percent 10;
    burst-size-limit 500k;
  }
  then discard;
}
policer p-icmp-500k-500k-discard {
  if-exceeding {
    bandwidth-limit 500k;
    burst-size-limit 500k;
  }
  then discard;
}
```

*Configuring the IPv4 Firewall Filter***Step-by-Step  
Procedure**

To configure the IPv4 firewall filter:

1. Enable configuration of the IPv4 firewall filter.

```
[edit]
user@host# edit firewall family inet filter filter-ipv4-with-limits
```

2. Configure the firewall filter as interface-specific.

```
[edit firewall family inet filter filter-ipv4-with-limits]
user@host# set interface-specific
```

The firewall filter must be interface-specific because one of the policers referenced is configured with a bandwidth limit expressed as a percentage value.

3. Enable configuration of a filter term to rate-limit FTP packets.

```
[edit firewall family inet filter filter-ipv4-with-limits]
user@host# edit term t-ftp
```

```
[edit firewall family inet filter filter-ipv4-with-limits term t-ftp]
user@host# set from protocol tcp
user@host# set from port [ ftp ftp-data ]
```

FTP messages are sent over TCP port 20 (**ftp**) and received over TCP port 21 (**ftp-data**).

4. Configure the filter term to match FTP packets.

```
[edit firewall family inet filter filter-ipv4-with-limits term t-ftp]
user@host# set then policer p-ftp-10p-500k-discard
```

5. Enable configuration of a filter term to rate-limit ICMP packets.

```
[edit firewall family inet filter filter-ipv4-with-limits term t-ftp]
user@host# up
```

```
[edit firewall family inet filter filter-ipv4-with-limits]
user@host# edit term t-icmp
```

6. Configure the filter term for ICMP packets

```
[edit firewall family inet filter filter-ipv4-with-limits term t-icmp]
user@host# set from protocol icmp
user@host# set then policer p-icmp-500k-500k-discard
```

7. Configure a filter term to accept all other packets without policing.

```
[edit firewall family inet filter filter-ipv4-with-limits term t-icmp]
user@host# up
```

```
[edit firewall family inet filter filter-ipv4-with-limits]
user@host# set term catch-all then accept
```

**Results** Confirm the configuration of the firewall filter by entering the **show firewall** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show firewall
family inet {
  filter filter-ipv4-with-limits {
    interface-specific;
    term t-ftp {
      from {
        protocol tcp;
        port [ ftp ftp-data ];
      }
      then policer p-ftp-10p-500k-discard;
    }
    term t-icmp {
      from {
        protocol icmp;
      }
      then policer p-icmp-500k-500k-discard;
    }
    term catch-all {
      then accept;
    }
  }
}
policer p-all-1m-5k-discard {
  if-exceeding {
    bandwidth-limit 1m;
    burst-size-limit 5k;
  }
  then discard;
}
policer p-ftp-10p-500k-discard {
  if-exceeding {
    bandwidth-percent 10;
    burst-size-limit 500k;
  }
  then discard;
}
policer p-icmp-500k-500k-discard {
  if-exceeding {
    bandwidth-limit 500k;
    burst-size-limit 500k;
  }
  then discard;
}
```

#### *Applying the Interface Policer and Firewall Filter Policers to the Logical Interface*

**Step-by-Step Procedure** To apply the three policers to the VLAN:

1. Enable configuration of IPv4 on the logical interface.

```
[edit]
```

```
user@host# edit interfaces fe-0/1/1 unit 1 family inet
```

2. Apply the firewall filter policers to the interface.

```
[edit interfaces fe-0/1/1 unit 1 family inet]
user@host# set filter input filter-ipv4-with-limits
```

3. Apply the interface policer to the interface.

```
[edit interfaces fe-0/1/1 unit 1 family inet]
user@host# set policer input p-all-1m-5k-discard
```

Input packets at **fe-0/1/1.0** are evaluated against the interface policer before they are evaluated against the firewall filter policers. For more information, see [“Order of Policer and Firewall Filter Operations” on page 10](#).

**Results** Confirm the configuration of the interface by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show interfaces
fe-0/1/1 {
  vlan-tagging;
  unit 0 {
    vlan-id 100;
    family inet {
      address 10.20.15.1/24;
    }
  }
  unit 1 {
    vlan-id 101;
    family inet {
      filter {
        input filter-ipv4-with-limits;
      }
      policer {
        input p-all-1m-5k-discard;
      }
      address 10.20.240.1/24;
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

Confirm that the configuration is working properly.

- [Displaying Policers Applied Directly to the Logical Interface on page 54](#)
- [Displaying Statistics for the Policer Applied Directly to the Logical Interface on page 54](#)
- [Displaying the Policers and Firewall Filters Applied to an Interface on page 54](#)
- [Displaying Statistics for the Firewall Filter Policers on page 55](#)

*Displaying Policers Applied Directly to the Logical Interface*

**Purpose** Verify that the interface policer is evaluated when packets are received on the logical interface.

**Action** Use the **show interfaces policers** operational mode command for logical interface **fe-0/1/1.1**. The command output section for the **Proto** column and **Input Policer** column shows that the policer **p-all-1m-5k-discard** is evaluated when packets are received on the logical interface.

```
user@host> show interfaces policers fe-0/1/1.1
Interface      Admin Link Proto Input Policer      Output Policer
fe-0/1/1.1     up      up      inet  p-all-1m-5k-discard-fe-0/1/1.1-inet-i
```

In this example, the interface policer is applied to logical interface traffic in the input direction only.

*Displaying Statistics for the Policer Applied Directly to the Logical Interface*

**Purpose** Verify the number of packets evaluated by the interface policer.

**Action** Use the **show policer** operational mode command and optionally specify the name of the policer. The command output displays the number of packets evaluated by each configured policer (or the specified policer), in each direction.

```
user@host> show policer p-all-1m-5k-discard-fe-0/1/1.1-inet-i
Policers:
Name                                     Packets
p-all-1m-5k-discard-fe-0/1/1.1-inet-i      5
```

*Displaying the Policers and Firewall Filters Applied to an Interface*

**Purpose** Verify that the firewall filter **filter-ipv4-with-limits** is applied to the IPv4 input traffic at logical interface **fe-0/1/1.1**.

**Action** Use the **show interfaces statistics** operational mode command for logical interface **fe-0/1/1.1**, and include the **detail** option. Under the **Protocol inet** section of the command output section, the **Input Filters** and **Policer** lines display the names of filter and policer applied to the logical interface in the input direction.

```
user@host> show interfaces statistics fe-0/1/1.1 detail
Logical interface fe-0/1/1.1 (Index 83) (SNMP ifIndex 545) (Generation 153)
Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.100 ] Encapsulation: ENET2
Traffic statistics:
  Input bytes : 0
  Output bytes : 46
  Input packets: 0
  Output packets: 1
Local statistics:
  Input bytes : 0
  Output bytes : 46
  Input packets: 0
  Output packets: 1
Transit statistics:
```

```

Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
Protocol inet, MTU: 1500, Generation: 176, Route table: 0
Flags: Sendbroadcast-pkt-to-re
Input Filters: filter-ipv4-with-limits-fe-0/1/1.1-i
Policer: Input: p-all-1m-5k-discard-fe-0/1/1.1-inet-i
Addresses, Flags: Is-Preferred Is-Primary
Destination: 10.20.130/24, Local: 10.20.130.1, Broadcast: 10.20.130.255,

Generation: 169

```

In this example, the two firewall filter policers are applied to logical interface traffic in the input direction only.

### *Displaying Statistics for the Firewall Filter Policers*

**Purpose** Verify the number of packets evaluated by the firewall filter policers.

**Action** Use the **show firewall** operational mode command for the filter you applied to the logical interface.

```

[edit]
user@host> show firewall filter filter-ipv4-with-limits-fe-0/1/1.1-i

Filter: filter-ipv4-with-limits-fe-0/1/1.1-i
Policers:
Name                                     Packets
p-ftp-10p-500k-discard-t-ftp-fe-0/1/1.1-i      0
p-icmp-500k-500k-discard-t-icmp-fe-0/1/1.1-i   0

```

The command output displays the names of the policers (**p-ftp-10p-500k-discard** and **p-icmp-500k-500k-discard**), combined with the names of the filter terms (**t-ftp** and **t-icmp**, respectively) under which the policer action is specified. The policer-specific output lines display the number of packets that matched the filter term. This is only the number of out-of-specification (out-of-spec) packet counts, not all packets policed by the policer.

- Related Documentation**
- [Order of Policar and Firewall Filter Operations on page 10](#)
  - [Statement Hierarchy for Configuring Policers on page 13](#)
  - [Two-Color Policar Configuration Overview on page 15](#)
  - [Guidelines for Applying Traffic Policers on page 24](#)
  - [Calculation of Policar Burst-Size Limit on page 33](#)

## Bandwidth Policers

- [Bandwidth Policar Overview on page 56](#)
- [Example: Configuring a Logical Bandwidth Policar on page 57](#)

## Bandwidth Policer Overview

For a single-rate two-color policer only, you can specify the bandwidth limit as a percentage value from 1 through 100 instead of as an absolute number of bits per second. This type of two-color policer, called a *bandwidth policer*, rate-limits traffic to a bandwidth limit that is calculated as a percentage of either the physical interface media rate or the logical interface configured shaping rate.

---

### Guidelines for Configuring a Bandwidth Policer

The following guidelines apply to configuring a bandwidth policer:

- To specify a percentage bandwidth limit, you include the **bandwidth-percent *percentage*** statement in place of the **bandwidth-limit *bps*** statement.
- By default, a bandwidth policer calculates the percentage bandwidth limit based on the physical interface port speed. To configure a bandwidth policer to calculate the percentage bandwidth limit based on the configured logical interface shaping rate instead, include the **logical-bandwidth-policer** statement at the **[edit firewall policer *policer-name*]** hierarchy level. This type of bandwidth policer is called a *logical bandwidth policer*.

You can configure a logical interface shaping rate by including the **shaping-rate *bps*** statement at the **[edit class-of-service interfaces interface *interface-name* unit *logical-unit-number*]** hierarchy level. A logical interface shaping rate causes the specified amount of bandwidth to be allocated to the logical interface.



**NOTE:** If you configure a logical-bandwidth policer and then apply the policer to a logical interface that is not configured with a shaping rate, then the policer rate-limits traffic on that logical interface to calculate the percentage bandwidth limit based on the physical interface port speed, even if you include the **logical-bandwidth-policer** statement in the bandwidth policer configuration.

- 
- If you reference a bandwidth policer from a stateless firewall filter term, you must include the **interface-specific** statement in the firewall filter configuration.

---

### Guidelines for Applying a Bandwidth Policer

The following guidelines pertain to applying a bandwidth policer to traffic:

- You can use a bandwidth policer to rate-limit protocol-specific traffic (not **family any**) at the input or output of a logical interface.
- You can apply a bandwidth policer directly to protocol-specific input or output traffic at a logical interface.



- To send only selected packets to a bandwidth policer, you can reference the bandwidth policer from a stateless firewall filter term and then apply the filter to logical interface traffic for a specific protocol family.
- To reference a *logical bandwidth policer* from a firewall filter, you must include the **interface-specific** statement in the firewall filter configuration.
- You cannot use a bandwidth policer for forwarding-table filters.
- You cannot apply a bandwidth policer to an aggregate interface, a tunnel interface, or a software interface.

## Example: Configuring a Logical Bandwidth Policor

This example shows how to configure a logical bandwidth policer.

- [Requirements on page 57](#)
- [Overview on page 57](#)
- [Configuration on page 58](#)
- [Verification on page 62](#)

### Requirements

Before you begin, make sure that you have two logical units available on a Gigabit Ethernet interface.

### Overview

In this example, you configure a single-rate two-color policer that specifies the bandwidth limit as a percentage value rather than as an absolute number of bits per second. This type of policer is called a *bandwidth policer*. By default, a bandwidth policer enforces a bandwidth limit based on the line rate of the underlying physical interface. As an option, you can configure a bandwidth policer to enforce a bandwidth limit based on the configured shaping rate of the logical interface. To configure this type of bandwidth policer, called a *logical bandwidth policer*, you include the **logical-bandwidth-policer** statement in the policer configuration.

To configure a logical interface shaping rate, include the **shaping-rate bps** statement at the **[edit class-of-service interfaces interface *interface-name* unit *logical-unit-number*]** hierarchy level. This class-of-service (CoS) configuration statement causes the specified amount of bandwidth to be allocated to the logical interface.



**NOTE:** If you configure a policer bandwidth limit as a percentage but a shaping rate is not configured for the target logical interface, the policer bandwidth limit is calculated as a percentage of the physical interface media rate, even if you enable the logical-bandwidth policing feature.

To apply a logical bandwidth policer to a logical interface, you can apply the policer directly to the logical interface at the protocol family level or (if you only need to rate-limit

filtered packets) you can reference the policer from a stateless firewall filter configured to operate in *interface-specific* mode.

### **Topology**

In this example, you configure two logical interfaces on a single Gigabit Ethernet interface and configure a shaping rate on each logical interface. On logical interface **ge-1/3/0.0**, you allocate 4 Mbps of bandwidth. On logical interface **ge-1/3/0.1**, you allocate 2 Mbps of bandwidth.

You also configure a logical bandwidth policer with a bandwidth limit of 50 percent and a maximum burst size of 125,000 bytes, and then you apply the policer to input and output traffic at the logical units configured on **ge-1/3/0.0**. For logical interface **ge-1/3/0.0**, the policer rate-limits to a bandwidth limit of 2 Mbps (50 percent of the 4 Mbps shaping rate configured for the logical interface). For logical interface **ge-1/3/0.1**, the policer rate-limits traffic to a bandwidth limit of 1 Mbps (50 percent of the 2 Mbps shaping rate configured for the logical interface).

If no shaping rate is configured for a target logical interface, the policer rate-limits to a bandwidth limit calculated as 50 percent of the physical interface media rate. For example, if you apply a 50 percent bandwidth policer to input or output traffic at a Gigabit Ethernet logical interface without rate shaping, the policer applies a bandwidth limit of 500 Mbps (50 percent of 1000 Mbps).

---

### **Configuration**

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see [“Using the CLI Editor in Configuration Mode” on page 215](#).

To configure this example, perform the following tasks:

- [Configuring the Logical Interfaces on page 59](#)
- [Configuring Traffic Rate-Shaping by Specifying the Amount of Bandwidth to be Allocated to the Logical Interface on page 60](#)
- [Configuring the Logical Bandwidth Policer on page 60](#)
- [Applying the Logical Bandwidth Policers to the Logical Interfaces on page 61](#)

#### **CLI Quick Configuration**

To quickly configure this example, copy the following configuration commands into a text file, remove any line breaks, and then paste the commands into the CLI at the **[edit]** hierarchy level.

```
set interfaces ge-1/3/0 per-unit-scheduler
set interfaces ge-1/3/0 vlan-tagging
set interfaces ge-1/3/0 unit 0 vlan-id 100
set interfaces ge-1/3/0 unit 0 family inet address 172.1.1.1/30
set interfaces ge-1/3/0 unit 1 vlan-id 200
set interfaces ge-1/3/0 unit 1 family inet address 172.2.1.1/30
set class-of-service interfaces ge-1/3/0 unit 0 shaping-rate 4m
set class-of-service interfaces ge-1/3/0 unit 1 shaping-rate 2m
set firewall policer LB-policer logical-bandwidth-policer
set firewall policer LB-policer if-exceeding bandwidth-percent 50
set firewall policer LB-policer if-exceeding burst-size-limit 125k
```

```

set firewall policer LB-policer then discard
set interfaces ge-1/3/0 unit 0 family inet policer input LB-policer
set interfaces ge-1/3/0 unit 0 family inet policer output LB-policer
set interfaces ge-1/3/0 unit 1 family inet policer input LB-policer
set interfaces ge-1/3/0 unit 1 family inet policer output LB-policer

```

### *Configuring the Logical Interfaces*

#### **Step-by-Step Procedure**

To configure the logical interfaces:

1. Enable configuration of the physical interface.

```

[edit]
user@host# edit interfaces ge-1/3/0

```

```

[edit interfaces ge-1/3/0]
user@host# set per-unit-scheduler
user@host# set vlan-tagging

```

2. Configure the first logical interface.

```

[edit interfaces ge-1/3/0]
user@host# set unit 0 vlan-id 100
user@host# set unit 0 family inet address 172.1.1.1/30

```

3. Configure the second logical interface.

```

[edit interfaces ge-1/3/0]
user@host# set unit 1 vlan-id 200
user@host# set unit 1 family inet address 172.2.1.1/30

```

**Results** Confirm the configuration of the interfaces by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```

[edit]
user@host# show interfaces
ge-1/3/0 {
  per-unit-scheduler;
  vlan-tagging;
  unit 0 {
    vlan-id 100;
    family inet {
      address 172.1.1.1/30;
    }
  }
  unit 1 {
    vlan-id 200;
    family inet {
      address 172.2.1.1/30;
    }
  }
}

```

### *Configuring Traffic Rate-Shaping by Specifying the Amount of Bandwidth to be Allocated to the Logical Interface*

**Step-by-Step Procedure** To configure rate shaping by specifying the bandwidth to be allocated to the logical interface:

1. Enable CoS configuration on the physical interface.

```
[edit]
user@host# edit class-of-service interfaces ge-1/3/0
```

2. Configure rate shaping for the logical interfaces.

```
[edit]
user@host# set unit 0 shaping-rate 4m
user@host# set unit 1 shaping-rate 2m
```

These statements allocate 4 Mbps of bandwidth to logical unit **ge-1/3/0.0** and 2 Mbps of bandwidth to logical unit **ge-1/3/0.1**.

**Results** Confirm the configuration of the rate shaping by entering the **show class-of-service** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show class-of-service
interfaces {
  ge-1/3/0 {
    unit 0 {
      shaping-rate 4m;
    }
    unit 1 {
      shaping-rate 2m;
    }
  }
}
```

### *Configuring the Logical Bandwidth Policer*

**Step-by-Step Procedure** To configure the logical bandwidth policer:

1. Enable configuration of a single-rate two-color policer.

```
[edit]
user@host# edit firewall policer LB-policer
```

2. Configure the policer as a logical-bandwidth policer.

```
[edit firewall policer LB-policer]
user@host# set logical-bandwidth-policer
```

This applies the rate-limiting to logical interfaces.

3. Configure the policer traffic limits and actions.

```
[edit firewall policer LB-policer]
user@host# set if-exceeding bandwidth-percent 50
user@host# set if-exceeding burst-size-limit 125k
```

```
user@host# set then discard
```

**Results** Confirm the configuration of the policer by entering the **show firewall** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show firewall
policer LB-policer {
  logical-bandwidth-policer;
  if-exceeding {
    bandwidth-percent 50;
    burst-size-limit 125k;
  }
  then discard;
}
```

### *Applying the Logical Bandwidth Policers to the Logical Interfaces*

**Step-by-Step Procedure** To configure the logical bandwidth policers to the logical interfaces:

1. Enable configuration of the interface.

```
[edit]
user@host# edit interfaces ge-1/3/0
```

2. Apply the logical bandwidth policer to the first logical interface.

```
[edit interfaces ge-1/3/0]
user@host# set unit 0 family inet policer input LB-policer
user@host# set unit 0 family inet policer output LB-policer
```

3. Apply the policing to the second logical interface.

```
[edit interfaces ge-1/3/0]
user@host# set unit 1 family inet policer input LB-policer
user@host# set unit 1 family inet policer output LB-policer
```

**Results** Confirm the configuration of the interfaces by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show interfaces
ge-1/3/0 {
  per-unit-scheduler;
  vlan-tagging;
  unit 0 {
    vlan-id 100;
    family inet {
      policer {
        input LB-policer;
        output LB-policer;
      }
    }
    address 172.1.1.1/30;
  }
}
```

```

    }
    unit 1 {
        vlan-id 200;
        family inet {
            policer {
                input LB-policer;
                output LB-policer;
            }
            address 172.2.1.1/30;
        }
    }
}

```

If you are done configuring the device, enter **commit** from configuration mode.

### Verification

Confirm that the configuration is working properly.

- [Displaying Traffic Statistics and Policers for the Logical Interface on page 62](#)
- [Displaying Statistics for the Policer on page 63](#)

#### *Displaying Traffic Statistics and Policers for the Logical Interface*

**Purpose** Verify the traffic flow through the logical interface and that the policer is evaluated when packets are received on the logical interface.

**Action** Use the **show interfaces** operational mode command for logical interfaces **ge-1/3/0.0** and **ge-1/3/0.1**, and include the **detail** or **extensive** option. The command output section for **Traffic statistics** lists the number of bytes and packets received and transmitted on the logical interface, and the **Protocol inet** section contains a **Policer** field that lists the policer **LB-policer** as an input or output policer as follows:

- **Input: LB-policer-ge-1/3/0.0-inet-i**
- **Output: LB-policer-ge-1/3/0.0-inet-o**

In this example, the policer is applied to logical interface traffic in both the input and output directions.

```

user@host> show interfaces ge-1/3/0.0 detail
Logical interface ge-1/3/0.0 (Index 80) (SNMP ifIndex 154) (Generation 150)
  Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.100 ] Encapsulation: ENET2
  Traffic statistics:
    Input bytes :          0
    Output bytes :         46
    Input packets:          0
    Output packets:         1
  Local statistics:
    Input bytes :          0
    Output bytes :         46
    Input packets:          0
    Output packets:         1
  Transit statistics:
    Input bytes :          0          0 bps
    Output bytes :          0          0 bps

```

```

      Input packets:                0                0 pps
      Output packets:              0                0 pps
      Protocol inet, MTU: 1500, Generation: 174, Route table: 0
      Flags: Sendbcast-pkt-to-re
      Policer: Input: LB-policer-ge-1/3/0.0-inet-i, Output:
LB-policer-ge-1/3/0.0-inet-o
      Addresses, Flags: Is-Preferred Is-Primary
      Destination: 172.1.1.0/30, Local: 172.1.1.1, Broadcast: 172.1.1.3,
      Generation: 165

```

```

user@host> show interfaces ge-1/3/0.1 detail
Logical interface ge-1/3/0.1 (Index 81) (SNMP ifIndex 543) (Generation 151)
  Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.200 ] Encapsulation: ENET2
  Traffic statistics:
    Input bytes :                0
    Output bytes :               46
    Input packets:               0
    Output packets:              1
  Local statistics:
    Input bytes :                0
    Output bytes :               46
    Input packets:               0
    Output packets:              1
  Transit statistics:
    Input bytes :                0                0 bps
    Output bytes :               0                0 bps
    Input packets:               0                0 pps
    Output packets:              0                0 pps
  Protocol inet, MTU: 1500, Generation: 175, Route table: 0
  Flags: Sendbcast-pkt-to-re
  Policer: Input: LB-policer-ge-1/3/0.1-inet-i, Output:
LB-policer-ge-1/3/0.1-inet-o
  Addresses, Flags: Is-Preferred Is-Primary
  Destination: 172.2.1.0/30, Local: 172.2.1.1, Broadcast: 172.2.1.3,
  Generation: 167

```

### *Displaying Statistics for the Policer*

**Purpose** Verify the number of packets evaluated by the policer.

**Action** Use the `show policer` operational mode command and optionally specify the name of the policer. The command output displays the number of packets evaluated by each configured policer (or the specified policer), in each direction. For the policer **LB-policer**, the input and output policer names are displayed as follows:

- LB-policer-ge-1/3/0.0-inet-i
- LB-policer-ge-1/3/0.0-inet-o
- LB-policer-ge-1/3/0.1-inet-i
- LB-policer-ge-1/3/0.1-inet-o

The **-inet-i** suffix denotes a policer applied to logical interface input traffic, while the **-inet-o** suffix denotes a policer applied to logical interface output traffic. In this example, the policer is applied to both input and output traffic on logical interface **ge-1/3/0.0** and logical interface **ge-1/3/0.1**.

```

user@host> show policer
Policers:
Name                                     Packets
__default_arp_policer__                 0
LB-policer-ge-1/3/0.0-inet-i            0
LB-policer-ge-1/3/0.0-inet-o            0
LB-policer-ge-1/3/0.1-inet-i            0
LB-policer-ge-1/3/0.1-inet-o            0

```

#### Related Documentation

- [Statement Hierarchy for Configuring Policers on page 13](#)
- [Two-Color Policer Configuration Overview on page 15](#)
- [Guidelines for Applying Traffic Policers on page 24](#)
- [bandwidth-percent on page 170](#)
- “interface-specific” in the *Junos OS Firewall Filter and Policer Configuration Guide*
- [logical-bandwidth-policer on page 190](#)
- [shaping-rate \(Applying to an Interface\) in the Junos OS Class of Service Configuration Guide](#)

## Filter-Specific Counters and Policers

- [Filter-Specific Policer Overview on page 64](#)
- [Example: Configuring a Stateless Firewall Filter to Protect Against TCP and ICMP Floods on page 65](#)

### Filter-Specific Policer Overview

By default, a policer operates in *term-specific* mode so that, for a given firewall filter, the Junos OS creates a separate policer instance for every filter term that references the policer. As an option, you can configure a policer to operate in *filter-specific* mode so that a single policer instance is used by all terms (within the same firewall filter) that reference the policer.

For an IPv4 firewall filter with multiple terms that reference the same policer, configuring the policer to operate in filter-specific mode enables you to count and monitor the activity of the policer at the firewall filter level.



**NOTE:** Term-specific mode and filter-specific mode also apply to prefix-specific policer sets.

To enable a single-rate two-color policer to operate in filter-specific mode, you can include the **filter-specific** statement at the following hierarchy levels:

- **[edit firewall policer *policer-name*]**
- **[edit logical-systems *logical-system-name* firewall policer *policer-name*]**

You can reference filter-specific policers from IPv4 (**family inet**) firewall filters only.



## Example: Configuring a Stateless Firewall Filter to Protect Against TCP and ICMP Floods

This example shows how to create a stateless firewall filter that protects against TCP and ICMP denial-of-service attacks.

- [Requirements on page 65](#)
- [Overview on page 65](#)
- [Configuration on page 66](#)
- [Verification on page 69](#)

### Requirements

No special configuration beyond device initialization is required before configuring stateless firewall filters.

### Overview

In this example, you create a stateless firewall filter called **protect-RE** that polices TCP and ICMP packets. This example includes the following policers:

- **tcp-connection-policer**—Limits the traffic rate of the TCP packets to 500,000 bps and the burst size to 15,000 bytes. Packets that exceed the traffic rate are discarded.
- **icmp-policer**—Limits the traffic rate of the ICMP packets to 1,000,000 bps and the burst size to 15,000 bytes. Packets that exceed the traffic rate are discarded.

When specifying limits, the bandwidth limit can be from 32,000 bps to 32,000,000,000 bps and the burst-size limit can be from 1,500 bytes through 100,000,000 bytes. Use the following abbreviations when specifying limits: k (1,000), m (1,000,000), and g (1,000,000,000).

Each policer is incorporated into the action of a filter term. This example includes the following terms:

- **tcp-connection-term**—Policies certain TCP packets with a source address of 192.168.122.0/24 or 10.2.1.0/24. These addresses are defined in the **trusted-addresses** prefix list.

Policed packets include connection request packets (SYN and ACK flag bits equal 1 and 0), connection release packets (FIN flag bit equals 1), and connection reset packets (RST flag bit equals 1).

- **icmp-term**—Policies echo request packets, echo response packets, unreachable packets, and time-exceeded packets. All of these ICMP packets are counted in the **icmp-counter** counter.



**NOTE:** You can move terms within the firewall filter by using the **insert** command. See **insert** in the [Junos OS CLI User Guide](#).

If you want to include the terms created in this procedure in the **protect-RE** firewall filter configured in Example: Configuring a Stateless Firewall Filter to Accept Traffic from Trusted Sources, perform the configuration tasks in this example first. Then configure the terms as described in Example: Configuring a Stateless Firewall Filter to Accept Traffic from Trusted Sources. This approach ensures that the rate-limiting terms are included as the first two terms in the firewall filter.



**NOTE:** You can move terms within the firewall filter by using the `insert` command. See `insert` in the [Junos OS CLI User Guide](#).

### Configuration

#### CLI Quick Configuration

To quickly configure the stateless firewall filter, copy the following commands to a text file, remove any line breaks, and then paste the commands into the CLI.

```
[edit]
set firewall family inet filter protect-RE term tcp-connection-term from source-prefix-list
  trusted-addresses
set firewall family inet filter protect-RE term tcp-connection-term from protocol tcp
set firewall family inet filter protect-RE term tcp-connection-term from tcp-flags "(syn
  & !ack) | fin | rst"
set firewall family inet filter protect-RE term tcp-connection-term then policer
  tcp-connection-policer
set firewall family inet filter protect-RE term tcp-connection-term then accept
set firewall family inet filter protect-RE term icmp-term from protocol icmp
set firewall family inet filter protect-RE term icmp-term from icmp-type echo-request
set firewall family inet filter protect-RE term icmp-term from icmp-type echo-reply
set firewall family inet filter protect-RE term icmp-term from icmp-type unreachable
set firewall family inet filter protect-RE term icmp-term from icmp-type time-exceeded
set firewall family inet filter protect-RE term icmp-term then policer icmp-policer
set firewall family inet filter protect-RE term icmp-term then count icmp-counter
set firewall family inet filter protect-RE term icmp-term then accept
set firewall policer tcp-connection-policer filter-specific
set firewall policer tcp-connection-policer if-exceeding bandwidth-limit 1m
set firewall policer tcp-connection-policer if-exceeding burst-size-limit 15k
set firewall policer tcp-connection-policer then discard
set firewall policer icmp-policer filter-specific
set firewall policer icmp-policer if-exceeding bandwidth-limit 1m
set firewall policer icmp-policer if-exceeding burst-size-limit 15k
set firewall policer icmp-policer then discard
set policy-options prefix-list trusted-addresses 10.2.1.0/24
set policy-options prefix-list trusted-addresses 192.168.122.0/24
```

#### Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see ["Using the CLI Editor in Configuration Mode" on page 215](#).

To configure stateless firewall filter policers:

1. Define the first policer.

```
[edit]
```

- ```

user@host# edit firewall policer tcp-connection-policer

```
2. Define the action for the policer.
 

```

[edit firewall policer tcp-connection-policer]
user@host# set then discard

```
3. Define the rate limits for the policer.
 

```

[edit firewall policer tcp-connection-policer]
user@host# set filter-specific
user@host# set if-exceeding burst-size-limit 15k bandwidth-limit 1m

```
4. Define the second policer.
 

```

[edit]
user@host# edit firewall policer icmp-policer

```
5. Define the action for the policer.
 

```

[edit firewall policer icmp-policer]
user@host# set then discard

```
6. Set the rate limits for the policer.
 

```

[edit firewall policer icmp-policer]
user@host# set filter-specific
user@host# set if-exceeding burst-size-limit 15k bandwidth-limit 1m

```
7. Define the prefix list.
 

```

[edit]
user@host# set policy-options prefix-list trusted-addresses 192.168.122.0/24
user@host# set policy-options prefix-list trusted-addresses 10.2.1.0/24

```
8. Create the stateless firewall filter.
 

```

[edit]
user@host# edit firewall family inet filter protect-RE

```
9. Define the first term for the filter.
 

```

[edit firewall family inet filter protect-RE]
user@host# edit term tcp-connection-term

```
10. Define the source address match condition for the term.
 

```

[edit firewall family inet filter protect-RE term tcp-connection-term]
user@host# set from source-prefix-list trusted-addresses

```
11. Define protocol match conditions for the term.
 

```

[edit firewall family inet filter protect-RE term tcp-connection-term]
user@host# set from protocol tcp tcp-flags "(syn & !ack) | fin | rst"

```
12. Define the actions for the term.
 

```

[edit firewall family inet filter protect-RE term tcp-connection-term]
user@host# set then policer tcp-connection-policer accept

```

13. Define the second term.

```
[edit]
user@host# edit firewall family inet filter protect-RE term icmp-term
```

14. Define the protocol for the term.

```
[edit firewall family inet filter protect-RE term icmp-term]
user@host# set from protocol icmp
```

15. Define the match conditions for the term.

```
[edit firewall family inet filter protect-RE term icmp-term]
user@host# set from icmp-type [echo-request echo-reply unreachable
time-exceeded]
```

16. Define the action for the term.

```
[edit firewall family inet filter protect-RE term icmp-term]
user@host# set then policer icmp-policer count icmp-counter accept
```

**Results** Confirm your configuration by entering the **show firewall** command and the **show policy-options** command from configuration mode. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show firewall
family inet {
  filter protect-RE {
    term tcp-connection-term {
      from {
        source-prefix-list {
          trusted-addresses;
        }
        protocol tcp;
        tcp-flags "(syn & !ack) | fin | rst";
      }
      then {
        policer tcp-connection-policer;
        accept;
      }
    }
    term icmp-term {
      from {
        protocol icmp;
        icmp-type [ echo-request echo-reply unreachable time-exceeded ];
      }
      then {
        policer icmp-policer;
        count icmp-counter;
        accept;
      }
    }
  }
}
policer tcp-connection-policer {
  filter-specific;
  if-exceeding {
```

```

        bandwidth-limit 1m;
        burst-size-limit 15k;
    }
    then discard;
}
policer icmp-policer {
    filter-specific;
    if-exceeding {
        bandwidth-limit 1m;
        burst-size-limit 15k;
    }
    then discard;
}

user@host# show policy-options
prefix-list trusted-addresses {
    10.2.1.0/24;
    192.168.122.0/24;
}

```

If you are done configuring the device, enter **commit** from configuration mode.

### Verification

Confirm that the configuration is working properly.

- [Displaying Stateless Firewall Filter Configurations on page 69](#)
- [Verifying a TCP and ICMP Flood Firewall Filter on page 69](#)
- [Displaying Firewall Filter Statistics on page 70](#)

#### *Displaying Stateless Firewall Filter Configurations*

|                |                                                                                                                                                                                                                                                                            |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b> | Verify the configuration of the firewall filter.                                                                                                                                                                                                                           |
| <b>Action</b>  | From configuration mode, enter the <b>show firewall</b> command.                                                                                                                                                                                                           |
| <b>Meaning</b> | Verify that the output shows the intended configuration of the firewall filter. In addition, verify that the terms are listed in the order in which you want the packets to be tested. You can move terms within a firewall filter by using the <b>insert</b> CLI command. |

#### *Verifying a TCP and ICMP Flood Firewall Filter*

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b> | Verify that the actions of the firewall filter terms are taken.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Action</b>  | <p>Send packets to the device that match the terms. In addition, verify that the filter actions are <i>not</i> taken for packets that do not match.</p> <ul style="list-style-type: none"> <li>• Verify that the device can establish only TCP sessions with a host at an IP address that matches 192.168.122.0/24 or 10.2.1.0/24. For example, log in to the device with the <b>telnet <i>host-name</i></b> command from another host with one of these address prefixes.</li> <li>• Use the <b>ping <i>host-name</i></b> command to verify that the device responds only to ICMP packets (such as ping requests) that do not exceed the policer traffic rates.</li> </ul> |

- Use the **ping *host-name* size *bytes*** command to exceed the policer traffic rates by sending ping requests with large data payloads.

## Sample Output

```
user@host> telnet 192.168.249.71
Trying 192.168.249.71...
Connected to host.acme.net.
Escape character is '^J'.

host (ttyp0)

login: user
Password:

--- JUNOS 6.4-20040521.1 built 2004-05-21 09:38:12 UTC

user@host>

user@host> ping 192.168.249.71
PING host-ge-000.acme.net (192.168.249.71): 56 data bytes
64 bytes from 192.168.249.71: icmp_seq=0 ttl=253 time=11.946 ms
64 bytes from 192.168.249.71: icmp_seq=1 ttl=253 time=19.474 ms
64 bytes from 192.168.249.71: icmp_seq=2 ttl=253 time=14.639 ms
...

user@host> ping 192.168.249.71 size 20000
PING host-ge-000.acme.net (192.168.249.71): 20000 data bytes
^C
--- host-ge-000.acme.net ping statistics ---
12 packets transmitted, 0 packets received, 100% packet loss
```

**Meaning** Verify the following information:

- You can successfully log in to the device using Telnet.
- The device sends responses to the **ping host** command.
- The device does not send responses to the **ping host size 20000** command.

### *Displaying Firewall Filter Statistics*

**Purpose** Verify that packets are being policed and counted.

**Action** From operational mode, enter the **show firewall filter *filter-name*** command.

## Sample Output

```
user@host> show firewall filter protect-RE
Filter: protect-RE
Counters:
Name                               Bytes          Packets
icmp-counter                        1040000         5600
Policers:
Name                               Packets
```

|                        |           |
|------------------------|-----------|
| tcp-connection-policer | 643254873 |
| icmp-policer           | 7391      |

**Meaning** Verify the following information:

- Next to **Filter**, the name of the firewall filter is correct.
- Under **Counters**:
  - Under **Name**, the names of any counters configured in the firewall filter are correct.
  - Under **Bytes**, the number of bytes that match the filter term containing the **count counter-name** action are shown.
  - Under **Packets**, the number of packets that match the filter term containing the **count counter-name** action are shown.
- Under **Policers**:
  - Under **Name**, the names of any policers configured in the firewall filter are correct.
  - Under **Packets**, the number of packets that match the conditions specified for the policer are shown.

**Related Documentation**

- [Statement Hierarchy for Configuring Policers on page 13](#)
- [Two-Color Policer Configuration Overview on page 15](#)
- [Guidelines for Applying Traffic Policers on page 24](#)
- [Prefix-Specific Counting and Policing Actions on page 71](#)

## Prefix-Specific Counting and Policing Actions

- [Prefix-Specific Counting and Policing Overview on page 71](#)
- [Filter-Specific Counter and Policer Set Overview on page 74](#)
- [Example: Configuring Prefix-Specific Counting and Policing on page 74](#)
- [Prefix-Specific Counting and Policing Configuration Scenarios on page 81](#)

## Prefix-Specific Counting and Policing Overview

This topic covers the following information:

- [Separate Counting and Policing for Each IPv4 Address Range on page 71](#)
- [Prefix-Specific Action Configuration on page 72](#)
- [Counter and Policer Set Size and Indexing on page 73](#)

### Separate Counting and Policing for Each IPv4 Address Range

Prefix-specific counting and policing enables you to configure an IPv4 firewall filter term that matches on a source or destination address, applies a single-rate two-color policer as the term action, but associates the matched packet with a specific counter and policer instance based on the source or destination in the packet header. You can implicitly

create a separate counter or policer instance for a single address or for a group of addresses.



**NOTE:** J Series Services Routers do not support prefix-specific counting and policing.

Prefix-specific counting and policing uses a *prefix-specific action* configuration that specifies the name of the policer you want to apply, whether prefix-specific counting is to be enabled, and a source or destination address prefix range.

The prefix range specifies between 1 and 16 sequential set bits of an IPv4 address mask. The length of the prefix range determines the size of the counter and policer set, which consists of as few as 2 or as many as 65,536 counter and policer instances. The position of the bits of the prefix range determines the indexing of filter-matched packets into the set of instances.



**NOTE:** A prefix-specific action is specific to a source or destination *prefix range*, but it is not specific to a particular source or destination *address range*, and it is not specific to a particular interface.

To apply a prefix-specific action to the traffic at an interface, you configure a firewall filter term that matches on source or destination addresses, and then you apply the firewall filter to the interface. The flow of filtered traffic is rate-limited using prefix-specific counter and policer instances that are selected per packet based on the source or destination address in the header of the filtered packet.

### Prefix-Specific Action Configuration

To configure a prefix-specific action, you specify the following information:

- Prefix-specific action name—Name that can be referenced as the action of an IPv4 standard firewall filter term that matches packets on source or destination addresses.
- Policer name—Name of a single-rate two-color policer for which you want to implicitly create prefix-specific instances.



**NOTE:** For aggregated Ethernet interfaces, you can configure a prefix-specific action that references a logical interface policer (also called an aggregate policer). You can reference this type of prefix-specific action from an IPv4 standard firewall filter and then apply the filter at the aggregate level of the interface.

- Counting option—Option to include if you want to enable prefix-specific counters.
- Filter-specific option—Option to include if you want a single counter and policer set to be shared across all terms in the firewall filter. A prefix-specific action that operates in this way is said to operate in *filter-specific* mode. If you do not enable this option,



the prefix-specific action operates in *term-specific* mode, meaning that a separate counter and policer set is created for each filter term that references the prefix-specific action.

- Source address prefix length—Length of the address prefix, from 0 through 32, to be used with a packet matched on the source address.
- Destination address prefix length—Length of the address prefix, from 0 through 32, to be used with a packet matched on the destination address.
- Subnet prefix length—Length of the subnet prefix, from 0 through 32, to be used with a packet matched on either the source or destination address.

You must configure source and destination address prefix lengths to be from 1 to 16 bits longer than the subnet prefix length. If you configure source or destination address prefix lengths to be more than 16 bits beyond the configured subnet prefix length, an error occurs when you try to commit the configuration.

### Counter and Policer Set Size and Indexing

The number of prefix-specific actions (counters or policers) implicitly created for a prefix-specific action is determined by the length of the address prefix and the length of the subnet prefix:

$$\text{Size of Counter and Policer Set} = 2^{(\text{source-or-destination-prefix-length} - \text{subnet-prefix-length})}$$

Table 7 on page 73 shows examples of counter and policer set size and indexing.

**Table 7: Examples of Counter and Policer Set Size and Indexing**

| Example Prefix Lengths Specified in the Prefix-Specific Action       | Calculation of Counter or Policer Set Size                                                                                              | Indexing of Instances |             |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-------------|
| <i>source-prefix-length</i> = 32<br><i>subnet-prefix-length</i> = 16 | Size = $2^{(32-16)} = 2^{16} = 65,536$ instances<br><br>NOTE: This calculation shows the largest counter or policer set size supported. | Instance 0:           | x.x.0.0     |
|                                                                      |                                                                                                                                         | Instance 1:           | x.x.0.1     |
|                                                                      |                                                                                                                                         | Instance 65535:       | x.x.255.255 |
| <i>source-prefix-length</i> = 32<br><i>subnet-prefix-length</i> = 24 | Size = $2^{(32-24)} = 2^8 = 256$ instances                                                                                              | Instance 0:           | x.x.x.0     |
|                                                                      |                                                                                                                                         | Instance 1:           | x.x.x.1     |
|                                                                      |                                                                                                                                         | Instance 255:         | x.x.x.255   |
| <i>source-prefix-length</i> = 32<br><i>subnet-prefix-length</i> = 25 | Size = $2^{(32-25)} = 2^7 = 128$ instances                                                                                              | Instance 0:           | x.x.x.0     |
|                                                                      |                                                                                                                                         | Instance 1:           | x.x.x.1     |
|                                                                      |                                                                                                                                         | Instance 127:         | x.x.x.127   |

**Table 7: Examples of Counter and Policer Set Size and Indexing (*continued*)**

| Example Prefix Lengths Specified in the Prefix-Specific Action                   | Calculation of Counter or Policer Set Size                 | Indexing of Instances              |
|----------------------------------------------------------------------------------|------------------------------------------------------------|------------------------------------|
| <code>source-prefix-length = 24</code><br><code>subnet-prefix-length = 20</code> | $\text{Size} = 2^{(24 - 20)} = 2^4 = 16 \text{ instances}$ | Instance 0: <code>x.x.0.x</code>   |
|                                                                                  |                                                            | Instance 1: <code>x.x.1.x</code>   |
|                                                                                  |                                                            | Instance 15: <code>x.x.15.x</code> |

## Filter-Specific Counter and Policer Set Overview

By default, a prefix-specific policer set operates in *term-specific* mode so that, for a given firewall filter, the Junos OS creates a separate counter and policer set for every filter term that references the prefix-specific action. As an option, you can configure a prefix-specific policer set to operate in *filter-specific* mode so that a single prefix-specific policer set is used by all terms (within the same firewall filter) that reference the policer.

For an IPv4 firewall filter with multiple terms that reference the same prefix-specific policer set, configuring the policer set to operate in filter-specific mode enables you to count and monitor the activity of the policer set at the firewall filter level.



**NOTE:** Term-specific mode and filter-specific mode also apply to policers. See [“Filter-Specific Policer Overview”](#) on page 64.

To enable a prefix-specific policer set to operate in filter-specific mode, you can include the **filter-specific** statement at following the hierarchy levels:

- `[edit firewall family inet prefix-action prefix-action-name]`
- `[edit logical-systems logical-system-name firewall family inet prefix-action prefix-action-name]`

You can reference filter-specific, prefix-specific policer sets from IPv4 (**family inet**) firewall filters only.

## Example: Configuring Prefix-Specific Counting and Policing

This example shows how to configure prefix-specific counting and policing.

- [Requirements on page 75](#)
- [Overview on page 75](#)
- [Configuration on page 76](#)
- [Verification on page 80](#)

## Requirements

---

No special configuration beyond device initialization is required before configuring this example.

## Overview

---

In this example, you configure prefix-specific counting and policing based on the last octet of the source address field in packets matched by an IPv4 firewall filter.

The single-rate two-color policer named **1Mbps-policer** rate-limits traffic to a bandwidth of 1,000,000 bps and a burst-size limit of 63,000 bytes, discarding any packets in a traffic flow that exceeds the traffic limits.

Independent of the IPv4 addresses contained in any packets passed from a firewall filter, the prefix-specific action named **psa-1Mbps-per-source-24-32-256** specifies a set of 256 counters and policers, numbered from 0 through 255. For each packet, the last octet of the source address field is used to index into the associated prefix-specific counter and policer in the set:

- Packets with a source address ending with the octet 0x0000 0000 index the first counter and policer in the set.
- Packets with a source address ending with the octet 0x0000 0001 index the second counter and policer in the set.
- Packets with a source address ending with the octet 0x1111 1111 index the last counter and policer in the set.

The **limit-source-one-24** firewall filter contains a single term that matches all packets from the /24 subnet of source address 10.10.10.0, passing these packets to the prefix-specific action **psa-1Mbps-per-source-24-32-256**.

## Topology

In this example, because the filter term matches the /24 subnet of a single source address, each counting and policing instance in the prefix-specific set is used for only one source address.

- Packets with a source address **10.10.10.0** index the first counter and policer in the set.
- Packets with a source address **10.10.10.1** index the second counter and policer in the set.
- Packets with a source address **10.10.10.255** index the last counter and policer in the set.

This example shows the simplest case of prefix-specific actions, in which the filter term matches on one address with a prefix length that is the same as the prefix length specified in the prefix-specific action for indexing into the set of prefix-specific counters and policers.

For descriptions of other configurations for prefix-specific counting and policing, see [“Prefix-Specific Counting and Policing Configuration Scenarios” on page 81](#).

## Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see [“Using the CLI Editor in Configuration Mode” on page 215](#).

To configure this example, perform the following tasks:

- [Configuring a Policer for Prefix-Specific Counting and Policing on page 76](#)
- [Configuring a Prefix-Specific Action Based on the Policer on page 77](#)
- [Configuring an IPv4 Filter That References the Prefix-Specific Action on page 78](#)
- [Applying the Firewall Filter to IPv4 Input Traffic at a Logical Interface on page 79](#)

### CLI Quick Configuration

To quickly configure this example, copy the following configuration commands into a text file, remove any line breaks, and then paste the commands into the CLI at the **[edit]** hierarchy level.

```
set firewall policer 1Mbps-policer if-exceeding bandwidth-limit 1m
set firewall policer 1Mbps-policer if-exceeding burst-size-limit 63k
set firewall policer 1Mbps-policer then discard
set firewall family inet prefix-action psa-1Mbps-per-source-24-32-256 policer
  1Mbps-policer
set firewall family inet prefix-action psa-1Mbps-per-source-24-32-256 count
set firewall family inet prefix-action psa-1Mbps-per-source-24-32-256
  subnet-prefix-length 24
set firewall family inet prefix-action psa-1Mbps-per-source-24-32-256 source-prefix-length
  32
set firewall family inet filter limit-source-one-24 term one from source-address
  10.10.10.0/24
set firewall family inet filter limit-source-one-24 term one then prefix-action
  psa-1Mbps-per-source-24-32-256
set interfaces so-0/0/2 unit 0 family inet filter input limit-source-one-24
set interfaces so-0/0/2 unit 0 family inet address 10.39.1.1/16
```

### Configuring a Policer for Prefix-Specific Counting and Policing

### Step-by-Step Procedure

To configure a policer to be used for prefix-specific counting and policing:

1. Enable configuration of a single-rate two-color policer.

```
[edit]
user@host# edit firewall policer 1Mbps-policer
```

2. Define the traffic limit.

```
[edit firewall policer 1Mbps-policer]
user@host# set if-exceeding bandwidth-limit 1m
user@host# set if-exceeding burst-size-limit 63k
```

Packets in a traffic flow that conforms to this limit are passed with the PLP set to **low**.

3. Define the actions for nonconforming traffic.

```
[edit firewall policer 1Mbps-policer]
user@host# set then discard
```

Packets in a traffic flow that exceeds this limit are discarded. Other configurable actions for a single-rate two-color policer are to set the forwarding class and to set the PLP level.

**Results** Confirm the configuration of the policer by entering the **show firewall** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show firewall
policer 1Mbps-policer {
  if-exceeding {
    bandwidth-limit 1m;
    burst-size-limit 63k;
  }
  then discard;
}
```

### *Configuring a Prefix-Specific Action Based on the Policer*

**Step-by-Step Procedure** To configure a prefix-specific action that references the policer and specifies a portion of a source address prefix:

1. Enable configuration of a prefix-specific action.

```
[edit]
user@host# edit firewall family inet prefix-action psa-1Mbps-per-source-24-32-256
```

Prefix-specific counting and policing can be defined for IPv4 traffic only.

2. Reference the policer for which a prefix-specific set is to be created.

```
[edit firewall family inet prefix-action psa-1Mbps-per-source-24-32-256]
user@host# set policer 1Mbps-policer
user@host# set count
```



**NOTE:** For aggregated Ethernet interfaces, you can configure a prefix-specific action that references a logical interface policer (also called an aggregate policer). You can reference this type of prefix-specific action from an IPv4 standard firewall filter and then apply the filter at the aggregate level of the interface.

3. Specify the prefix range on which IPv4 addresses are to be indexed to the counter and policer set.

```
[edit firewall family inet prefix-action psa-1Mbps-per-source-24-32-256]
user@host# set source-prefix-length 32
user@host# set subnet-prefix-length 24
```

**Results** Confirm the configuration of the prefix-specific action by entering the **show firewall** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show firewall
policer 1Mbps-policer {
  if-exceeding {
    bandwidth-limit 1m;
    burst-size-limit 63k;
  }
  then discard;
}
family inet {
  prefix-action psa-1Mbps-per-source-24-32-256 {
    policer 1Mbps-policer;
    subnet-prefix-length 24;
    source-prefix-length 32;
  }
}
```

#### *Configuring an IPv4 Filter That References the Prefix-Specific Action*

**Step-by-Step Procedure** To configure an IPv4 standard firewall filter that references the prefix-specific action:

1. Enable configuration of the IPv4 standard firewall filter.

```
[edit]
user@host# edit firewall family inet filter limit-source-one-24
```

Prefix-specific counting and policing can be defined for IPv4 traffic only.

2. Configure the filter term to match on the packet source address or destination address.

```
[edit firewall family inet filter limit-source-one-24]
user@host# set term one from source-address 10.10.10.0/24
```

3. Configure the filter term to reference the prefix-specific action.

```
[edit firewall family inet filter limit-source-one-24]
user@host# set term one then prefix-action psa-1Mbps-per-source-24-32-256
```

You could also use the **next term** action to configure all Hypertext Transfer Protocol (HTTP) traffic to each host to transmit at 500 Kbps and have the total HTTP traffic limited to 1 Mbps.

**Results** Confirm the configuration of the prefix-specific action by entering the **show firewall** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show firewall
policer 1Mbps-policer {
  if-exceeding {
    bandwidth-limit 1m;
    burst-size-limit 63k;
```

```

    }
    then discard;
  }
  family inet {
    prefix-action psa-1Mbps-per-source-24-32-256 {
      policer 1Mbps-policer;
      subnet-prefix-length 24;
      source-prefix-length 32;
    }
    filter limit-source-one-24 {
      term one {
        from {
          source-address {
            10.10.10.0/24;
          }
        }
        then prefix-action psa-1Mbps-per-source-24-32-256;
      }
    }
  }
}

```

### *Applying the Firewall Filter to IPv4 Input Traffic at a Logical Interface*

#### **Step-by-Step Procedure**

To apply the firewall filter to IPv4 input traffic at a logical interface:

1. Enable configuration of IPv4 on the logical interface.

```

[edit]
user@host# edit interfaces so-0/0/2 unit 0 family inet

```

2. Configure an IP address.

```

[edit interfaces so-0/0/2 unit 0 family inet]
user@host# set address 10.39.1.1/16

```

3. Apply the IPv4 standard stateless firewall filter.

```

[edit interfaces so-0/0/2 unit 0 family inet]
user@host# set filter input limit-source-one-24

```

#### **Results**

Confirm the configuration of the prefix-specific action by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```

[edit]
user@host# show interfaces
so-0/0/2 {
  unit 0 {
    family inet {
      filter {
        input limit-source-one-24;
      }
      address 10.39.1.1/16;
    }
  }
}

```

If you are done configuring the device, enter **commit** from configuration mode.

### Verification

---

Confirm that the configuration is working properly.

- [Displaying the Firewall Filters Applied to an Interface on page 80](#)
- [Displaying Prefix-Specific Actions Statistics for the Firewall Filter on page 80](#)

#### *Displaying the Firewall Filters Applied to an Interface*

**Purpose** Verify that the firewall filter **limit-source-one-24** is applied to the IPv4 input traffic at logical interface **so-0/0/2.0**.

**Action** Use the **show interfaces statistics** operational mode command for logical interface **so-0/0/2.0**, and include the **detail** option. In the command output section for **Protocol inet**, the **Input Filters** field displays **limit-source-one-24**, indicating that the filter is applied to IPv4 traffic in the input direction:

```
user@host> show interfaces statistics so-0/0/2.0 detail
Logical interface so-0/0/2.0 (Index 79) (SNMP ifIndex 510) (Generation 149)
Flags: Hardware-Down Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
Protocol inet, MTU: 4470, Generation: 173, Route table: 0
Flags: Sendbcst-pkt-to-re, Protocol-Down
Input Filters: limit-source-one-24
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
Destination: 10.39/16, Local: 10.39.1.1, Broadcast: 10.39.255.255,
Generation: 163
```

#### *Displaying Prefix-Specific Actions Statistics for the Firewall Filter*

**Purpose** Verify the number of packets evaluated by the policer.

**Action** Use the **show firewall prefix-action-stats** filter *filter-name* prefix-action *name* operational mode command to display statistics about a prefix-specific action configured on a firewall filter.

As an option, you can use the **from set-index to set-index** command option to specify the starting and ending counter or policer to be displayed. A policer set is indexed from 0 through 65535.

The command output displays the specified filter name followed by a listing of the number of bytes and packets processed by each policer in the policer set.

For a term-specific policer, each policer in the set is identified as follows:

*prefix-specific-action-name-term-name-set-index*

For a filter-specific policer, each policer is identified in the command output as follows:

*prefix-specific-action-name-set-index*

Because the example prefix-specific action **psa-1Mbps-per-source-24-32-256** is referenced by only one term of the example filter **limit-source-one-24**, the example policer **1Mbps-policer** is configured as term-specific. In the **show firewall prefix-action-stats**



command output, the policer statistics are displayed as

**psa-1Mbps-per-source-24-32-256-one-0**, **psa-1Mbps-per-source-24-32-256-one-1**, and so on through **psa-1Mbps-per-source-24-32-256-one-255**.

```
user@host> show firewall prefix-action-stats filter limit-source-one-24 prefix-action
psa-1Mbps-per-source-24-32-256 from 0 to 9
Filter: limit-source-one-24
```

Counters:

| Name                                 | Bytes | Packets |
|--------------------------------------|-------|---------|
| psa-1Mbps-per-source-24-32-256-one-0 | 0     | 0       |
| psa-1Mbps-per-source-24-32-256-one-1 | 0     | 0       |
| psa-1Mbps-per-source-24-32-256-one-2 | 0     | 0       |
| psa-1Mbps-per-source-24-32-256-one-3 | 0     | 0       |
| psa-1Mbps-per-source-24-32-256-one-4 | 0     | 0       |
| psa-1Mbps-per-source-24-32-256-one-5 | 0     | 0       |
| psa-1Mbps-per-source-24-32-256-one-6 | 0     | 0       |
| psa-1Mbps-per-source-24-32-256-one-7 | 0     | 0       |
| psa-1Mbps-per-source-24-32-256-one-8 | 0     | 0       |
| psa-1Mbps-per-source-24-32-256-one-9 | 0     | 0       |

## Prefix-Specific Counting and Policing Configuration Scenarios

This topic covers the following information:

- [Prefix Length of the Action and Prefix Length of Addresses in Filtered Packets on page 81](#)
- [Scenario 1: Firewall Filter Term Matches on Multiple Addresses on page 82](#)
- [Scenario 2: Subnet Prefix Is Longer Than the Prefix in the Filter Match Condition on page 84](#)
- [Scenario 3: Subnet Prefix Is Shorter Than the Prefix in the Firewall Filter Match Condition on page 85](#)

### Prefix Length of the Action and Prefix Length of Addresses in Filtered Packets

[Table 8 on page 81](#) describes the relationship between the prefix length specified in the prefix-specific action and the prefix length of the addresses matched by the firewall filter term that references the prefix-specific action.

**Table 8: Summary of Prefix-Specific Action Scenarios**

| Counter and Policer Set                                                                                                              | Packet-Filtering Criteria             | Indexing of Instances |              |
|--------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|-----------------------|--------------|
| <b>Prefix-specific action scenario:</b><br>“ <a href="#">Example: Configuring Prefix-Specific Counting and Policing</a> ” on page 74 |                                       |                       |              |
| <i>source-prefix-length</i> = 32<br><i>subnet-prefix-length</i> = 24<br><br>Set size: 2^8 = 256<br>Instance numbers: 0 - 255         | <i>source-address</i> = 10.10.10.0/24 | Instance 0            | 10.10.10.0   |
|                                                                                                                                      |                                       | Instance 1:           | 10.10.10.1   |
|                                                                                                                                      |                                       | ...                   | ...          |
|                                                                                                                                      |                                       | Instance 255:         | 10.10.10.255 |
|                                                                                                                                      |                                       |                       |              |

Table 8: Summary of Prefix-Specific Action Scenarios (*continued*)

| Counter and Policer Set                                                                                                                             | Packet-Filtering Criteria                                                                                                                                                           | Indexing of Instances                                         |                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|-------------------------------|
| <b>Prefix-specific action scenario:</b><br>“Scenario 1: Firewall Filter Term Matches on Multiple Addresses” on page 82                              |                                                                                                                                                                                     |                                                               |                               |
| <i>source-prefix-length</i> = 32<br><i>subnet-prefix-length</i> = 24<br><br>Set size: 2^8 = 256<br>Instance numbers: 0 - 255                        | <i>source-address</i> = 10.10.10.0/24<br><br><i>source-address</i> = 10.11.0.0/16                                                                                                   | Instance 0                                                    | 10.10.10.0,<br>10.11.x.0      |
|                                                                                                                                                     |                                                                                                                                                                                     | Instance 1:                                                   | 10.10.10.1,<br>10.11.x.1      |
|                                                                                                                                                     |                                                                                                                                                                                     | ...                                                           | ...                           |
|                                                                                                                                                     |                                                                                                                                                                                     | Instance 255:                                                 | 10.10.10.255,<br>10.11.x.255  |
|                                                                                                                                                     |                                                                                                                                                                                     | For addresses in the /16 subnet, x ranges from 0 through 255. |                               |
| <b>Prefix-specific action scenario:</b><br>“Scenario 2: Subnet Prefix Is Longer Than the Prefix in the Filter Match Condition” on page 84           |                                                                                                                                                                                     |                                                               |                               |
| <i>source-prefix-length</i> = 32<br><i>subnet-prefix-length</i> = 25<br><br>Set size: 2^7 = 128<br>Instance numbers: 0 - 127                        | <i>source-address</i> = 10.10.10.0/24                                                                                                                                               | Instance 0                                                    | 10.10.10.0,<br>10.10.10.128   |
|                                                                                                                                                     |                                                                                                                                                                                     | Instance 1:                                                   | 10.10.10.1,<br>10.10.10.120   |
|                                                                                                                                                     |                                                                                                                                                                                     | ...                                                           | ...                           |
|                                                                                                                                                     |                                                                                                                                                                                     | Instance 127:                                                 | 10.10.10.255,<br>10.10.10.127 |
|                                                                                                                                                     |                                                                                                                                                                                     |                                                               |                               |
| <b>Prefix-specific action scenario:</b><br>“Scenario 3: Subnet Prefix Is Shorter Than the Prefix in the Firewall Filter Match Condition” on page 85 |                                                                                                                                                                                     |                                                               |                               |
| <i>source-prefix-length</i> = 32<br><i>subnet-prefix-length</i> = 24<br><br>Set size: 2^8 = 256<br>Instance numbers: 0 - 255                        | <i>source-address</i> = 10.10.10.0/25<br><br><b>NOTE:</b> Only packets with source addresses ranging from 10.10.10.0 through 10.10.10.127 are passed to the prefix-specific action. | Instance 0                                                    | 10.10.10.0                    |
|                                                                                                                                                     |                                                                                                                                                                                     | Instance 1:                                                   | 10.10.10.1                    |
|                                                                                                                                                     |                                                                                                                                                                                     | ...                                                           | ...                           |
|                                                                                                                                                     |                                                                                                                                                                                     | Instance 127:                                                 | 10.10.10.127                  |
|                                                                                                                                                     |                                                                                                                                                                                     | Instances 128 – 255: unused                                   |                               |

### Scenario 1: Firewall Filter Term Matches on Multiple Addresses

The complete example, [“Example: Configuring Prefix-Specific Counting and Policing” on page 74](#), shows the simplest case of prefix-specific actions, in which a single-term firewall

filter matches on one address with a prefix length that is the same as the subnet prefix length specified in the prefix-specific action. Unlike the example, this scenario describes a configuration in which a single-term firewall filter matches on two IPv4 source addresses. In addition, the additional condition matches on a source address with a prefix length that is different from the subnet prefix length defined in the prefix-specific action. In this case, the additional condition matches on the /16 subnet of the source address 10.11.0.0.



**NOTE:** Unlike packets that match the source address 10.10.10.0/24, packets that match the source address 10.11.0.0/16 are in a many-to-one correspondence with the instances in the counter and policer set.

The filter-matched packets that are passed to the prefix-specific action index into the counter and policer set in such a way that the counting and policing instances are shared by packets that contain source addresses across the 10.10.10.0/24 and 10.11.0.0/16 subnets as follows:

- The first counter and policer in the set are indexed by packets with source addresses 10.10.10.0 and 10.11.x.0, where x ranges from 0 through 255.
- The second counter and policer in the set are indexed by packets with source addresses 10.10.10.1 and 10.11.x.1, where x ranges from 0 through 255.
- The 256th (last) counter and policer in the set are indexed by packets with source addresses 10.10.10.255 and 10.11.x.255, where x ranges from 0 through 255.

The following configuration shows the statements for configuring the single-rate two-color policer, the prefix-specific action that references the policer, and the IPv4 standard stateless firewall filter that references the prefix-specific action:

```
[edit]
firewall {
  policer 1Mbps-policer {
    if-exceeding {
      bandwidth-limit 1m;
      burst-size-limit 63k;
    }
    then discard;
  }
  family inet {
    prefix-action psa-1Mbps-per-source-24-32-256 {
      policer 1Mbps-policer;
      subnet-prefix-length 24;
      source-prefix-length 32;
    }
    filter limit-source-two-24-16 {
      term one {
        from {
          source-address {
            10.10.10.0/24;
            10.11.0.0/16;
          }
        }
      }
    }
  }
}
```

```

        then prefix-action psa-1Mbps-per-source-24-32-256;
    }
}
}
}
interfaces {
  so-0/0/2 {
    unit 0 {
      family inet {
        filter {
          input limit-source-two-24-16;
        }
        address 10.39.1.1/16;
      }
    }
  }
}
}

```

### Scenario 2: Subnet Prefix Is Longer Than the Prefix in the Filter Match Condition

The complete example, “[Example: Configuring Prefix-Specific Counting and Policing](#)” on [page 74](#), shows the simplest case of prefix-specific actions, in which the single-term firewall filter matches on one address with a prefix length that is the same as the subnet prefix length specified in the prefix-specific action. Unlike the example, this scenario describes a configuration in which the prefix-specific action defines a subnet prefix length that is longer than the prefix of the source address matched by the firewall filter. In this case, the prefix-specific action defines a subnet-prefix value of **25**, while the firewall filter matches on a source address in the **/24** subnet.



**NOTE:** The firewall filter passes the prefix-specific action packets with source addresses that range from 10.10.10.0 through 10.10.10.255, while the prefix-specific action specifies a set of only 128 counters and policers, numbered from 0 through 127.

The filter-matched packets that are passed to the prefix-specific action index into the counter and policer set in such a way that the counting and policing instances are shared by packets that contain either of two source addresses within the **10.10.10.0/24** subnet:

- The first counter and policer in the set are indexed by packets with source addresses **10.10.10.0** and **10.10.10.128**.
- The second counter and policer in the set are indexed by packets with source addresses **10.10.10.1** and **10.10.10.129**.
- The 128th (last) counter and policer in the set are indexed by packets with source addresses **10.10.10.127** and **10.10.10.255**.

The following configuration shows the statements for configuring the single-rate two-color policer, the prefix-specific action that references the policer, and the IPv4 standard stateless firewall filter that references the prefix-specific action:

[edit]

```

firewall {
  policer 1Mbps-policer {
    if-exceeding {
      bandwidth-limit 1m;
      burst-size-limit 63k;
    }
    then discard;
  }
  family inet {
    prefix-action psa-1Mbps-per-source-25-32-128 {
      policer 1Mbps-policer;
      subnet-prefix-length 25;
      source-prefix-length 32;
    }
    filter limit-source-one-24 {
      term one {
        from {
          source-address {
            10.10.10.0/24;
          }
        }
        then prefix-action psa-1Mbps-per-source-25-32-128;
      }
    }
  }
}
interfaces {
  so-0/0/2 {
    unit 0 {
      family inet {
        filter {
          input limit-source-one-24;
        }
        address 10.39.1.1/16;
      }
    }
  }
}

```

### Scenario 3: Subnet Prefix Is Shorter Than the Prefix in the Firewall Filter Match Condition

The complete example, [“Example: Configuring Prefix-Specific Counting and Policing” on page 74](#), shows the simplest case of prefix-specific actions, in which the single-term firewall filter matches on one address with a prefix length that is the same as the subnet prefix length specified in the prefix-specific action. Unlike the example, this scenario describes a configuration in which the prefix-specific action defines a subnet prefix length that is shorter than the prefix of the source address matched by the firewall filter. In this case, the filter term matches on the /25 subnet of the source address 10.10.10.0.



**NOTE:** The firewall filter passes the prefix-specific action only packets with source addresses that range from 10.10.10.0 through 10.10.10.127, while the prefix-specific action specifies a set of 256 counters and policers, numbered from 0 through 255.

The matched packets that are passed to the prefix-specific action index into the lower half of the counter and policer set only:

- The first counter and policer in the set are indexed by packets with source address **10.10.10.0**.
- The second counter and policer in the set are indexed by packets with source address **10.10.10.1** and **10.10.10.129**.
- The 128th counter and policer in the set are indexed by packets with source address **10.10.10.127**.
- The upper half of the set (instances numbered from 128 through 255) are not indexed by packets passed to the prefix-specific action from this particular firewall filter.

The following configuration shows the statements for configuring the single-rate two-color policer, the prefix-specific action that references the policer, and the IPv4 standard stateless firewall filter that references the prefix-specific action:

```
[edit]
firewall {
  policer 1Mbps-policer {
    if-exceeding {
      bandwidth-limit 1m;
      burst-size-limit 63k;
    }
    then discard;
  }
  family inet {
    prefix-action psa-1Mbps-per-source-24-32-256 {
      policer 1Mbps-policer;
      subnet-prefix-length 24;
      source-prefix-length 32;
    }
    filter limit-source-one-25 {
      term one {
        from {
          source-address {
            10.10.10.0/25;
          }
        }
        then prefix-action psa-1Mbps-per-source-24-32-256;
      }
    }
  }
}
interfaces {
  so-0/0/2 {
```

```
unit 0 {  
  family inet {  
    filter {  
      input limit-source-one-25;  
    }  
    address 10.39.1.1/16;  
  }  
}
```

- Related Documentation**
- [Statement Hierarchy for Configuring Policers on page 13](#)
  - [Two-Color Policer Configuration Overview on page 15](#)
  - [Guidelines for Applying Traffic Policers on page 24](#)

## Multifield Classification

---

- [Multifield Classification Overview on page 87](#)
- [Multifield Classification Requirements and Restrictions on page 89](#)
- [Multifield Classification Limitations on M Series Routers on page 90](#)
- [Example: Configuring Multifield Classification on page 92](#)

### Multifield Classification Overview

This topic covers the following information:

- [Forwarding Classes and PLP Levels on page 87](#)
- [Multifield Classification and BA Classification on page 88](#)
- [Multifield Classification Used In Conjunction with Policers on page 88](#)

#### Forwarding Classes and PLP Levels

---

You can configure the Junos OS class of service (CoS) features to classify incoming traffic by associating each packet with a forwarding class, a packet loss priority (PLP) level, or both:

- Based on the associated forwarding class, each packet is assigned to an output queue, and the router services the output queues according to the associated scheduling you configure.
- Based on the associated PLP, each packet carries a lower or higher likelihood of being dropped if congestion occurs. The CoS random early detection (RED) process uses the drop probability configuration, output queue fullness percentage, and packet PLP to drop packet as needed to control congestion at the output stage.

## Multifield Classification and BA Classification

---

The Junos OS supports two general types of packet classification: behavior aggregate (BA) classification and multifield classification:

- BA classification, or CoS value traffic classification, refers to a method of packet classification that uses a CoS configuration to set the forwarding class or PLP of a packet based on the *CoS value* in the IP packet header. The CoS value examined for BA classification purposes can be the Differentiated Services code point (DSCP) value, DSCP IPv6 value, IP precedence value, MPLS EXP bits, and IEEE 802.1p value. The default classifier is based on the IP precedence value.
- Multifield classification refers to a method of packet classification that uses a standard stateless firewall filter configuration to set the forwarding class or PLP for each packet entering or exiting the interface based on *multiple fields* in the IP packet header, including the DSCP value (for IPv4 only), the IP precedence value, the MPLS EXP bits, and the IEEE 802.1p bits. Multifield classification commonly matches on IP address fields, the IP protocol type field, or the port number in the UDP or TCP pseudoheader field. Multifield classification is used instead of BA classification when you need to classify packets based on information in the packet information other than the CoS values only.

With multifield classification, a firewall filter term can specify the packet classification actions for matching packets through the use of the **forwarding-class** *class-name* or **loss-priority** (**high** | **medium-high** | **medium-low** | **low**) nonterminating actions in the term's **then** clause. For more information about these actions, see .



.....

**NOTE:** BA classification of a packet can be overridden by the stateless firewall filter actions **forwarding-class** and **loss-priority**.

.....

## Multifield Classification Used In Conjunction with Policers

---

To configure multifield classification in conjunction with rate limiting, a firewall filter term can specify the packet classification actions for matching packets through the use of a **policer** nonterminating action that references a single-rate two-color policer.

When multifield classification is configured to perform classification through a policer, the filter-matched packets in the traffic flow are rate-limited to the policer-specified traffic limits. Packets in a conforming flow of filter-matched packets are implicitly set to a **low** PLP. Packets in a nonconforming traffic flow can be discarded, or the packets can be set to a specified forwarding class, set to a specified PLP level, or both, depending on the type of policer and how the policer is configured to handle nonconforming traffic.





**NOTE:** Before you apply a firewall filter that performs multifield classification and also a policer to the same logical interface and for the same traffic direction, make sure that you consider the order of policer and firewall filter operations.

As an example, consider the following scenario:

- You configure a firewall filter that performs multifield classification (acts on matched packets by setting the forwarding class, the PLP, or both) based on the packet's existing forwarding class or PLP. You apply the firewall filter at the input of a logical interface.
- You also configure a single-rate two-color policer that acts on a red traffic flow by re-marking (setting the forwarding class, the PLP, or both) rather than discarding those packets. You apply the policer as an interface policer at the input of the same logical interface to which you apply the firewall filter.

Because of the order of policer and firewall operations, the input policer is executed before the input firewall filter. This means that the multifield classification specified by the firewall filter is performed on input packets that have already been re-marked once by policing actions. Consequently, any input packet that matches the conditions specified in a firewall filter term is then subject to a second re-marking according to the forwarding-class or loss-priority nonterminating actions also specified in that term.

## Multifield Classification Requirements and Restrictions

This topic covers the following information:

- [Supported Platforms on page 89](#)
- [CoS Tricolor Marking Requirement on page 90](#)
- [Restrictions on page 90](#)

### Supported Platforms

The **loss-priority** firewall filter action is supported on the following routing platforms only:

- M7i and M10i routers with the Enhanced CFEB (CFEB-E)
- M120 and M320 routers
- MX Series routers
- T Series routers with Enhanced II Flexible PIC Concentrators (FPCs)

### CoS Tricolor Marking Requirement

---

The **loss-priority** firewall filter action has platform-specific requirements dependencies on the CoS tricolor marking feature, as defined in RFC 2698:

- On an M320 router, you cannot commit a configuration that includes the **loss-priority** firewall filter action unless you enable the CoS tricolor marking feature.
- On all routing platforms that support the **loss-priority** firewall filter action, you cannot set the **loss-priority** firewall filter action to **medium-low** or **medium-high** unless you enable the CoS tricolor marking feature. .

To enable the CoS tricolor marking feature, include the **tri-color** statement at the **[edit class-of-service]** hierarchy level.

### Restrictions

---

You cannot configure the **loss-priority** and **three-color-policer** nonterminating actions for the same firewall filter term. These two nonterminating actions are mutually exclusive.

## Multifield Classification Limitations on M Series Routers

This topic covers the following information:

- [Problem: Output-Filter Matching on Input-Filter Classification on page 90](#)
- [Workaround: Configure All Actions in the Ingress Filter on page 91](#)

### Problem: Output-Filter Matching on Input-Filter Classification

---

On M Series routers (except M120 routers), you cannot classify packets with an output filter match based on the ingress classification that is set with an input filter applied to the same IPv4 logical interface.

For example, in the following configuration, the filter called **ingress** assigns all incoming IPv4 packets to the **expedited-forwarding** class. The filter called **egress** counts all packets that were assigned to the **expedited-forwarding** class in the **ingress** filter. This configuration does not work on most M Series routers. It works on all other routing platforms, including M120 routers, MX Series routers, and T Series routers.

```
[edit]
user@host # show firewall
family inet {
  filter ingress {
    term 1 {
      then {
        forwarding-class expedited-forwarding;
        accept;
      }
    }
    term 2 {
      then accept;
    }
  }
  filter egress {
```

```

term 1 {
  from {
    forwarding-class expedited-forwarding;
  }
  then count ef;
}
term 2 {
  then accept;
}
}
}

```

```

[edit]
user@host# show interfaces
ge-1/2/0 {
  unit 0 {
    family inet {
      filter {
        input ingress;
        output egress;
      }
    }
  }
}

```

### Workaround: Configure All Actions in the Ingress Filter

As a workaround, you can configure all of the actions in the ingress filter.

```

user@host # show firewall
family inet {
  filter ingress {
    term 1 {
      then {
        forwarding-class expedited-forwarding;
        accept;
        count ef;
      }
    }
    term 2 {
      then accept;
    }
  }
}

```

```

[edit]
user@host# show interfaces
ge-1/2/0 {
  unit 0 {
    family inet {
      filter {
        input ingress;
      }
    }
  }
}

```

## Example: Configuring Multifield Classification

This example shows how to configure multifield classification of IPv4 traffic by using firewall filter actions and two firewall filter policers.

- [Requirements on page 92](#)
- [Overview on page 93](#)
- [Configuration on page 94](#)
- [Verification on page 98](#)

### Requirements

---

Before you begin, make sure that your environment supports the features shown in this example:

1. The **loss-priority** firewall filter action must be supported on the router and configurable to all four values.
  - a. To be able to set a **loss-priority** firewall filter action, configure this example on logical interface **ge-1/2/0.0** on one of the following routing platforms:
    - MX Series router
    - M120 or M320 router
    - M7i or M10i router with the Enhanced CFEB (CFEB-E)
    - T Series router with Enhanced II Flexible PIC Concentrator (FPC)
  - b. To be able to set a **loss-priority** firewall filter action to **medium-low** or **medium-high**, make sure that the CoS tricolor marking feature is enabled. To enable the CoS tricolor marking feature, include the **tri-color** statement at the **[edit class-of-service]** hierarchy level.
2. The **expedited-forwarding** and **assured-forwarding** forwarding classes must be scheduled on the underlying physical interface **ge-1/2/0**.
  - a. Make sure that the following forwarding classes are assigned to output queues:
    - **expedited-forwarding**
    - **assured-forwarding**

Forwarding-class assignments are configured at the **[edit class-of-service forwarding-classes queue *queue-number*]** hierarchy level.



**NOTE:** You cannot commit a configuration that assigns the same forwarding class to two different queues.

---

- b. Make sure that the output queues to which the forwarding classes are assigned are associated with schedulers. A scheduler defines the amount of interface bandwidth assigned to the queue, the size of the memory buffer allocated for storing packets, the priority of the queue, and the random early detection (RED) drop profiles associated with the queue.
  - You configure output queue schedulers at the **[edit class-of-service schedulers]** hierarchy level.
  - You associate output queue schedulers with forwarding classes by means of a scheduler map that you configure at the **[edit class-of-service scheduler-maps map-name]** hierarchy level.
- c. Make sure that output-queue scheduling is applied to the physical interface **ge-1/2/0**.

You apply a scheduler map to a physical interface at the **[edit class-of-service interfaces ge-1/2/0 scheduler-map map-name]** hierarchy level.

## Overview

In this example, you apply multifield classification to the input IPv4 traffic at a logical interface by using stateless firewall filter actions and two firewall filter policers that are referenced from the firewall filter. Based on the source address field, packets are either set to the **low** loss priority or else policed. Neither of the policers discards nonconforming traffic. Packets in nonconforming flows are marked for a specific forwarding class (**expedited-forwarding** or **assured-forwarding**), set to a specific loss priority, and then transmitted.



**NOTE:** Single-rate two-color policers always transmit packets in a conforming traffic flow after implicitly setting a **low** loss priority.

## Topology

In this example, you apply multifield classification to the IPv4 traffic on logical interface **ge-1/2/0.0**. The classification rules are specified in the IPv4 stateless firewall filter **mfc-filter** and two single-rate two-color policers, **ef-policer** and **af-policer**.

The IPv4 standard stateless firewall filter **mfc-filter** defines three filter terms:

- **isp1-customers**—The first filter term matches packets with the source address 10.1.1.0/24 or 10.1.2.0/24. Matched packets are assigned to the **expedited-forwarding** forwarding class and set to the **low** loss priority.
- **isp2-customers**—The second filter term matches packets with the source address 10.1.3.0/24 or 10.1.4.0/24. Matched packets are passed to **ef-policer**, a policer that rate-limits traffic to a bandwidth limit of 300 Kbps with a burst-size limit of 50 KB. This policer specifies that packets in a nonconforming flow are marked for the **expedited-forwarding** forwarding class and set to the **high** loss priority.

- **other-customers**—The third and final filter term passes all other packets to **af-policer**, a policer that rate-limits traffic to a bandwidth limit of 300 Kbps and a burst-size limit of 50 KB (the same traffic limits as defined by **ef-policer**). This policer specifies that packets in a nonconforming flow are marked for the **assured-forwarding** forwarding class and set to the **medium-high** loss priority.

## Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see [“Using the CLI Editor in Configuration Mode” on page 215](#).

To configure this example, perform the following tasks:

- [Configuring Policers to Rate-Limit Expedited-Forwarding and Assured-Forwarding Traffic on page 94](#)
- [Configuring a Multifield Classification Filter That Also Applies Policing on page 95](#)
- [Applying Multifield Classification Filtering and Policing to the Logical Interface on page 97](#)

### CLI Quick Configuration

To quickly configure this example, copy the following configuration commands into a text file, remove any line breaks, and then paste the commands into the CLI at the **[edit]** hierarchy level.

```
set firewall policer ef-policer if-exceeding bandwidth-limit 300k
set firewall policer ef-policer if-exceeding burst-size-limit 50k
set firewall policer ef-policer then loss-priority high
set firewall policer ef-policer then forwarding-class expedited-forwarding
set firewall policer af-policer if-exceeding bandwidth-limit 300k
set firewall policer af-policer if-exceeding burst-size-limit 50k
set firewall policer af-policer then loss-priority high
set firewall policer af-policer then forwarding-class assured-forwarding
set firewall family inet filter mfc-filter term isp1-customers from source-address 10.1.1.0/24
set firewall family inet filter mfc-filter term isp1-customers from source-address 10.1.2.0/24
set firewall family inet filter mfc-filter term isp1-customers then loss-priority low
set firewall family inet filter mfc-filter term isp1-customers then forwarding-class
  expedited-forwarding
set firewall family inet filter mfc-filter term isp2-customers from source-address
  10.1.3.0/24
set firewall family inet filter mfc-filter term isp2-customers from source-address
  10.1.4.0/24
set firewall family inet filter mfc-filter term isp2-customers then policer ef-policer
set firewall family inet filter mfc-filter term other-customers then policer af-policer
set interfaces ge-1/2/0 unit 0 family inet address 192.168.1.1/24
set interfaces ge-1/2/0 unit 0 family inet filter input mfc-filter
```

### Configuring Policers to Rate-Limit Expedited-Forwarding and Assured-Forwarding Traffic

#### Step-by-Step Procedure

To configure policers to rate-limit expedited-forwarding and assured-forwarding traffic:

1. Define traffic limits for expedited-forwarding traffic.

```
[edit]
user@host# edit firewall policer ef-policer
```

```
[edit firewall policer ef-policer]
user@host# set if-exceeding bandwidth-limit 300k
user@host# set if-exceeding burst-size-limit 50k
user@host# set then loss-priority high
user@host# set then forwarding-class expedited-forwarding
```

2. Configure a policer for assured-forwarding traffic.

```
[edit firewall policer ef-policer]
user@host# up
```

```
[edit firewall]
user@host# edit policer af-policer
```

```
[edit firewall policer af-policer]
user@host# set if-exceeding bandwidth-limit 300k
user@host# set if-exceeding burst-size-limit 50k
user@host# set then loss-priority high
user@host# set then forwarding-class assured-forwarding
```

**Results** Confirm the configuration of the policer by entering the **show firewall** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show firewall
policer af-policer {
  if-exceeding {
    bandwidth-limit 300k;
    burst-size-limit 50k;
  }
  then {
    loss-priority high;
    forwarding-class assured-forwarding;
  }
}
policer ef-policer {
  if-exceeding {
    bandwidth-limit 300k;
    burst-size-limit 50k;
  }
  then {
    loss-priority high;
    forwarding-class expedited-forwarding;
  }
}
```

### *Configuring a Multifield Classification Filter That Also Applies Policing*

**Step-by-Step Procedure** To configure a multifield classification filter that additionally applies policing:

1. Enable configuration of a firewall filter term for IPv4 traffic.

```
[edit]
user@host# edit firewall family inet filter mfc-filter
```

2. Configure the first term to match on source addresses and then classify the matched packets.

```
[edit firewall family inet filter mfc-filter]
user@host# set term isp1-customers from source-address 10.1.1.0/24
user@host# set term isp1-customers from source-address 10.1.2.0/24
user@host# set term isp1-customers then loss-priority low
user@host# set term isp1-customers then forwarding-class expedited-forwarding
```

3. Configure the second term to match on different source addresses and then police the matched packets.

```
[edit firewall family inet filter mfc-filter]
user@host# set term isp2-customers from source-address 10.1.3.0/24
user@host# set term isp2-customers from source-address 10.1.4.0/24
user@host# set term isp2-customers then policer ef-policer
```

4. Configure the third term to police all other packets to a different set of traffic limits and actions.

```
[edit firewall family inet filter mfc-filter]
user@host# set term other-customers then policer af-policer
```

**Results** Confirm the configuration of the filter by entering the **show firewall** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show firewall
family inet {
  filter mfc-filter {
    term isp1-customers {
      from {
        source-address 10.1.1.0/24;
        source-address 10.1.2.0/24;
      }
      then {
        loss-priority low;
        forwarding-class expedited-forwarding;
      }
    }
    term isp2-customers {
      from {
        source-address 10.1.3.0/24;
        source-address 10.1.4.0/24;
      }
      then {
        policer ef-policer;
      }
    }
    term other-customers {
      then {
        policer af-policer;
      }
    }
  }
}
```



```

policer af-policer {
  if-exceeding {
    bandwidth-limit 300k;
    burst-size-limit 50k;
  }
  then discard;
}
policer ef-policer {
  if-exceeding {
    bandwidth-limit 200k;
    burst-size-limit 50k;
  }
  then {
    loss-priority high;
    forwarding-class expedited-forwarding;
  }
}

```

### *Applying Multifield Classification Filtering and Policing to the Logical Interface*

#### **Step-by-Step Procedure**

To apply multifield classification filtering and policing to the logical interface:

1. Enable configuration of IPv4 on the logical interface.

```

[edit]
user@host# edit interfaces ge-1/2/0 unit 0 family inet

```

2. Configure an IP address for the logical interface.

```

[edit interfaces ge-1/2/0 unit 0 family inet ]
user@host# set address 192.168.1.1/24

```

3. Apply the firewall filter to the logical interface input.

```

[edit interfaces ge-1/2/0 unit 0 family inet ]
user@host# set filter input mfc-filter

```



**NOTE:** Because the policer is executed before the filter, if an input policer is also configured on the logical interface, it cannot use the forwarding class and PLP of a multifield classifier associated with the interface.

**Results** Confirm the configuration of the interface by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```

[edit]
user@host# show interfaces
ge-1/2/0 {
  unit 0 {
    family inet {
      filter {
        input mfc-filter;
      }
      address 192.168.1.1/24;
    }
  }
}

```

```

    }
  }
}

```

If you are done configuring the device, enter **commit** from configuration mode.

### Verification

Confirm that the configuration is working properly.

#### *Displaying the Number of Packets Processed by the Policer at the Logical Interface*

**Purpose** Verify the traffic flow through the logical interface and that the policer is evaluated when packets are received on the logical interface.

**Action** Use the **show firewall** operational mode command for the filter you applied to the logical interface.

```

user@host> show firewall filter rate-limit-in
Filter: rate-limit-in
Policers:
Name                               Packets
ef-policer-isp2-customers          32863
af-policer-other-customers         3870

```

The command output lists the policers applied by the firewall filter **rate-limit-in**, and the number of packets that matched the filter term.



**NOTE:** The packet count includes the number of out-of-specification (out-of-spec) packet counts, not all packets policed by the policer.

The policer name is displayed concatenated with the name of the firewall filter term in which the policer is referenced as an action.

- Related Documentation**
- “Standard Firewall Filter Nonterminating Actions” in the *Junos OS Firewall Filter and Policer Configuration Guide*
  - [Order of Policer and Firewall Filter Operations on page 10](#)
  - [Statement Hierarchy for Configuring Policers on page 13](#)
  - [Two-Color Policer Configuration Overview on page 15](#)
  - [Guidelines for Applying Traffic Policers on page 24](#)
  - “Junos CoS Components” in the *Junos OS Class of Service Configuration Guide*
  - “BA Classifier Overview” in the *Junos OS Class of Service Configuration Guide*
  - “Overview of Forwarding Classes” in the *Junos OS Class of Service Configuration Guide*
  - “Default Forwarding Classes” in the *Junos OS Class of Service Configuration Guide*
  - “RED Drop Profiles Overview” in the *Junos OS Class of Service Configuration Guide*

- **tri-color** statement in the *Junos OS Class of Service Configuration Guide*

## --- Policer Overhead to Account for Rate Shaping in the Traffic Manager

- [Policer Overhead to Account for Rate Shaping Overview on page 99](#)
- [Example: Configuring Policer Overhead to Account for Rate Shaping on page 99](#)

### Policer Overhead to Account for Rate Shaping Overview

If you configure ingress or egress traffic-shaping overhead values for an interface, the traffic manager cannot apply these values to any rate-limiting also applied to the interface. To enable the router to account for the additional Ethernet frame length when policing actions are being determined, you must configure the ingress or egress overhead values for policers separately.



**NOTE:** When a policer overhead value is changed, the PIC or DPC goes offline and then comes back online.

For Gigabit Ethernet Intelligent Queuing 2 (IQ2) and Enhanced IQ2 (IQ2E) PICs or interfaces on Dense Port Concentrators (DPCs) in MX Series routers, you can control the rate of traffic that passes through all interfaces on the PIC or DPC by configuring a *policer overhead*. You can configure a policer ingress overhead and a policer egress overhead, each with values from 0 through 255 bytes. The policer overhead values are added to the length of the final Ethernet frame when determining ingress and egress policer actions.

### Example: Configuring Policer Overhead to Account for Rate Shaping

This example shows how to configure overhead values for policers when rate-shaping overhead is configured.

- [Requirements on page 99](#)
- [Overview on page 100](#)
- [Configuration on page 100](#)
- [Verification on page 106](#)

#### Requirements

---

Before you begin, make sure that interface for which you are applying ingress or egress policer overhead is hosted on one of the following:

- Gigabit Ethernet IQ2 PIC
- IQ2E PIC
- DPCs in MX Series routers

## Overview

This example shows how to configure policer overhead values for all physical interfaces on a supported PIC or MPC so that the rate shaping value configured on a logical interface is accounted for in any policing on that logical interface.

## Topology

The router hosts a Gigabit Ethernet IQ2 PIC, installed in PIC location 3 of the Flexible PIC Concentrator (FPC) in slot number 1. The physical interface on port 1 on that PIC is configured to receive traffic on logical interface 0 and send it back out on logical interface 1. Class-of-service scheduling includes 100 Mbps of traffic rate-shaping overhead for the output traffic. A policer egress overhead of 100 bytes is configured on the entire PIC so that, for any policers applied to the output traffic, 100 bytes are added to the final Ethernet frame length when determining ingress and egress policer actions.



### NOTE:

Traffic rate-shaping and corresponding policer overhead are configured separately:

- You configure rate shaping at the `[edit class-of-service interfaces interface-name unit unit-number]` hierarchy level.
- You configure policer overhead at the `[edit chassis fpc slot-number pic pic-number]` hierarchy level.

When a policer overhead value is changed, the PIC or DPC goes offline and then comes back online.

## Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see [“Using the CLI Editor in Configuration Mode” on page 215](#).

To configure this example, perform the following tasks:

- [Configuring the Logical Interfaces on page 101](#)
- [Configuring Traffic Rate-Shaping on the Logical Interface That Carries Output Traffic on page 102](#)
- [Configuring Policer Overhead on the PIC or MPC That Hosts the Rate-Shaped Logical Interface on page 104](#)
- [Applying a Policer to the Logical Interface That Carries Input Traffic on page 105](#)

### CLI Quick Configuration

To quickly configure this example, copy the following configuration commands into a text file, remove any line breaks, and then paste the commands into the CLI at the `[edit]` hierarchy level.

```
set interfaces ge-1/3/1 per-unit-scheduler
set interfaces ge-1/3/1 vlan-tagging
set interfaces ge-1/3/1 unit 0 vlan-id 100
```

```

set interfaces ge-1/3/1 unit 0 family inet address 10.10.10.1/30
set interfaces ge-1/3/1 unit 1 vlan-id 101
set interfaces ge-1/3/1 unit 1 family inet address 20.20.20.1/30 arp 20.20.20.2 mac
  00:00:11:22:33:44
set class-of-service schedulers be transmit-rate percent 5
set class-of-service schedulers ef transmit-rate percent 30
set class-of-service schedulers af transmit-rate percent 30
set class-of-service schedulers nc transmit-rate percent 35
set class-of-service scheduler-maps my-map forwarding-class best-effort scheduler be
set class-of-service scheduler-maps my-map forwarding-class expedited-forwarding
  scheduler ef
set class-of-service scheduler-maps my-map forwarding-class network-control scheduler
  nc
set class-of-service scheduler-maps my-map forwarding-class assured-forwarding
  scheduler af
set class-of-service interfaces ge-1/3/1 unit 1 scheduler-map my-map
set class-of-service interfaces ge-1/3/1 unit 1 shaping-rate 100m
set firewall policer 500Kbps logical-interface-policer
set firewall policer 500Kbps if-exceeding bandwidth-limit 500k
set firewall policer 500Kbps if-exceeding burst-size-limit 625k
set firewall policer 500Kbps then discard
set chassis fpc 1 pic 3 ingress-policer-overhead 100
set chassis fpc 1 pic 3 egress-policer-overhead 100
set interfaces ge-1/3/1 unit 0 family inet policer input 500Kbps

```

### Configuring the Logical Interfaces

#### Step-by-Step Procedure

To configure the logical interfaces:

1. Enable configuration of the interface

```

[edit]
user@host# edit interfaces ge-1/3/1

```

2. Enable multiple queues for each logical interface (so that you can associate an output scheduler with each logical interface).

```

[edit interfaces ge-1/3/1]
user@host# set per-unit scheduler
user@host# set vlan-tagging

```



**NOTE:** For Gigabit Ethernet IQ2 PICs only, use the shared-scheduler statement to enable shared schedulers and shapers on a physical interface.

3. Configure logical interface **ge-1/3/1.0**.

```

[edit interfaces ge-1/3/1]
user@host# set unit 0 vlan-id 100
user@host# set unit 0 family inet address 10.10.10.1/30

```

4. Configure logical interface **ge-1/3/1.1**.

```

[edit interfaces ge-1/3/1]

```

```
user@host# set unit 1 vlan-id 101
user@host# set unit 1 family inet address 20.20.20.1/30 arp 20.20.20.2 mac
00:00:11:22:33:44
```

**Results** Confirm the configuration of the interfaces by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show interfaces
ge-1/3/1 {
  per-unit-scheduler;
  vlan-tagging;
  unit 0 {
    vlan-id 100;
    family inet {
      address 10.10.10.1/30;
    }
  }
  unit 1 {
    vlan-id 101;
    family inet {
      address 20.20.20.1/30 {
        arp 20.20.20.2 mac 00:00:11:22:33:44;
      }
    }
  }
}
```

### *Configuring Traffic Rate-Shaping on the Logical Interface That Carries Output Traffic*

**Step-by-Step Procedure** To configure traffic rate-shaping on the logical interface that carries output traffic:

1. Enable configuration of class-of-service features.

```
[edit]
user@host# edit class-of-service
```

2. Configure packet scheduling on logical interface **ge-1/3/1.0**.
  - a. Configure schedulers that specify the percentage of transmission capacity.

```
[edit class-of-service]
user@host# edit schedulers
```

```
[edit class-of-service schedulers]
user@host# set be transmit-rate percent 5
user@host# set ef transmit-rate percent 30
user@host# set af transmit-rate percent 30
user@host# set nc transmit-rate percent 35
```

A percentage of zero drops all packets in the queue. When the **rate-limit** option is specified, the transmission rate is limited to the rate-controlled amount. In contrast with the **exact** option, a scheduler with the **rate-limit** option shares unused bandwidth above the rate-controlled amount.

- b. Configure a scheduler map to associate each scheduler with a forwarding class.

```
[edit class-of-service]
user@host# edit scheduler-maps my-map

[edit class-of-service scheduler-maps my-map]
user@host# set forwarding-class best-effort scheduler be
user@host# set forwarding-class expedited-forwarding scheduler ef
user@host# set forwarding-class network-control scheduler nc
user@host# set forwarding-class assured-forwarding scheduler af
```

- c. Associate the scheduler map with logical interface **ge-1/3/1.0**.

```
[edit class-of-service]
user@host# edit interfaces ge-1/3/1 unit 1

[edit class-of-service interfaces ge-1/3/1 unit 1]
user@host# set scheduler-map my-map
```

3. Configure 100 Mbps of traffic rate-shaping overhead on logical interface **ge-1/3/1.1**.

```
[edit class-of-service interfaces ge-1/3/1 unit 1]
user@host# set shaping-rate 100
```

Alternatively, you can configure a shaping rate for a logical interface and oversubscribe the physical interface by including the **shaping-rate** statement at the **[edit class-of-service traffic-control-profiles]** hierarchy level. With this configuration approach, you can independently control the delay-buffer rate.

**Results** Confirm the configuration of the class-of-service features (including the 100 Mbp of shaping of the egress traffic) by entering the **show class-of-service** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show class-of-service
interfaces {
  ge-1/3/1 {
    unit 1 {
      scheduler-map my-map;
      shaping-rate 100m;
    }
  }
}
scheduler-maps {
  my-map {
    forwarding-class best-effort scheduler be;
    forwarding-class expedited-forwarding scheduler ef;
    forwarding-class network-control scheduler nc;
    forwarding-class assured-forwarding scheduler af;
  }
}
schedulers {
  be {
    transmit-rate percent 5;
  }
}
```

```

ef {
    transmit-rate percent 30;
}
af {
    transmit-rate percent 30;
}
nc {
    transmit-rate percent 35;
}
}

```

### *Configuring Policer Overhead on the PIC or MPC That Hosts the Rate-Shaped Logical Interface*

#### **Step-by-Step Procedure**

To configure policer overhead on the PIC or MPC that hosts the rate-shaped logical interface:

1. Enable configuration of the supported PIC or MPC.

```

[edit]
user@host# set chassis fpc 1 pic 3

```

2. Configure 100 bytes of policer overhead on the supported PIC or MPC.

```

[edit]
user@host# set ingress-policer-overhead 100
user@host# set egress-policer-overhead 100

```



**NOTE:** These values are added to the length of the final Ethernet frame when determining ingress and egress policer actions for all physical interfaces on the PIC or MPC.

You can specify policer overhead with values from 0 through 255 bytes.

**Results** Confirm the configuration of the policer overhead on the physical interface to account for rate-shaping by entering the **show chassis** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```

[edit]
user@host# show chassis
chassis {
  fpc 1 {
    pic 3 {
      egress-policer-overhead 100;
      ingress-policer-overhead 100;
    }
  }
}

```



*Applying a Policer to the Logical Interface That Carries Input Traffic***Step-by-Step Procedure**

To apply a policer to the logical interface that carries input traffic:

1. Configure the logical interface (aggregate) policer.

```
[edit]
user@host# edit firewall policer 500Kbps

[edit firewall policer 500Kbps]
user@host# set logical-interface-policer
user@host# set if-exceeding bandwidth-limit 500k
user@host# set if-exceeding burst-size-limit 625k
user@host# set then discard
```

2. Apply the policer to Layer 3 input on the IPv4 logical interface.

```
[edit]
user@host# set interfaces ge-1/3/1 unit 0 family inet policer input 500Kbps
```



**NOTE:** The 100 Mbps policer overhead is added to the length of the final Ethernet frame when determining ingress and egress policer actions,

**Results** Confirm the configuration of the policer with rate-shaping overhead by entering the **show firewall** and **show interfaces** configuration mode commands. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show firewall
policer 500Kbps {
  logical-interface-policer;
  if-exceeding {
    bandwidth-limit 500k;
    burst-size-limit 625k;
  }
  then discard;
}
[edit]
user@host# show interfaces
ge-1/3/1 {
  per-unit-scheduler;
  vlan-tagging;
  unit 0 {
    vlan-id 100;
    layer2-policer {
      input-policer 500Kbps;
    }
    family inet {
      address 10.10.10.1/30;
    }
  }
  unit 0 {
```

```
vlan-id 101;
family inet {
    address 20.20.20.1/30 {
        arp 20.20.20.2 mac 00:00:11:22:33:44;
    }
}
}
```

If you are done configuring the device, enter **commit** from configuration mode.

---

### Verification

Confirm that the configuration is working properly.

- [Displaying Traffic Statistics and Policers for the Logical Interface on page 106](#)
- [Displaying Statistics for the Policer on page 106](#)

#### *Displaying Traffic Statistics and Policers for the Logical Interface*

**Purpose** Verify the traffic flow through the logical interface and that the policer is evaluated when packets are received on the logical interface.

**Action** Use the **show interfaces** operational mode command for logical interface **ge-1/3/1.0**, and include the **detail** or **extensive** option. The command output section for **Traffic statistics** lists the number of bytes and packets received and transmitted on the logical interface, and the **Protocol inet** section contains a **Policer** field that would list the policer **500Kbps** as an input or output policer as follows:

- **Input: 500Kbps-ge-1/3/1.0-log\_int-i**
- **Output: 500Kbps-ge-1/3/1.0-log\_int-o**

The **log\_int-i** suffix denotes a logical interface policer applied to input traffic, while the **log\_int-o** suffix denotes a logical interface policer applied to output traffic. In this example, the logical interface policer is applied to Input traffic only.

#### *Displaying Statistics for the Policer*

**Purpose** Verify the number of packets evaluated by the policer.

**Action** Use the **show policer** operational mode command and optionally specify the name of the policer. The command output displays the number of packets evaluated by each configured policer (or the specified policer), in each direction. For the policer **500Kbps**, the input and output policer names are displayed as follows:

- **500Kbps-ge-1/3/1.0-log\_int-i**
- **500Kbps-ge-1/3/1.0-log\_int-o**

The **log\_int-i** suffix denotes a logical interface policer applied to input traffic, while the **log\_int-o** suffix denotes a logical interface policer applied to output traffic. In this example, the logical interface policer is applied to input traffic only.

- Related Documentation**
- [Statement Hierarchy for Configuring Policers on page 13](#)
  - [Two-Color Policer Configuration Overview on page 15](#)
  - [Guidelines for Applying Traffic Policers on page 24](#)
  - “Configuring a Policer Overhead” in the *[Junos OS System Basics and Services Command Reference](#)*



## CHAPTER 6

# Three-Color Policers

- [Three-Color Policer Configuration Guidelines on page 109](#)
- [Basic Single-Rate Three-Color Policers on page 111](#)
- [Basic Two-Rate Three-Color Policers on page 117](#)

### Three-Color Policer Configuration Guidelines

---

- [Platforms Supported for Three-Color Policers on page 109](#)
- [Color Modes for Three-Color Policers on page 109](#)
- [Naming Conventions for Three-Color Policers on page 110](#)

### Platforms Supported for Three-Color Policers

Three-color policers are 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

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

The **discard** action for a tricolor marking policer for a firewall filter is supported on the M120, M320 with Enhanced-III FPCs, M7i and M10i with the Enhanced CFEB (CFEB-E), and the MX Series routers, so it is not necessary to include the **logical-interface-policer** statement for them.

### Color Modes for Three-Color Policers

Three-color policers—both single-rate and two-rate three-color policer schemes—can operate in either of two modes:

- [Color-Blind Mode on page 110](#)
- [Color-Aware Mode on page 110](#)

### Color-Blind Mode

---

In *color-blind* mode, the three-color policer assumes that all packets examined have not been previously marked or metered. If you configure a three-color policer to be color-blind instead of color-aware, the policer ignores preexisting color markings that might have been set for a packet by another traffic policer configured at a previous network node.

### Color-Aware Mode

---

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 takes into account any coloring markings that might have been set for a packet by another traffic policer configured at a previous network node. At the node where color-aware policing is configured, any preexisting color markings are used in determining the appropriate policing action for the packet.

In color-aware mode, the three-color policer can increase the packet loss priority (PLP) level 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.

For two-rate, three-color policing, the Junos OS uses two token buckets to manage bandwidth based on the two rates of traffic. For example, two-rate policing might be configured on a node upstream in the network. The two-rate policer has marked a packet as yellow (loss priority medium-low). The color-aware policer takes this yellow marking into account when determining the appropriate policing action. In color-aware policing, the yellow packet would never receive the action associated with either the green packets or red packets. This way, tokens for violating packets are never taken from the metering token buckets at the color-aware policing node.

## Naming Conventions for Three-Color Policers

Because policers can be numerous and must be applied correctly to work, a simple naming convention makes it easier to apply the policers properly.

We recommend that you name your policer using a convention that identifies the basic components of the policer:

- Three-color policer type—Where **srTCM** identifies a *single-rate* three-color policer and **trTCM** identifies a *two-rate* three-color policer.
- Three-color policer color mode—Where **ca** identifies a *color-aware* three-color policer and **cb** identifies a *color-blind three-color policer*.



#### NOTE:

TCM stands for tricolor marking.

---

[Table 9 on page 111](#) describes a recommended naming convention for policers.

Table 9: Recommended Naming Convention for Policers

| Three-Color Policer Type             | Naming Convention     | Example Names                                 |
|--------------------------------------|-----------------------|-----------------------------------------------|
| Single-rate three-color, color-aware | <i>srTCMnumber-ca</i> | srTCM1-ca,<br>srTCM2-ca,<br>srTCM3-ca,<br>... |
| Single-rate three-color, color-blind | <i>srTCMnumber-cb</i> | srTCM1-cb,<br>srTCM2-cb,<br>srTCM3-cb,<br>... |
| Two-rate three-color, color-aware    | <i>trTCMnumber-ca</i> | trTCM1-ca,<br>trTCM2-ca,<br>trTCM3-ca,<br>... |
| Two-rate three-color, color-blind    | <i>trTCMnumber-cb</i> | trTCM1-cb,<br>trTCM2-cb,<br>trTCM3-cb,<br>... |

- Related Documentation**
- [Statement Hierarchy for Configuring Policers on page 13](#)
  - [Three-Color Policer Configuration Overview on page 19](#)
  - [Guidelines for Applying Traffic Policers on page 24](#)

## Basic Single-Rate Three-Color Policers

- [Single-Rate Three-Color Policer Overview on page 111](#)
- [Example: Configuring a Single-Rate Three-Color Policer on page 112](#)

### Single-Rate Three-Color Policer Overview

A single-rate three-color policer defines a bandwidth limit and a maximum burst size for guaranteed traffic and a second burst size for peak traffic. A single-rate three-color policer is most useful when a service is structured according to packet length and not peak arrival rate.

Single-rate three-color policing meters a traffic stream based on the following configured traffic criteria:

- Committed information rate (CIR)—Bandwidth limit for guaranteed traffic.
- Committed burst size (CBS)—Maximum packet size permitted for bursts of data that exceed the CIR.
- Excess burst size (EBS)—Maximum packet size permitted for peak traffic.

Single-rate tricolor marking (single-rate TCM) classifies traffic as belonging to one of three color categories and performs congestion-control actions on the packets based on the color marking:

- Green—Traffic that conforms to *either* the bandwidth limit *or* the burst size for guaranteed traffic (CIR and CBS). For a green traffic flow, single-rate marks the packets with an implicit loss priority of **low** and transmits the packets.
- Yellow—Traffic that exceeds *both* the bandwidth limit *and* the burst size for guaranteed traffic (CIR or CBS) but not the burst size for peak traffic (EBS). For a yellow traffic flow, single-rate marks the packets with an implicit loss priority of **medium-high** and transmits the packets.
- Red—Traffic that exceeds the burst size for peak traffic (EBS), single-rate marks packets with an implicit loss priority of **high** and, optionally, discards the packets.

If congestion occurs downstream, the packets with higher loss priority are more likely to be discarded.



**NOTE:** For both single-rate and two-rate three-color policers, the only *configurable* action is to discard packets in a red traffic flow.

---

The **discard** action for a tricolor marking policer for a firewall filter is supported on the M120, M320 with Enhanced-III FPCs, M7i and M10i with the Enhanced CFEB (CFEB-E), and the MX Series routers, so it is not necessary to include the **logical-interface-policer** statement for them.

## Example: Configuring a Single-Rate Three-Color Policer

This example shows how to configure a single-rate three-color policer.

- [Requirements on page 112](#)
- [Overview on page 112](#)
- [Configuration on page 113](#)
- [Verification on page 116](#)

---

### Requirements

No special configuration beyond device initialization is required before configuring this example.

---

### Overview

A single-rate three-color policer meters a traffic flow against a bandwidth limit and burst-size limit for guaranteed traffic, plus a second burst-size limit for excess traffic. Traffic that conforms to the limits for guaranteed traffic is categorized as green, and nonconforming traffic falls into one of two categories:

- Nonconforming traffic that does not exceed the burst size for excess traffic is categorized as yellow.



- Nonconforming traffic that exceeds the burst size for excess traffic is categorized as red.

Each category is associated with an action. For green traffic, packets are implicitly set with a loss-priority value of **low** and then transmitted. For yellow traffic, packets are implicitly set with a loss-priority value of **medium-high** and then transmitted. For red traffic, packets are implicitly set with a loss-priority value of **high** and then transmitted. If the policer configuration includes the optional **action** statement (**action loss-priority high then discard**), then packets in a red flow are discarded instead.

You can apply a three-color policer to Layer 3 traffic as a firewall filter policer only. You reference the policer from a stateless firewall filter term, and then you apply the filter to the input or output of a logical interface at the protocol level.

### Topology

In this example, you apply a color-aware, single-rate three-color policer to the input IPv4 traffic at logical interface **ge-2/0/5.0**. The IPv4 firewall filter term that references the policer does not apply any packet-filtering. The filter is used only to apply the three-color policer to the interface.

You configure the policer to rate-limit traffic to a bandwidth limit of 40 Mbps and a burst-size limit of 100 KB for green traffic but also allow an excess burst-size limit of 200 KB for yellow traffic. Only nonconforming traffic that exceeds the peak burst-size limit is categorized as red. In this example, you configure the three-color policer action **loss-priority high then discard**, which overrides the implicit marking of red traffic to a **high** loss priority.

### Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see [“Using the CLI Editor in Configuration Mode” on page 215](#).

To configure this example, perform the following tasks:

- [Configuring a Single-Rate Three-Color Policer on page 114](#)
- [Configuring an IPv4 Stateless Firewall Filter That References the Policer on page 115](#)
- [Applying the Filter to the Logical Interface on page 115](#)

### CLI Quick Configuration

To quickly configure this example, copy the following configuration commands into a text file, remove any line breaks, and then paste the commands into the CLI at the **[edit]** hierarchy level.

```
set firewall three-color-policer srTCM1-ca single-rate color-aware
set firewall three-color-policer srTCM1-ca single-rate committed-information-rate 40m
set firewall three-color-policer srTCM1-ca single-rate committed-burst-size 100k
set firewall three-color-policer srTCM1-ca single-rate excess-burst-size 200k
set firewall three-color-policer srTCM1-ca action loss-priority high then discard
set firewall family inet filter filter-srTCM1ca-all term 1 then three-color-policer single-rate
srTCM1-ca
set class-of-service interfaces ge-2/0/5 unit 0 forwarding-class af
set interfaces ge-2/0/5 unit 0 family inet address 10.20.130.1/24
```

```
set interfaces ge-2/0/5 unit 0 family inet filter input filter-srtcm1ca-all
```

### Configuring a Single-Rate Three-Color Policer

#### Step-by-Step Procedure

To configure a single-rate three-color policer:

1. Enable configuration of a three-color policer.

```
[edit]
user@host# edit firewall three-color-policer srTCM1-ca
```

2. Configure the color mode of the single-rate three-color policer.

```
[edit firewall three-color-policer srTCM1-ca]
user@host# set single-rate color-aware
```

3. Configure the single-rate guaranteed traffic limits.

```
[edit firewall three-color-policer srTCM1-ca]
user@host# set single-rate committed-information-rate 40m
user@host# set single-rate committed-burst-size 100k
```

4. Configure the single-rate burst-size limit that is used to classify nonconforming traffic.

```
[edit firewall three-color-policer srTCM1-ca]
user@host# set single-rate excess-burst-size 200k
```

5. (Optional) Configure the action for nonconforming traffic.

```
[edit firewall three-color-policer srTCM1-ca]
user@host# set action loss-priority high then discard
```

For three-color policers, the only configurable action is to discard packets in a red traffic flow. In this example, packets in a red traffic flow have been implicitly marked with a **high** packet loss priority (PLP) level because the traffic flow exceeded the rate-limiting defined by the single rate-limit (specified by the **committed-information-rate 40m** statement) and the larger burst-size limit (specified by the **excess-burst-size 200k** statement). Because the optional **action** statement is included, this example takes the more severe action of discarding packets in a red traffic flow.

**Results** Confirm the configuration of the hierarchical policer by entering the **show firewall** configuration command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
three-color-policer srTCM1-ca {
  action {
    loss-priority high then discard;
  }
  single-rate {
    color-aware;
    committed-information-rate 40m;
    committed-burst-size 100k;
    excess-burst-size 200k;
  }
}
```

*Configuring an IPv4 Stateless Firewall Filter That References the Policer***Step-by-Step Procedure**

To configure a standard stateless firewall filter that references the policer:

1. Enable configuration of an IPv4 standard stateless firewall filter.

```
[edit]
user@host# edit firewall family inet filter filter-srtcm1ca-all
```

2. Specify the filter term that references the policer.

```
[edit firewall family inet filter filter-srtcm1ca-all]
user@host# set term 1 then three-color-policer single-rate srTCM1-ca
```

Note that the term does not specify any match conditions. The firewall filter passes all packets to the policer.

**Results**

Confirm the configuration of the firewall filter by entering the **show firewall** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show firewall
family inet {
  filter filter-srtcm1ca-all {
    term 1 {
      then {
        three-color-policer {
          single-rate srTCM1-ca;
        }
      }
    }
  }
}
three-color-policer srTCM1-ca {
  action {
    loss-priority high then discard;
  }
  single-rate {
    color-aware;
    committed-information-rate 40m;
    committed-burst-size 100k;
    excess-burst-size 200k;
  }
}
```

*Applying the Filter to the Logical Interface***Step-by-Step Procedure**

To apply the filter to the logical interface:

1. (MX Series routers only) (Optional) Reclassify all incoming packets on the logical interface **ge-2/0/5.0** to assured forwarding, regardless of any preexisting classification.

```
[edit]
user@host# set class-of-service interfaces ge-2/0/5 unit 0 forwarding-class af
```

The classifier name can be a configured classifier or one of the default classifiers.

2. Enable configuration of the logical interface.

```
[edit]
user@host# edit interfaces ge-2/0/5 unit 0 family inet
```

3. Configure an IP address.

```
[edit interfaces ge-2/0/5 unit 0 family inet]
user@host# set address 10.20.130.1/24
```

4. Reference the filter as an input filter.

```
[edit interfaces ge-2/0/5 unit 0 family inet]
user@host# set filter input filter-srtcm1ca-all
```

**Results** Confirm the configuration of the interface by entering the **show class-of-service** and **show interfaces** configuration mode commands. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show class-of-service
interfaces {
  ge-2/0/5 {
    unit 0 {
      forwarding-class af;
    }
  }
}
[edit]
user@host# show interfaces
ge-2/0/5 {
  unit 0 {
    family inet {
      filter {
        input filter-srtcm1ca-all;
      }
      address 10.20.130.1/24;
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

---

### Verification

Confirm that the configuration is working properly.

#### *Displaying the Firewall Filters Applied to the Logical Interface*

**Purpose** Verify that the firewall filter is applied to IPv4 input traffic at the logical interface.

**Action** Use the **show interfaces** operational mode command for the logical interface **ge-2/0/5.0**, and specify **detail** mode. The **Protocol inet** section of the command output displays IPv4

information for the logical interface. Within that section, the **Input Filters** field displays the name of the firewall filter applied to IPv4 input traffic at the logical interface.

```
user@host> show interfaces ge-2/0/5.0 detail
Logical interface ge-2/0/5.0 (Index 105) (SNMP ifIndex 556) (Generation 170)
Flags: Device-Down SNMP-Traps 0x4004000 Encapsulation: ENET2
Traffic statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Local statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Transit statistics:
  Input bytes : 0 0 bps
  Output bytes : 0 0 bps
  Input packets: 0 0 pps
  Output packets: 0 0 pps
Protocol inet, MTU: 1500, Generation: 242, Route table: 0
Flags: Sendbcast-pkt-to-re
Input Filters: filter-srtcm1ca-all
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
Destination: 10.20.130/24, Local: 10.20.130.1, Broadcast: 10.20.130.255,
Generation: 171
Protocol multiservice, MTU: Unlimited, Generation: 243, Route table: 0
Policer: Input: __default_arp_policer__
```

- Related Documentation**
- [Statement Hierarchy for Configuring Policers on page 13](#)
  - [Three-Color Policer Configuration Overview on page 19](#)
  - [Three-Color Policer Configuration Guidelines on page 109](#)

## Basic Two-Rate Three-Color Policers

- [Two-Rate Three-Color Policer Overview on page 117](#)
- [Example: Configuring a Two-Rate Three-Color Policer on page 118](#)

### Two-Rate Three-Color Policer Overview

A two-rate three-color policer defines two bandwidth limits (one for guaranteed traffic and one for peak traffic) and two burst sizes (one for each of the bandwidth limits). A two-rate three-color policer is most useful when a service is structured according to arrival rates and not necessarily packet length.

Two-rate three-color policing meters a traffic stream based on the following configured traffic criteria:

- Committed information rate (CIR)—Bandwidth limit for guaranteed traffic.
- Committed burst size (CBS)—Maximum packet size permitted for bursts of data that exceed the CIR.

- Peak information rate (PIR)—Bandwidth limit for peak traffic.
- Peak burst size (PBS)—Maximum packet size permitted for bursts of data that exceed the PIR.

Two-rate tricolor marking (two-rate TCM) classifies traffic as belonging to one of three color categories and performs congestion-control actions on the packets based on the color marking:

- Green—Traffic that conforms to the bandwidth limit and burst size for guaranteed traffic (CIR and CBS). For a green traffic flow, two-rate TCM marks the packets with an implicit loss priority of **low** and transmits the packets.
- Yellow—Traffic that exceeds the bandwidth limit or burst size for guaranteed traffic (CIR or CBS) but not the bandwidth limit and burst size for peak traffic (PIR and PBS). For a yellow traffic flow, two-rate TCM marks packets with an implicit loss priority of **medium-high** and transmits the packets.
- Red—Traffic that exceeds the bandwidth limit and burst size for peak traffic (PIR and PBS). For a red traffic flow, two-rate TCM marks packets with an implicit loss priority of **high** and, optionally, discards the packets.

If congestion occurs downstream, the packets with higher loss priority are more likely to be discarded.



**NOTE:** For both single-rate and two-rate three-color policers, the only *configurable* action is to discard packets in a red traffic flow.

---

For a tricolor marking policer referenced by a firewall filter term, the **discard** policing action is supported on the following routing platforms:

- M7i and M10i routers with the Enhanced CFEB (CFEB-E)
- M120 and M320 routers with Enhanced-III FPCs
- MX Series routers

To apply a tricolor marking policer on these routing platforms, it is not necessary to include the **logical-interface-policer** statement.

### Example: Configuring a Two-Rate Three-Color Policer

This example shows how to configure a two-rate three-color policer.

- [Requirements on page 119](#)
- [Overview on page 119](#)
- [Configuration on page 119](#)
- [Verification on page 122](#)

---

## Requirements

No special configuration beyond device initialization is required before configuring this example.

---

## Overview

A two-rate three-color policer meters a traffic flow against a bandwidth limit and burst-size limit for guaranteed traffic, plus a bandwidth limit and burst-size limit for peak traffic. Traffic that conforms to the limits for guaranteed traffic is categorized as green, and nonconforming traffic falls into one of two categories:

- Nonconforming traffic that does not exceed peak traffic limits is categorized as yellow.
- Nonconforming traffic that exceeds peak traffic limits is categorized as red.

Each category is associated with an action. For green traffic, packets are implicitly set with a loss-priority value of **low** and then transmitted. For yellow traffic, packets are implicitly set with a loss-priority value of **medium-high** and then transmitted. For red traffic, packets are implicitly set with a loss-priority value of **high** and then transmitted. If the policer configuration includes the optional **action** statement (**action loss-priority high then discard**), then packets in a red flow are discarded instead.

You can apply a three-color policer to Layer 3 traffic as a firewall filter policer only. You reference the policer from a stateless firewall filter term, and then you apply the filter to the input or output of a logical interface at the protocol level.

## Topology

In this example, you apply a color-aware, two-rate three-color policer to the input IPv4 traffic at logical interface **fe-0/1/1.0**. The IPv4 firewall filter term that references the policer does not apply any packet-filtering. The filter is used only to apply the three-color policer to the interface.

You configure the policer to rate-limit traffic to a bandwidth limit of 40 Mbps and a burst-size limit of 100 KB for green traffic, and you configure the policer to also allow a peak bandwidth limit of 60 Mbps and a peak burst-size limit of 200 KB for yellow traffic. Only nonconforming traffic that exceeds the peak traffic limits is categorized as red. In this example, you configure the three-color policer action **loss-priority high then discard**, which overrides the implicit marking of red traffic to a **high** loss priority.

---

## Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see [“Using the CLI Editor in Configuration Mode” on page 215](#).

To configure this example, perform the following tasks:

- [Configuring a Two-Rate Three-Color Policer on page 120](#)
- [Configuring an IPv4 Stateless Firewall Filter That References the Policer on page 121](#)
- [Applying the Filter to a Logical Interface at the Protocol Family Level on page 122](#)

**CLI Quick Configuration** To quickly configure this example, copy the following configuration commands into a text file, remove any line breaks, and then paste the commands into the CLI at the [edit] hierarchy level.

```
set firewall three-color-policer trTCM1-ca two-rate color-aware
set firewall three-color-policer trTCM1-ca two-rate committed-information-rate 40m
set firewall three-color-policer trTCM1-ca two-rate committed-burst-size 100k
set firewall three-color-policer trTCM1-ca two-rate peak-information-rate 60m
set firewall three-color-policer trTCM1-ca two-rate peak-burst-size 200k
set firewall three-color-policer trTCM1-ca action loss-priority high then discard
set firewall family inet filter filter-trtcm1ca-all term 1 then three-color-policer two-rate
trTCM1-ca
set interfaces ge-2/0/5 unit 0 family inet address 10.10.10.1/30
set interfaces ge-2/0/5 unit 0 family inet filter input filter-trtcm1ca-all
set class-of-service interfaces ge-2/0/5 forwarding-class af
```

### *Configuring a Two-Rate Three-Color Policer*

**Step-by-Step Procedure** To configure a two-rate three-color policer:

1. Enable configuration of a three-color policer.

```
[edit]
user@host# set firewall three-color-policer trTCM1-ca
```

2. Configure the color mode of the two-rate three-color policer.

```
[edit firewall three-color-policer trTCM1-ca]
user@host# set two-rate color-aware
```

3. Configure the two-rate guaranteed traffic limits.

```
[edit firewall three-color-policer trTCM1-ca]
user@host# set two-rate committed-information-rate 40m
user@host# set two-rate committed-burst-size 100k
```

Traffic that does not exceed both of these limits is categorized as green. Packets in a green flow are implicitly set to **low** loss priority and then transmitted.

4. Configure the two-rate peak traffic limits

```
[edit firewall three-color-policer trTCM1-ca]
user@host# set two-rate peak-information-rate 60m
user@host# set two-rate peak-burst-size 200k
```

Nonconforming traffic that does not exceed both of these limits is categorized as yellow. Packets in a yellow flow are implicitly set to **medium-high** loss priority and then transmitted. Nonconforming traffic that exceeds both of these limits is categorized as red. Packets in a red flow are implicitly set to **high** loss priority.

5. (Optional) Configure the policer action for red traffic.

```
[edit firewall three-color-policer trTCM1-ca]
user@host# set action loss-priority high then discard
```

For three-color policers, the only configurable action is to discard red packets. Red packets are packets that have been assigned high loss priority because they exceeded the peak information rate (PIR) and the peak burst size (PBS).



**Results** Confirm the configuration of the policer by entering the **show firewall** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show firewall
three-color-policer trTCM1-ca {
  action {
    loss-priority high then discard;
  }
  two-rate {
    color-aware;
    committed-information-rate 40m;
    committed-burst-size 100k;
    peak-information-rate 60m;
    peak-burst-size 200k;
  }
}
```

#### *Configuring an IPv4 Stateless Firewall Filter That References the Policer*

**Step-by-Step Procedure** To configure an IPv4 stateless firewall filter that references the policer:

1. Enable configuration of an IPv4 standard stateless firewall filter.

```
[edit]
user@host# set firewall family inet filter filter-trtcm1ca-all
```

2. Specify the filter term that references the policer.

```
[edit firewall family inet filter filter-trtcm1ca-all]
user@host# set term 1 then three-color-policer two-rate trTCM1-ca
```

Note that the term does not specify any match conditions. The firewall filter passes all packets to the policer.

**Results** Confirm the configuration of the firewall filter by entering the **show firewall** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show firewall
family inet {
  filter filter-trtcm1ca-all {
    term 1 {
      then {
        three-color-policer {
          two-rate trTCM1-ca;
        }
      }
    }
  }
}
three-color-policer trTCM1-ca {
  action {
    loss-priority high then discard;
  }
}
```

```
two-rate {
  color-aware;
  committed-information-rate 40m;
  committed-burst-size 100k;
  peak-information-rate 60m;
  peak-burst-size 200k;
}
```

### *Applying the Filter to a Logical Interface at the Protocol Family Level*

#### **Step-by-Step Procedure**

To apply the filter to the logical interface at the protocol family level:

1. Enable configuration of an IPv4 firewall filter.

```
[edit]
user@host# edit interfaces ge-2/0/5 unit 0 family inet
```

2. Apply the policer to the logical interface at the protocol family level.

```
[edit interfaces ge-2/0/5 unit 0 family inet]
user@host# set address 10.10.10.1/30
user@host# set filter input filter-trtcm1ca-all
```

3. (MX Series routers only) (Optional) For input policers, you can configure a fixed classifier. A fixed classifier reclassifies all incoming packets, regardless of any preexisting classification.

```
[edit]
user@host# set class-of-service interfaces ge-2/0/5 forwarding-class af
```

The classifier name can be a configured classifier or one of the default classifiers.

**Results** Confirm the configuration of the interface by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show interfaces
ge-2/0/5 {
  unit 0 {
    family inet {
      address 10.10.10.1/30;
      filter {
        input filter-trtcm1ca-all;
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

---

### **Verification**

Confirm that the configuration is working properly.

*Displaying the Firewall Filters Applied to the Logical Interface*

**Purpose** Verify that the firewall filter is applied to IPv4 input traffic at the logical interface.

**Action** Use the **show interfaces** operational mode command for the logical interface **ge-2/0/5.0**, and specify **detail** mode. The **Protocol inet** section of the command output displays IPv4 information for the logical interface. Within that section, the **Input Filters** field displays the name of IPv4 firewall filters associated with the logical interface.

```
user@host> show interfaces ge-2/0/5.0 detail
Logical interface ge-2/0/5.0 (Index 105) (SNMP ifIndex 556) (Generation 170)
  Flags: Device-Down SNMP-Traps 0x4004000 Encapsulation: ENET2
  Traffic statistics:
    Input bytes : 0
    Output bytes : 0
    Input packets: 0
    Output packets: 0
  Local statistics:
    Input bytes : 0
    Output bytes : 0
    Input packets: 0
    Output packets: 0
  Transit statistics:
    Input bytes : 0 0 bps
    Output bytes : 0 0 bps
    Input packets: 0 0 pps
    Output packets: 0 0 pps
  Protocol inet, MTU: 1500, Generation: 242, Route table: 0
    Flags: Sendbroadcast-pkt-to-re
    Input Filters: filter-trtcm1ca-all
    Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
      Destination: 10.20.130/24, Local: 10.20.130.1, Broadcast: 10.20.130.255,

      Generation: 171
  Protocol multiservice, MTU: Unlimited, Generation: 243, Route table: 0
    Policers: Input: __default_arp_policer__
```

- Related Documentation**
- [Statement Hierarchy for Configuring Policers on page 13](#)
  - [Three-Color Policer Configuration Overview on page 19](#)
  - [Three-Color Policer Configuration Guidelines on page 109](#)



## CHAPTER 7

# Logical and Physical Interface Policers

- [Two-Color and Three-Color Logical Interface Policers on page 125](#)
- [Two-Color and Three-Color Physical Interface Policers on page 137](#)

## Two-Color and Three-Color Logical Interface Policers

---

- [Logical Interface \(Aggregate\) Policer Overview on page 125](#)
- [Example: Configuring a Two-Color Logical Interface \(Aggregate\) Policer on page 126](#)
- [Example: Configuring a Three-Color Logical Interface \(Aggregate\) Policer on page 131](#)

### Logical Interface (Aggregate) Policer Overview

A *logical interface policer*—also called an *aggregate policer*—is a two-color or three-color policer that defines traffic rate limiting that you can apply to input or output traffic for multiple protocol families on the same logical interface without creating multiple instances of the policer.

To configure a single-rate two-color logical interface policer, include the **logical-interface-policer** statement at one of the following hierarchy levels:

- **[edit firewall *policer policer-name*]**
- **[edit logical-systems *logical-system-name* firewall *policer policer-name*]**

To configure a single-rate or two-rate three-color logical interface policer, include the **logical-interface-policer** statement at one of the following hierarchy levels:

- **[edit firewall *three-color-policer name*]**
- **[edit logical-systems *logical-system-name* firewall *three-color-policer name*]**



**NOTE:** A three-color policer can be applied to Layer 2 traffic as a logical interface policer only. You cannot apply a three-color policer to Layer 2 traffic as a physical interface policer (through a firewall filter).

You apply a logical interface policer to Layer 3 traffic directly to the interface configuration at the logical unit level (to rate-limit all traffic types, regardless of the protocol family) or at the protocol family level (to rate-limit traffic of a specific protocol family). You

cannot reference a logical interface policer from a stateless firewall filter term and then apply the filter to a logical interface.

You can apply a logical interface policer to unicast traffic only. For information about configuring a stateless firewall filter for flooded traffic, see “Applying Filters to Forwarding Tables” in the “Traffic Sampling, Forwarding, and Monitoring” section of the *Junos OS Routing Policy Configuration Guide*.

To display a logical interface policer on a particular interface, issue the **show interfaces policers** operational mode command.

## Example: Configuring a Two-Color Logical Interface (Aggregate) Policer

This example shows how to configure a single-rate two-color policer as a logical interface policer and apply it to incoming IPv4 traffic on a logical interface.

- [Requirements on page 126](#)
- [Overview on page 126](#)
- [Configuration on page 126](#)
- [Verification on page 130](#)

---

### Requirements

Before you begin, make sure that the logical interface to which you apply the two-color logical interface policer is hosted on a Gigabit Ethernet interface (**ge-**) or a 10-Gigabit Ethernet interface (**xe-**).

---

### Overview

In this example, you configure the single-rate two-color policer **policer\_IFL** as a logical interface policer and apply it to incoming IPv4 traffic at logical interface **ge-1/3/1.0**.

### Topology

If the input IPv4 traffic on the physical interface **ge-1/3/1** exceeds the bandwidth limit equal to 90 percent of the media rate with a 300 KB burst-size limit, then the logical interface policer **policer\_IFL** rate-limits the input IPv4 traffic on the logical interface **ge-1/3/1.0**. Configure the policer to mark nonconforming traffic by setting packet loss priority (PLP) levels to **high** and classifying packets as **best-effort**.

As the incoming IPv4 traffic rate on the physical interface slows and conforms to the configured limits, Junos OS stops marking the incoming IPv4 packets at the logical interface.

---

### Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see “[Using the CLI Editor in Configuration Mode](#)” on page 215.

To configure this example, perform the following tasks:

- [Configuring the Logical Interfaces on page 127](#)
- [Configuring the Single-Rate Two-Color Policer as a Logical Interface Policer on page 128](#)
- [Applying the Logical Interface Policer to Input IPv4 Traffic at a Logical Interface on page 129](#)

#### CLI Quick Configuration

To quickly configure this example, copy the following configuration commands into a text file, remove any line breaks, and then paste the commands into the CLI at the **[edit]** hierarchy level.

```
set interfaces ge-1/3/1 vlan-tagging
set interfaces ge-1/3/1 unit 0 vlan-id 100
set interfaces ge-1/3/1 unit 0 family inet address 10.10.10.1/30
set interfaces ge-1/3/1 unit 1 vlan-id 101
set interfaces ge-1/3/1 unit 1 family inet address 20.20.20.1/30 arp 20.20.20.2 mac
00:00:11:22:33:44
set firewall policer policer_IFL logical-interface-policer
set firewall policer policer_IFL if-exceeding bandwidth-percent 90
set firewall policer policer_IFL if-exceeding burst-size-limit 300k
set firewall policer policer_IFL then loss-priority high
set firewall policer policer_IFL then forwarding-class best-effort
set interfaces ge-1/3/1 unit 0 family inet policer input policer_IFL
```

#### Configuring the Logical Interfaces

#### Step-by-Step Procedure

To configure the logical interfaces:

1. Enable configuration of the interface.

```
[edit]
user@host# edit interfaces ge-1/3/1
```

2. Configure single tagging.

```
[edit interfaces ge-1/3/1]
user@host# set vlan-tagging
```

3. Configure logical interface **ge-1/3/1.0**.

```
[edit interfaces ge-1/3/1]
user@host# set unit 0 vlan-id 100
user@host# set unit 0 family inet address 10.10.10.1/30
```

4. Configure logical interface **ge-1/3/1.0**.

```
[edit interfaces ge-1/3/1]
user@host# set unit 1 vlan-id 101
user@host# set unit 1 family inet address 20.20.20.1/30 arp 20.20.20.2 mac
00:00:11:22:33:44
```

#### Results

Confirm the configuration of the logical interfaces by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show interfaces
```

```

ge-1/3/1 {
  vlan-tagging;
  unit 0 {
    vlan-id 100;
    family inet {
      address 10.10.10.1/30;
    }
  }
  unit 1 {
    vlan-id 101;
    family inet {
      address 20.20.20.1/30 {
        arp 20.20.20.2 mac 00:00:11:22:33:44;
      }
    }
  }
}

```

### *Configuring the Single-Rate Two-Color Policer as a Logical Interface Policer*

#### **Step-by-Step Procedure**

To configure a single-rate two-color policer as a logical interface policer:

1. Enable configuration of a single-rate two-color policer.

```

[edit]
user@host# edit firewall policer policer_IFL

```

2. Specify that the policer is a logical interface (aggregate) policer.

```

[edit firewall policer policer_IFL]
user@host# set logical-interface-policer

```

A logical interface policer rate-limits traffic based on a percentage of the media rate of the physical interface underlying the logical interface to which the policer is applied. The policer is applied directly to the interface rather than referenced by a firewall filter.

3. Specify the policer traffic limits.
  - a. Specify the bandwidth limit.
    - To specify the bandwidth limit as an absolute rate, from 8,000 bits per second through 50,000,000,000 bits per second, include the **bandwidth-limit *bps*** statement.
    - To specify the bandwidth limit as a percentage of the physical port speed on the interface, include the **bandwidth-percent *percent*** statement.

In this example, the CLI commands and output are based on a bandwidth limit specified as a percentage rather than as an absolute rate.

```

[edit firewall policer policer_IFL]
user@host# set if-exceeding bandwidth-percent 90

```



- b. Specify the burst-size limit, from 1,500 bytes through 100,000,000,000 bytes, which is the maximum packet size to be permitted for bursts of data that exceed the specified bandwidth limit.

```
[edit firewall policer policer_IFL]
user@host# set if-exceeding burst-size-limit 300k
```

4. Specify the policer actions to be taken on traffic that exceeds the configured rate limits.
  - To discard the packet, include the **discard** statement.
  - To set the loss-priority value of the packet, include the **loss-priority (low | medium-low | medium-high | high)** statement.
  - To classify the packet to a forwarding class, include the **forwarding-class (forwarding-class | assured-forwarding | best-effort | expedited-forwarding | network-control)** statement.

In this example, the CLI commands and output are based on both setting the packet loss priority level and classifying the packet.

```
[edit firewall policer policer_IFL]
user@host# set then loss-priority high
user@host# set then forwarding-class best-effort
```

**Results** Confirm the configuration of the policer by entering the **show firewall** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show firewall
policer policer_IFL {
  logical-interface-policer;
  if-exceeding {
    bandwidth-percent 90;
    burst-size-limit 300k;
  }
  then {
    loss-priority high;
    forwarding-class best-effort;
  }
}
```

#### *Applying the Logical Interface Policer to Input IPv4 Traffic at a Logical Interface*

**Step-by-Step Procedure** To apply the two-color logical interface policer to input IPv4 traffic a logical interface:

1. Enable configuration of the logical interface.

```
[edit]
user@host# edit interfaces ge-1/3/1 unit 0
```

2. Apply the policer to all traffic types or to a specific traffic type on the logical interface.

- To apply the policer to all traffic types, regardless of the protocol family, include the **policer (input | output) *policer-name*** statement at the **[edit interfaces *interface-name* unit *number*]** hierarchy level.
- To apply the policer to traffic of a specific protocol family, include the **policer (input | output) *policer-name*** statement at the **[edit interfaces *interface-name* unit *unit-number* family *family-name*]** hierarchy level.

To apply the logical interface policer to incoming packets, use the **policer input *policer-name*** statement. To apply the logical interface policer to outgoing packets, use the **policer output *policer-name*** statement.

In this example, the CLI commands and output are based on rate-limiting the IPv4 input traffic at logical interface **ge-1/3/1.0**.

```
[edit interfaces ge-1/3/1 unit 0]
user@host# set family inet policer input policer_IFL
```

**Results** Confirm the configuration of the interface by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show interfaces
ge-1/3/1 {
  vlan-tagging;
  unit 0 {
    vlan-id 100;
    family inet {
      policer input policer_IFL;
      address 10.10.10.1/30;
    }
  }
  unit 1 {
    vlan-id 101;
    family inet {
      address 20.20.20.1/30 {
        arp 20.20.20.2 mac 00:00:11:22:33:44;
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

---

## Verification

Confirm that the configuration is working properly.

- [Displaying Traffic Statistics and Policers for the Logical Interface on page 131](#)
- [Displaying Statistics for the Policer on page 131](#)

### *Displaying Traffic Statistics and Policers for the Logical Interface*

**Purpose** Verify the traffic flow through the logical interface and that the policer is evaluated when packets are received on the logical interface.

**Action** Use the **show interfaces** operational mode command for logical interface **ge-1/3/1.0**, and include the **detail** or **extensive** option. The command output section for **Traffic statistics** lists the number of bytes and packets received and transmitted on the logical interface. The **Protocol inet** subsection contains a **Policer** field that would list the policer **policer\_IFL** as an input or output logical interface policer as follows:

- Input: **policer\_IFL-ge-1/3/1.0-log\_int-i**
- Output: **policer\_IFL-ge-1/3/1.0-log\_int-o**

The **log\_int-i** suffix denotes a logical interface policer applied to input traffic, while the **log\_int-o** suffix denotes a logical interface policer applied to output traffic. In this example, the logical interface policer is applied to input traffic only.

### *Displaying Statistics for the Policer*

**Purpose** Verify the number of packets evaluated by the policer.

**Action** Use the **show policer** operational mode command and optionally specify the name of the policer. The command output displays the number of packets evaluated by each configured policer (or the specified policer), in each direction. For the policer **policer\_IFL**, the input and output policer names are displayed as follows:

- **policer\_IFL-ge-1/3/1.0-log\_int-i**
- **policer\_IFL-ge-1/3/1.0-log\_int-o**

The **log\_int-i** suffix denotes a logical interface policer applied to input traffic, while the **log\_int-o** suffix denotes a logical interface policer applied to output traffic. In this example, the logical interface policer is applied to input traffic only.

## **Example: Configuring a Three-Color Logical Interface (Aggregate) Policer**

This example shows how to configure a two-rate three-color color-blind policer as a logical interface (aggregate) policer and apply the policer directly to Layer 2 input traffic at a supported logical interface.

- [Requirements on page 132](#)
- [Overview on page 132](#)
- [Configuration on page 133](#)
- [Verification on page 136](#)

## Requirements

---

Before you begin, make sure that the logical interface to which you apply the three-color logical interface policer is hosted on a Gigabit Ethernet interface (**ge-**) or a 10-Gigabit Ethernet interface (**xe-**) on an MX Series router.

## Overview

---

A two-rate three-color policer meters a traffic flow against a bandwidth limit and burst-size limit for guaranteed traffic, plus a second set of bandwidth and burst-size limits for peak traffic. Traffic that conforms to the limits for guaranteed traffic is categorized as green, and nonconforming traffic falls into one of two categories:

- Nonconforming traffic that does not exceed the bandwidth and burst-size limits for peak traffic is categorized as yellow.
- Nonconforming traffic that exceeds the bandwidth and burst-size limits for peak traffic is categorized as red.

A logical interface policer defines traffic rate-limiting rules that you can apply to multiple protocol families on the same logical interface without creating multiple instances of the policer.



**NOTE:** You apply a logical interface policer directly to a logical interface at the logical unit level, and not by referencing the policer in a stateless firewall filter and then applying the filter to the logical interface at the protocol family level.

---

## Topology

In this example, you configure the two-rate three-color policer **trTCM2-cb** as a color-blind logical interface policer and apply the policer to incoming Layer 2 traffic on logical interface **ge-1/3/1.0**.



**NOTE:** When using a three-color policer to rate-limit Layer 2 traffic, color-aware policing can be applied to egress traffic only.

---

The policer defines guaranteed traffic rate limits such that traffic that conforms to the bandwidth limit of 40 Mbps with a 100 KB allowance for traffic bursting (based on the token-bucket formula) is categorized as green. As with any policed traffic, the packets in a green flow are implicitly set to a **low** loss priority and then transmitted.

Nonconforming traffic that falls within the peak traffic limits of a 60 Mbps bandwidth limit and a 200 KB allowance for traffic bursting (based on the token-bucket formula) is categorized as yellow. The packets in a yellow traffic flow are implicitly set to a **medium-high** loss priority and then transmitted.

Nonconforming traffic that exceeds the peak traffic limits are categorized as red. The packets in a red traffic flow are implicitly set to a **high** loss priority. In this example, the

optional policer action for red traffic (**loss-priority high then discard**) is configured, so packets in a red traffic flow are discarded instead of transmitted.

### Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see [“Using the CLI Editor in Configuration Mode” on page 215](#).

To configure this example, perform the following tasks:

- [Configuring the Logical Interfaces on page 133](#)
- [Configuring the Two-Rate Three-Color Policer as a Logical Interface Policer on page 134](#)
- [Applying the Three-Color Policer to the Layer 2 Input at the Logical Interface on page 135](#)

#### CLI Quick Configuration

To quickly configure this example, copy the following configuration commands into a text file, remove any line breaks, and then paste the commands into the CLI at the **[edit]** hierarchy level.

```
set interfaces ge-1/3/1 vlan-tagging
set interfaces ge-1/3/1 unit 0 vlan-id 100
set interfaces ge-1/3/1 unit 0 family inet address 10.10.10.1/30
set interfaces ge-1/3/1 unit 1 vlan-id 101
set interfaces ge-1/3/1 unit 1 family inet address 20.20.20.1/30 arp 20.20.20.2 mac
  00:00:11:22:33:44
set firewall three-color-policer trTCM2-cb logical-interface-policer
set firewall three-color-policer trTCM2-cb two-rate color-blind
set firewall three-color-policer trTCM2-cb two-rate committed-information-rate 40m
set firewall three-color-policer trTCM2-cb two-rate committed-burst-size 100k
set firewall three-color-policer trTCM2-cb two-rate peak-information-rate 60m
set firewall three-color-policer trTCM2-cb two-rate peak-burst-size 200k
set firewall three-color-policer trTCM2-cb action loss-priority high then discard
set interfaces ge-1/3/1 unit 0 layer2-policer input-three-color trTCM2-cb
```

#### Configuring the Logical Interfaces

#### Step-by-Step Procedure

To configure the logical interfaces:

1. Enable configuration of the interface.  
  
[edit]  
user@host# edit interfaces ge-1/3/1
2. Configure single tagging.  
  
[edit interfaces ge-1/3/1]  
user@host# set vlan-tagging
3. Configure logical interface ge-1/3/1.0.  
  
[edit interfaces ge-1/3/1]  
user@host# set unit 0 vlan-id 100  
user@host# set unit 0 family inet address 10.10.10.1/30
4. Configure logical interface ge-1/3/1.0.  
  
[edit interfaces ge-1/3/1]

```

user@host# set unit 1 vlan-id 101
user@host# set unit 1 family inet address 20.20.20.1/30 arp 20.20.20.2 mac
00:00:11:22:33:44

```

**Results** Confirm the configuration of the logical interfaces by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```

[edit]
user@host# show interfaces
ge-1/3/1 {
  vlan-tagging;
  unit 0 {
    vlan-id 100;
    family inet {
      address 10.10.10.1/30;
    }
  }
  unit 1 {
    vlan-id 101;
    family inet {
      address 20.20.20.1/30 {
        arp 20.20.20.2 mac 00:00:11:22:33:44;
      }
    }
  }
}

```

### *Configuring the Two-Rate Three-Color Policer as a Logical Interface Policer*

#### **Step-by-Step Procedure**

To configure the two-rate three-color policer as a logical interface policer:

1. Enable configuration of a three-color policer.

```

[edit]
user@host# edit firewall three-color-policer trTCM2-cb

```

2. Specify that the policer is a logical interface (aggregate) policer.

```

[edit firewall three-color-policer trTCM2-cb]
user@host# set logical-interface-policer

```

A logical interface policer rate-limits traffic based on a percentage of the media rate of the physical interface underlying the logical interface to which the policer is applied, and the policer is applied directly to the interface rather than referenced by a firewall filter.

3. Specify that the policer is two-rate and color-blind.

```

[edit firewall three-color-policer trTCM2-cb]
user@host# set two-rate color-blind

```

A color-aware three-color policer takes into account any coloring markings that might have been set for a packet by another traffic policer configured at a previous network node, and any preexisting color markings are used in determining the appropriate policing action for the packet.

Because you are applying this three-color policer applied to input at Layer 2, you must configure the policer to be color-blind.

4. Specify the policer traffic limits used to classify a green traffic flow.

```
[edit firewall three-color-policer trTCM2-cb]
user@host# set two-rate committed-information-rate 40m
user@host# set two-rate committed-burst-size 100k
```

5. Specify the additional policer traffic limits used to classify a yellow or red traffic flow.

```
[edit firewall three-color-policer trTCM2-cb]
user@host# set two-rate peak-information-rate 60m
user@host# set two-rate peak-burst-size 200k
```

6. (Optional) Specify the configured policer action for packets in a red traffic flow.

```
[edit firewall three-color-policer trTCM2-cb]
user@host# set action loss-priority high then discard
```

In color-aware mode, the three-color policer configured action can increase the packet loss priority (PLP) level 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.

**Results** Confirm the configuration of the three-color policer by entering the **show firewall** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show firewall
three-color-policer trTCM2-cb {
  logical-interface-policer;
  action {
    loss-priority high then discard;
  }
  two-rate {
    color-blind;
    committed-information-rate 40m;
    committed-burst-size 100k;
    peak-information-rate 60m;
    peak-burst-size 200k;
  }
}
```

### *Applying the Three-Color Policer to the Layer 2 Input at the Logical Interface*

#### **Step-by-Step Procedure**

To apply the three-color policer to the Layer 2 input at the logical interface:

1. Enable application of Layer 2 logical interface policers.

```
[edit]
user@host# edit interfaces ge-1/3/1 unit 0
```

2. Apply the three-color logical interface policer to a logical interface input.

```
[edit interfaces ge-1/3/1 unit 0]
```

```
user@host# set layer2-policer input-three-color trTCM2-cb
```

**Results** Confirm the configuration of the logical interfaces by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show interfaces
ge-1/3/1 {
  vlan-tagging;
  unit 0 {
    vlan-id 100;
    layer2-policer {
      input-three-color trTCM2-cb;
    }
    family inet {
      address 10.10.10.1/30;
    }
  }
  unit 1 {
    vlan-id 101;
    family inet {
      address 20.20.20.1/30 {
        arp 20.20.20.2 mac 00:00:11:22:33:44;
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

---

### Verification

Confirm that the configuration is working properly.

- [Displaying Traffic Statistics and Policers for the Logical Interface on page 136](#)
- [Displaying Statistics for the Policer on page 137](#)

#### *Displaying Traffic Statistics and Policers for the Logical Interface*

**Purpose** Verify the traffic flow through the logical interface and that the policer is evaluated when packets are received on the logical interface.

**Action** Use the **show interfaces** operational mode command for logical interface **ge-1/3/1.0**, and include the **detail** or **extensive** option. The command output section for **Traffic statistics** lists the number of bytes and packets received and transmitted on the logical interface, and the **Protocol inet** section contains a **Policer** field that would list the policer **trTCM2-cb** as an input or output policer as follows:

- **Input:** trTCM2-cb-ge-1/3/1.0-log\_int-i
- **Output:** trTCM2-cb-ge-1/3/1.0-log\_int-o



The **log\_int-i** suffix denotes a logical interface policer applied to input traffic, while the **log\_int-o** suffix denotes a logical interface policer applied to output traffic. In this example, the logical interface policer is applied to in the input direction only.

#### *Displaying Statistics for the Policer*

**Purpose** Verify the number of packets evaluated by the policer.

**Action** Use the **show policer** operational mode command and optionally specify the name of the policer. The command output displays the number of packets evaluated by each configured policer (or the specified policer), in each direction. For the policer **trTCM2-cb**, the input and output policer names are displayed as follows:

- **trTCM2-cb-ge-1/3/1.0-log\_int-i**
- **trTCM2-cb-e-1/3/1.0-log\_int-o**

The **log\_int-i** suffix denotes a logical interface policer applied to input traffic, while the **log\_int-o** suffix denotes a logical interface policer applied to output traffic. In this example, the logical interface policer is applied to input traffic only.

- Related Documentation**
- [Statement Hierarchy for Configuring Policers on page 13](#)
  - [Two-Color Policer Configuration Overview on page 15](#)
  - [Three-Color Policer Configuration Overview on page 19](#)
  - [Guidelines for Applying Traffic Policers on page 24](#)

---

## Two-Color and Three-Color Physical Interface Policers

- [Physical Interface Policer Overview on page 137](#)
- [Example: Configuring a Physical Interface Policer for Aggregate Traffic at a Physical Interface on page 139](#)

### Physical Interface Policer Overview

A *physical interface policer* is a two-color or three-color policer that defines traffic rate limiting that you can apply to input or output traffic for all the logical interfaces and protocol families configured on a physical interface, even if the logical interfaces belong to different routing instances. This feature is useful when you want to perform aggregate policing for different protocol families and different logical interfaces on the same physical interface.

For example, suppose that a provider edge (PE) router has numerous logical interfaces, each corresponding to a different customer, configured on the same link to a customer edge (CE) device. Now suppose that a customer wants to apply one set of rate limits aggregately for certain types of traffic on a single physical interface. To accomplish this, you could apply a single physical interface policer to the physical interface, which rate-limits all the logical interfaces configured on the interface and all the routing instances to which those interfaces belong.

To configure a single-rate two-color physical interface policer, include the **physical-interface-policer** statement at one of the following hierarchy levels:

- [edit firewall **policer** *policer-name*]
- [edit logical-system *logical-system-name* firewall **policer** *policer-name*]
- [edit routing-instances *routing-instance-name* firewall **policer** *policer-name*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* firewall **policer** *policer-name*]

To configure a single-rate or two-rate three-color physical interface policer, include the **physical-interface-policer** statement at one of the following hierarchy levels:

- [edit firewall **three-color-policer** *policer-name*]
- [edit logical-system *logical-system-name* firewall **three-color-policer** *policer-name*]
- [edit routing-instances *routing-instance-name* firewall **three-color-policer** *policer-name*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* firewall **three-color-policer** *policer-name*]

You apply a physical interface policer to Layer 3 traffic by referencing the policer from a stateless firewall filter term and then applying the filter to a logical interface. You cannot apply a physical interface to Layer 3 traffic directly to the interface configuration.

To reference a single-rate two-color policer from a stateless firewall filter term, use the **policer** nonterminating action. To reference a single-rate or two-rate three-color policer from a stateless firewall filter term, use the **three-color-policer** nonterminating action.

The following requirements apply to a stateless firewall filter that references a physical interface policer:

- You must configure the firewall filter for a specific, supported protocol family: **ipv4**, **ipv6**, **mpls**, **vpls**, or circuit cross-connect (**ccc**), but not for **family any**.
- You must configure the firewall filter as a *physical interface filter* by including the **physical-interface-filter** statement at the [edit firewall **family** *family-name* **filter** *filter-name*] hierarchy level.
- A firewall filter that is defined as a physical interface filter can reference a physical interface policer only.
- A firewall filter that is defined as a physical interface filter cannot reference a policer configured with the **interface-specific** statement.
- You cannot configure a firewall filter as both a physical interface filter and as a logical interface filter that also includes the **interface-specific** statement.

## Example: Configuring a Physical Interface Policer for Aggregate Traffic at a Physical Interface

This example shows how to configure a single-rate two-color policer as a physical interface policer.

- [Requirements on page 139](#)
- [Overview on page 139](#)
- [Configuration on page 140](#)
- [Verification on page 144](#)

---

### Requirements

No special configuration beyond device initialization is required before configuring this example.

---

### Overview

A *physical interface policer* specifies rate-limiting for aggregate traffic, which encompasses all protocol families and logical interfaces configured on a physical interface, even if the interfaces belong to different routing instances.

You can apply a physical interface policer to Layer 3 input or output traffic only by referencing the policer from a stateless firewall filter that is configured for specific a specific protocol family (not for **family any**) and configured as a physical interface filter. You configure the filter terms with match conditions that select the types of packets you want to rate-limit, and you specify the physical interface policer as the action to apply to matched packets.

### Topology

The physical interface policer in this example, **shared-policer-A**, rate-limits to 100,000,000 bps and permits a maximum burst of traffic of 500,000 bytes. You configure the policer to discard packets in nonconforming flows, but you could instead configure the policer to re-mark nonconforming traffic with a forwarding class, a packet loss priority (PLP) level, or both.

To be able to use the policer to rate-limit IPv4 traffic, you reference the policer from an IPv4 physical interface filter. For this example, you configure the filter to pass the policer IPv4 packets that meet either of the following match terms:

- Packets received through TCP and with the IP precedence fields **critical-ecp** (0xa0), **immediate** (0x40), or **priority** (0x20)
- Packets received through TCP and with the IP precedence fields **internet-control** (0xc0) or **routine** (0x00)

You could also reference the policer from physical interface filters for other protocol families.

## Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see [“Using the CLI Editor in Configuration Mode” on page 215](#).

To configure this example, perform the following tasks:

- [Configuring the Logical Interfaces on the Physical Interface on page 140](#)
- [Configuring a Physical Interface Policer on page 141](#)
- [Configuring an IPv4 Physical Interface Filter on page 142](#)
- [Applying the IPv4 Physical interface Filter to a Physical Interface on page 143](#)

### CLI Quick Configuration

To quickly configure this example, copy the following configuration commands into a text file, remove any line breaks, and then paste the commands into the CLI at the **[edit]** hierarchy level.

```
set interfaces so-1/0/0 unit 0 family inet address 192.168.1.1/24
set interfaces so-1/0/0 unit 0 family vpls
set interfaces so-1/0/0 unit 1 family mpls
set firewall policer shared-policer-A physical-interface-policer
set firewall policer shared-policer-A if-exceeding bandwidth-limit 100m burst-size-limit 500k
set firewall policer shared-policer-A then discard
set firewall family inet filter ipv4-filter physical-interface-filter
set firewall family inet filter ipv4-filter term tcp-police-1 from precedence [ critical-ecp immediate priority ]
set firewall family inet filter ipv4-filter term tcp-police-1 from protocol tcp
set firewall family inet filter ipv4-filter term tcp-police-1 then policer shared-policer-A
set firewall family inet filter ipv4-filter term tcp-police-2 from precedence [ internet-control routine ]
set firewall family inet filter ipv4-filter term tcp-police-2 from protocol tcp
set firewall family inet filter ipv4-filter term tcp-police-2 then policer shared-policer-A
set interfaces so-1/0/0 unit 0 family inet filter input ipv4-filter
```

### *Configuring the Logical Interfaces on the Physical Interface*

### Step-by-Step Procedure

To configure the logical interfaces on the physical interface:

1. Enable configuration of logical interfaces.  
  
[edit]  
user@host# edit interfaces so-1/0/0
2. Configure protocol families on logical unit 0.  
  
[edit interfaces so-1/0/0]  
user@host# set unit 0 family inet address 192.168.1.1/24  
user@host# set unit 0 family vpls
3. Configure protocol families on logical unit 1.  
  
[edit interfaces so-1/0/0]  
user@host# set unit 1 family mpls

**Results** Confirm the configuration of the firewall filter by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show interfaces
so-1/0/0 {
  unit 0 {
    family inet {
      address 192.168.1.1/24;
    }
    family vpls;
  }
  unit 1 {
    family mpls;
  }
}
```

### *Configuring a Physical Interface Policer*

**Step-by-Step Procedure** To configure a physical interface policer:

1. Enable configuration of the two-color policer.

```
[edit]
user@host# edit firewall policer shared-policer-A
```

2. Configure the type of two-color policer.

```
[edit firewall policer shared-policer-A]
user@host# set physical-interface-policer
```

3. Configure the traffic limits and the action for packets in a nonconforming traffic flow.

```
[edit firewall policer shared-policer-A]
user@host# set if-exceeding bandwidth-limit 100m burst-size-limit 500k
user@host# set then discard
```

For a physical interface filter, the actions you can configure for packets in a nonconforming traffic flow are to discard the packets, assign a forwarding class, assign a PLP value, or assign both a forwarding class and a PLP value.

**Results** Confirm the configuration of the policer by entering the **show firewall** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show firewall
policer shared-policer-A {
  physical-interface-policer;
  if-exceeding {
    bandwidth-limit 100m;
    burst-size-limit 500k;
  }
  then discard;
}
```

*Configuring an IPv4 Physical Interface Filter*

- Step-by-Step Procedure** To configure a physical interface policer as the action for terms in an IPv4 physical interface policer:
1. Configure a standard stateless firewall filter under a specific protocol family.  

```
[edit]
user@host# edit firewall family inet filter ipv4-filter
```

You cannot configure a physical interface firewall filter for **family any**.
  2. Configure the filter as a physical interface filter so that you can apply the physical interface policer as an action.  

```
[edit firewall family inet filter ipv4-filter]
user@host# set physical-interface-filter
```
  3. Configure the first term to match IPv4 packets received through TCP with the IP precedence fields **critical-ecp**, **immediate**, or **priority** and to apply the physical interface policer as a filter action.  

```
[edit firewall family inet filter ipv4-filter]
user@host# set term tcp-police-1 from precedence [ critical-ecp immediate priority ]
user@host# set term tcp-police-1 from protocol tcp
user@host# set term tcp-police-1 then policer shared-policer-A
```
  4. Configure the first term to match IPv4 packets received through TCP with the IP precedence fields **internet-control** or **routine** and to apply the physical interface policer as a filter action.  

```
[edit firewall family inet filter ipv4-filter]
user@host# set term tcp-police-2 from precedence [ internet-control routine ]
user@host# set term tcp-police-2 from protocol tcp
user@host# set term tcp-police-2 then policer shared-policer-A
```
- Results** Confirm the configuration of the firewall filter by entering the **show firewall** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show firewall
family inet {
  filter ipv4-filter {
    physical-interface-filter;
    term tcp-police-1 {
      from {
        precedence [ critical-ecp immediate priority ];
        protocol tcp;
      }
      then policer shared-policer-A;
    }
  }
  term tcp-police-2 {
    from {
      precedence [ internet-control routine ];
      protocol tcp;
    }
  }
}
```

```

    }
    then policer shared-policer-A;
  }
}
}
policer shared-policer-A {
  physical-interface-policer;
  if-exceeding {
    bandwidth-limit 100m;
    burst-size-limit 500k;
  }
  then discard;
}
}

```

### *Applying the IPv4 Physical interface Filter to a Physical Interface*

**Step-by-Step Procedure** To apply the physical interface filter to a physical interface:

1. Enable configuration of IPv4 on the logical interface.

```

[edit]
user@host# edit interfaces so-1/0/0 unit 0 family inet

```

2. Apply the IPv4 physical interface filter in the input direction.

```

[edit interfaces so-1/0/0 unit 0 family inet]
user@host# set filter input ipv4-filter

```

**Results** Confirm the configuration of the firewall filter by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```

[edit]
user@host# show interfaces
so-1/0/0 {
  unit 0 {
    family inet {
      filter {
        input ipv4-filter;
      }
      address 192.168.1.1/24;
    }
    family vpls;
  }
  unit 1 {
    family mpls;
  }
}

```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

Confirm that the configuration is working properly.

- [Displaying the Firewall Filters Applied to an Interface on page 144](#)
- [Displaying the Number of Packets Processed by the Policer at the Logical Interface on page 144](#)

### *Displaying the Firewall Filters Applied to an Interface*

**Purpose** Verify that the firewall filter **ipv4-filter** is applied to the IPv4 input traffic at logical interface **so-1/0/0.0**.

**Action** Use the **show interfaces statistics** operational mode command for logical interface **so-1/0/0.0**, and include the **detail** option. In the **Protocol inet** section of the command output, the **Input Filters** field shows that the firewall filter **ipv4-filter** is applied in the input direction.

```
user@host> show interfaces statistics so-1/0/0 detail
Logical interface so-1/0/0.0 (Index 79) (SNMP ifIndex 510) (Generation 149)
Flags: Hardware-Down Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
Protocol inet, MTU: 4470, Generation: 173, Route table: 0
Flags: Sendbcast-pkt-to-re, Protocol-Down
Input Filters: ipv4-filter
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
Destination: 10.39/16, Local: 10.39.1.1, Broadcast: 10.39.255.255,
Generation: 163
```

### *Displaying the Number of Packets Processed by the Policer at the Logical Interface*

**Purpose** Verify the traffic flow through the logical interface and that the policer is evaluated when packets are received on the logical interface.

**Action** Use the **show firewall** operational mode command for the filter you applied to the logical interface.

```
user@host> show firewall filter ipv4-filter
Filter: ipv4-filter
Policers:
Name                                     Packets
shared-policer-A-tcp-police-1           32863
shared-policer-A-tcp-police-2           3870
```

The command output displays the name of policer (**shared-policer-A**), the name of the filter term (**police-1**) under which the policer action is specified, and the number of packets that matched the filter term. This is only the number of out-of-specification (out-of-spec) packet counts, not all packets policed by the policer.

- Related Documentation**
- “Firewall Filter Match Conditions Based on Numbers or Text Aliases” in the [Junos OS Firewall Filter and Policer Configuration Guide](#)
  - “Firewall Filter Match Conditions Based on Bit-Field Values” in the [Junos OS Firewall Filter and Policer Configuration Guide](#)



- “Firewall Filter Match Conditions Based on Address Fields” in the *Junos OS Firewall Filter and Policer Configuration Guide*
- “Firewall Filter Match Conditions Based on Address Classes” in the *Junos OS Firewall Filter and Policer Configuration Guide*
- Statement Hierarchy for Configuring Policers on page 13
- Two-Color Policer Configuration Overview on page 15
- Three-Color Policer Configuration Overview on page 19
- Guidelines for Applying Traffic Policers on page 24
- **physical-interface-filter on page 198**
- **physical-interface-policer on page 199**



## CHAPTER 8

# Layer 2 Policers

- [Hierarchical Policers on page 147](#)
- [Two-Color and Three-Color Policers at Layer 2 on page 154](#)

## Hierarchical Policers

---

- [Hierarchical Policer Overview on page 147](#)
- [Example: Configuring a Hierarchical Policer on page 149](#)

### Hierarchical Policer Overview

You can use a hierarchical policer to rate-limit ingress Layer 2 traffic at a physical or logical interface and apply different policing actions based on whether the packets are classified for expedited forwarding (EF) or for a lower priority.

Hierarchical policing is supported on SONET interfaces hosted on M40e, M120, and M320 edge routers with incoming Flexible PIC Concentrators (FPCs) as SFPC and outgoing FPCs as FFPC, and on MX Series, T320, T640, and T1600 core routers with Enhanced Intelligent Queuing (IQE) PICs.

You can apply hierarchical policing to a physical interface or a logical interface. Applied to a physical interface configuration, a hierarchical policer rate-limits ingress Layer 2 traffic for all protocol families and logical interfaces configured on the physical interface. Applied to a logical interface configured with at least one protocol family, a hierarchical policer rate-limits ingress Layer 2 traffic for all protocol families configured on the logical interface. If you apply a hierarchical policer at a physical interface, you cannot also apply a hierarchical policer to any of the member logical interfaces.

A hierarchical policer configuration defines two policers—one for EF traffic only and another for non-EF traffic—that function in a hierarchical manner:

- **Premium policer**—You configure the premium policer with traffic limits for high-priority EF traffic only: a guaranteed bandwidth and a corresponding burst-size limit. EF traffic is categorized as nonconforming when its average arrival rate exceeds the guaranteed bandwidth and its average packet size exceeds the premium burst-size limit. For a premium policer, the only configurable action for nonconforming traffic is to discard the packets.

- **Aggregate policer**—You configure the aggregate policer with an aggregate bandwidth (to accommodate both high-priority EF traffic up to the guaranteed bandwidth and normal-priority non-EF traffic) and a burst-size limit for non-EF traffic only. Non-EF traffic is categorized as nonconforming when its average arrival rate exceeds the amount of aggregate bandwidth not currently consumed by EF traffic and its average packet size exceeds the burst-size limit defined in the aggregate policer. For an aggregate policer, the configurable actions for nonconforming traffic are to discard the packets, assign a forwarding class, assign a packet loss priority (PLP) level, or assign both a forwarding class and a PLP level to the packets.



**NOTE:** You must configure the bandwidth limit of the premium policer at or below the bandwidth limit of the aggregate policer. If the two bandwidth limits are equal, then non-EF traffic passes through the interface unrestricted only while no EF traffic arrives at the interface.

EF traffic is guaranteed the bandwidth specified as the premium bandwidth limit, while non-EF traffic is rate-limited to the amount of aggregate bandwidth not currently consumed by the EF traffic. Non-EF traffic is rate-limited to the entire aggregate bandwidth only while no EF traffic is present.

For example, suppose that you configure a hierarchical policer with the following components:

- Premium policer with bandwidth limit set to 2 Mbps, burst-size limit set to 3000 bytes, and nonconforming action set to discard packets.
- Aggregate policer with bandwidth limit set to 10 Mbps, burst-size limit set to 3000 bytes, and nonconforming action set to discard packets.

EF traffic is guaranteed a bandwidth of 2 Mbps. Bursts of EF traffic—EF traffic that arrives at the interface at rates above 2 Mbps—can also pass through the interface provided sufficient tokens are available in the 3000-byte bucket. When no tokens are available for a burst of non-EF traffic, packets are rate-limited using policing actions for the premium policer.

Non-EF traffic is metered to a bandwidth limit that ranges between 8 Mbps and 10 Mbps, depending on the average arrival rate of the EF traffic. Bursts of non-EF traffic—non-EF traffic that arrives at the interface at rates above the current limit for non-EF traffic—also pass through the interface provided sufficient tokens are available in the 3000-byte bucket. When non-EF traffic exceeds the currently allowed bandwidth or when no tokens are available for a burst of non-EF traffic, packets are rate-limited using policing actions for the aggregate policer.

## Example: Configuring a Hierarchical Policer

This example shows how to configure a hierarchical policer and apply the policer to ingress Layer 2 traffic at a logical interface on a supported platform.

- [Requirements on page 149](#)
- [Overview on page 149](#)
- [Configuration on page 149](#)
- [Verification on page 153](#)

### Requirements

---

Before you begin, be sure that your environment meets the following requirements:

- The interface on which you apply the hierarchical policer is a SONET interface hosted on one of the following routing platforms:
  - M40e, M120, or M320 edge router with incoming FPCs as SFPC and outgoing FPCs as FFPC.
  - MX Series, T320, T640, or T1600 core router with Enhanced Intelligent Queuing (IQE) PICs.
- No other policer is applied to the input of the interface on which you apply the hierarchical policer.
- You are aware that, if you apply the hierarchical policer to logical interface on which an input filter is also applied, the policer is executed first.

### Overview

---

In this example, you configure a hierarchical policer and apply the policer to ingress Layer 2 traffic at a logical interface.

#### *Topology*

You apply the policer to the SONET logical interface **so-1/0/0.0**, which you configure for IPv4 and VPLS traffic. When you apply the hierarchical policer to that logical interface, both IPv4 and VPLS traffic is hierarchically rate-limited.

You also configure the logical interface **so-1/0/0.1** for MPLS traffic. If you choose to apply the hierarchical policer to physical interface **so-1/0/0**, hierarchical policing would apply to IPv4 and VPLS traffic at **so-1/0/0.0** and to MPLS traffic at **so-1/0/0.1**.

### Configuration

---

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see [“Using the CLI Editor in Configuration Mode” on page 215](#).

To configure this example, perform the following tasks:

- [Defining the Interfaces on page 150](#)
- [Defining the Forwarding Classes on page 151](#)
- [Configuring the Hierarchical Policer on page 151](#)
- [Applying the Hierarchical Policer to Layer 2 Ingress Traffic at a Physical or Logical Interface on page 152](#)

#### CLI Quick Configuration

To quickly configure this example, copy the following configuration commands into a text file, remove any line breaks, and then paste the commands into the CLI at the **[edit]** hierarchy level.

```
set interfaces so-1/0/0 unit 0 family inet address 192.168.1.1/24
set interfaces so-1/0/0 unit 0 family vpls
set interfaces so-1/0/0 unit 1 family mpls
set class-of-service forwarding-classes class fc0 queue-num 0 priority high
  policing-priority premium
set class-of-service forwarding-classes class fc1 queue-num 1 priority low policing-priority
  normal
set class-of-service forwarding-classes class fc2 queue-num 2 priority low policing-priority
  normal
set class-of-service forwarding-classes class fc3 queue-num 3 priority low policing-priority
  normal
set firewall hierarchical-policer policer1 aggregate if-exceeding bandwidth-limit 300m
  burst-size-limit 30k
set firewall hierarchical-policer policer1 aggregate then forwarding-class fc1
set firewall hierarchical-policer policer1 premium if-exceeding bandwidth-limit 100m
  burst-size-limit 50k
set firewall hierarchical-policer policer1 premium then discard
set interfaces so-1/0/0 unit 0 layer2-policer input-hierarchical-policer policer1
```

#### *Defining the Interfaces*

#### Step-by-Step Procedure

To define the interfaces:

1. Enable configuration of the physical interface.

```
[edit]
user@host# edit interfaces so-1/0/0
```

2. Configure logical unit 0.

```
[edit interfaces so-1/0/0]
user@host# set unit 0 family inet address 192.168.1.1/24
user@host# set unit 0 family vpls
```

If you apply a Layer 2 policer to this logical interface, you must configure at least one protocol family.

3. Configure logical unit 1.

```
[edit interfaces so-1/0/0]
user@host# set unit 1 family mpls
```

**Results** Confirm the configuration of the interfaces by entering the **show interfaces** configuration command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show interfaces
so-1/0/0 {
  unit 0 {
    family inet {
      address 192.168.1.1/24;
    }
    family vpls;
  }
  unit 1 {
    family mpls;
  }
}
```

### *Defining the Forwarding Classes*

**Step-by-Step Procedure** To define the forwarding classes referenced as aggregate policer actions:

1. Enable configuration of the forwarding classes.

```
[edit]
user@host# edit class-of-service forwarding-classes
```

2. Define the forwarding classes.

```
[edit class-of-service forwarding-classes]
user@host# set class fc0 queue-num 0 priority high policing-priority premium
user@host# set class fc1 queue-num 1 priority low policing-priority normal
user@host# set class fc2 queue-num 2 priority low policing-priority normal
user@host# set class fc3 queue-num 3 priority low policing-priority normal
```

**Results** Confirm the configuration of the forwarding classes referenced as aggregate policer actions by entering the **show class-of-service** configuration command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show class-of-service
forwarding-classes {
  class fc0 queue-num 0 priority high policing-priority premium;
  class fc1 queue-num 1 priority low policing-priority normal;
  class fc2 queue-num 2 priority low policing-priority normal;
  class fc3 queue-num 3 priority low policing-priority normal;
}
```

### *Configuring the Hierarchical Policier*

**Step-by-Step Procedure** To configure a hierarchical policer:

1. Enable configuration of the hierarchical policer.

```
[edit]
user@host# edit firewall hierarchical-policer policer1
```

2. Configure the aggregate policer.

```
[edit firewall hierarchical-policer policer1]
user@host# set aggregate if-exceeding bandwidth-limit 300m burst-size-limit 30k
user@host# set aggregate then forwarding-class fc1
```

For the aggregate policer, the configurable actions for a packet in a nonconforming flow are to discard the packet, change the loss priority, change the forwarding class, or change both the loss priority and the forwarding class.

3. Configure the premium policer.

```
[edit firewall hierarchical-policer policer1]
user@host# set premium if-exceeding bandwidth-limit 100m burst-size-limit 50k
user@host# set premium then discard
```

The bandwidth limit for the premium policer must not be greater than that of the aggregate policer.

For the premium policer, the only configurable action for a packet in a nonconforming traffic flow is to discard the packet.

**Results** Confirm the configuration of the hierarchical policer by entering the **show firewall** configuration command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show firewall
hierarchical-policer policer1 {
  aggregate {
    if-exceeding {
      bandwidth-limit 300m;
      burst-size-limit 30k;
    }
    then {
      forwarding-class fc1;
    }
  }
  premium {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 50k;
    }
    then {
      discard;
    }
  }
}
```

#### *Applying the Hierarchical Policer to Layer 2 Ingress Traffic at a Physical or Logical Interface*

**Step-by-Step Procedure** To hierarchically rate-limit Layer 2 ingress traffic for IPv4 and VPLS traffic only on logical interface **so-1/0/0.0**, reference the policer from the logical interface configuration:

1. Enable configuration of the logical interface.

```
[edit]
```



```
user@host# edit interfaces so-1/0/0 unit 0
```

When you apply a policer to Layer 2 traffic at a logical interface, you must define at least one protocol family for the logical interface.

2. Apply the policer to the logical interface.

```
[edit]
user@host# set layer2-policer input-hierarchical-policer policer1
```

Alternatively, to hierarchically rate-limit Layer 2 ingress traffic for all protocol families and for *all logical interfaces* configured on physical interface **so-1/0/0**, you could reference the policer from the physical interface configuration.

**Results** Confirm the configuration of the hierarchical policer by entering the **show interfaces** configuration command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show interfaces
so-1/0/0 {
  unit 0 {
    layer2-policer {
      input-hierarchical-policer policer1;
    }
    family inet {
      address 192.168.1.1/24;
    }
    family vpls;
  }
  unit 1 {
    family mpls;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

Confirm that the configuration is working properly.

- [Displaying Traffic Statistics and Policers for the Logical Interface on page 153](#)
- [Displaying Statistics for the Policer on page 154](#)

### *Displaying Traffic Statistics and Policers for the Logical Interface*

**Purpose** Verify the traffic flow through the logical interface and that the policer is evaluated when packets are received on the logical interface.

**Action** Use the **show interfaces** operational mode command for logical interface **so-1/0/0.0**, and include the **detail** or **extensive** option. The command output section for **Traffic statistics** lists the number of bytes and packets received and transmitted on the logical interface, and the **Protocol inet** section contains a **Policer** field that would list the policer **policer1** as an input or output policer as follows:

- **Input:** policer1-so-1/0/0.0-inet-i
- **Output:** policer1-so-1/0/0.0-inet-o

In this example, the policer is applied to logical interface traffic in the input direction only.

#### *Displaying Statistics for the Policer*

**Purpose** Verify the number of packets evaluated by the policer.

**Action** Use the **show policer** operational mode command and optionally specify the name of the policer. The command output displays the number of packets evaluated by each configured policer (or the specified policer), in each direction. For the policer **policer1**, the input and output policer names are displayed as follows:

- **policer1-so-1/0/0.0-inet-i**
- **policer1-so-1/0/0.0-inet-o**

The **-inet-i** suffix denotes a policer applied to IPv4 input traffic, while the **-inet-o** suffix denotes a policer applied to IPv4 output traffic. In this example, the policer is applied to input traffic only.

- Related Documentation**
- [Statement Hierarchy for Configuring Policers on page 13](#)
  - [Hierarchical Policer Configuration Overview on page 22](#)
  - [Guidelines for Applying Traffic Policers on page 24](#)

---

## Two-Color and Three-Color Policers at Layer 2

- [Two-Color Policing at Layer 2 Overview on page 154](#)
- [Three-Color Policing at Layer 2 Overview on page 156](#)
- [Example: Configuring a Three-Color Logical Interface \(Aggregate\) Policer on page 157](#)

### Two-Color Policing at Layer 2 Overview

This topic covers the following information:

- [Guidelines for Configuring Two-Color Policing of Layer 2 Traffic on page 155](#)
- [Statement Hierarchy for Configuring a Two-Color Policer for Layer 2 Traffic on page 155](#)
- [Statement Hierarchy for Applying a Two-Color Policer to Layer 2 Traffic on page 155](#)

### Guidelines for Configuring Two-Color Policing of Layer 2 Traffic

The following guidelines apply to two-color policing of Layer 2 traffic:

- You can apply a two-color policer to ingress or egress Layer 2 traffic at a logical interface hosted on a Gigabit Ethernet interface (**ge-**) or a 10-Gigabit Ethernet interface (**xe-**) only.
- A single logical interface supports Layer 2 policing in both directions.
- You can apply a two-color policer to Layer 2 traffic as a logical interface policer only. You cannot apply a two-color policer to Layer 2 traffic as a stateless firewall filter action.
- You can apply a two-color policer to Layer 2 traffic by referencing the policer in the interface configuration at the logical unit level, and not at the protocol level.

For information about configuring three-color policing of Layer 2 traffic, see [“Three-Color Policing at Layer 2 Overview” on page 156](#).

### Statement Hierarchy for Configuring a Two-Color Policer for Layer 2 Traffic

To enable a single-rate two-color policer to rate-limit Layer 2 traffic, include the **logical-interface-policer** statement in the **policer** configuration.

```

firewall {
  policer policer-name {
    logical-interface-policer;
    if-exceeding {
      (bandwidth-limit bps | bandwidth-percent percentage);
      burst-size-limit bytes;
    }
    then {
      discard;
      forwarding-class class-name;
      loss-priority (high | low | medium-high | medium-low);
    }
  }
}

```

You can include the configuration at the following hierarchy levels:

- **[edit]**
- **[edit logical-systems *logical-system-name*]**

### Statement Hierarchy for Applying a Two-Color Policer to Layer 2 Traffic

To apply a logical interface policer to Layer 2 traffic, include the **layer2-policer input-policer *policer-name*** statement or the **layer2-policer output-policer *policer-name*** statement to a supported logical interface. Use the **input-policer** or **output-policer** statements to apply a two-color policer at Layer 2.

```

interfaces {
  (ge-fpc/pic/port | xe-fpc/pic/port) {
    unit unit-number {

```

```

    layer2-policer {
        input-policer policer-name;
        output-policer policer-name;
    }
}

```

You can include the configuration at the following hierarchy levels:

- **[edit]**
- **[edit logical-systems *logical-system-name*]**

## Three-Color Policing at Layer 2 Overview

This topic covers the following information:

- [Guidelines for Configuring Three-Color Policing of Layer 2 Traffic on page 156](#)
- [Statement Hierarchy for Configuring a Three-Color Policer for Layer 2 Traffic on page 156](#)
- [Statement Hierarchy for Applying a Three-Color Policer to Layer 2 Traffic on page 157](#)

### Guidelines for Configuring Three-Color Policing of Layer 2 Traffic

The following guidelines apply to three-color policing of Layer 2 traffic:

- You can apply a three-color policer to Layer 2 traffic at a logical interface hosted on a Gigabit Ethernet interface (**ge-**) or a 10-Gigabit Ethernet interface (**xe-**) only.
- A single logical interface supports Layer 2 policing in both directions.
- You can apply a three-color policer to Layer 2 traffic as a logical interface policer only. You cannot apply a two-color policer to Layer 2 traffic as a stateless firewall filter action.
- You can apply a three-color policer to Layer 2 traffic by referencing the policer in the interface configuration at the logical unit level, and not at the protocol level.
- You can apply a color-aware three-color policer to Layer 2 traffic in the egress direction only, but you apply a color-blind three-color policer to Layer 2 traffic in either direction.

For information about configuring two-color policing of Layer 2 traffic, see [“Two-Color Policing at Layer 2 Overview” on page 154](#).

### Statement Hierarchy for Configuring a Three-Color Policer for Layer 2 Traffic

To enable a single-rate or two-rate three-color policer to rate-limit Layer 2 traffic, include the **logical-interface-policer** statement in the **three-color-policer** configuration.

```

firewall {
    three-color-policer policer-name {
        action {
            loss-priority high then discard;
        }
        logical-interface-policer;
        single-rate {

```

```

    (color-aware | color-blind);
    committed-burst-size bytes;
    committed-information-rate bps;
    excess-burst-size bytes;
}
two-rate {
    (color-aware | color-blind);
    committed-burst-size bytes;
    committed-information-rate bps;
    peak-burst-size bytes;
    peak-information-rate bps;
}
}
}

```

You can include the configuration at the following hierarchy levels:

- [\[edit\]](#)
- [\[edit logical-systems \*logical-system-name\*\]](#)

### Statement Hierarchy for Applying a Three-Color Policer to Layer 2 Traffic

To apply a logical interface policer to Layer 2 traffic, include the **layer2-policer** statement for a supported logical interface at the logical unit level. Use the **input-three-color *policer-name*** statement or **output-three-color *policer-name*** statement to specify the direction of the traffic to be policed.

```

interfaces {
    (ge-fpc/pic/port | xe-fpc/pic/port) {
        unit unit-number {
            layer2-policer {
                input-three-color policer-name;
                output-three-color policer-name;
            }
        }
    }
}

```

You can include the configuration at the following hierarchy levels:

- [\[edit\]](#)
- [\[edit logical-systems \*logical-system-name\*\]](#)

### Example: Configuring a Three-Color Logical Interface (Aggregate) Policer

This example shows how to configure a two-rate three-color color-blind policer as a logical interface (aggregate) policer and apply the policer directly to Layer 2 input traffic at a supported logical interface.

- [Requirements on page 158](#)
- [Overview on page 158](#)
- [Configuration on page 159](#)
- [Verification on page 162](#)

## Requirements

---

Before you begin, make sure that the logical interface to which you apply the three-color logical interface policer is hosted on a Gigabit Ethernet interface (**ge-**) or a 10-Gigabit Ethernet interface (**xe-**) on an MX Series router.

## Overview

---

A two-rate three-color policer meters a traffic flow against a bandwidth limit and burst-size limit for guaranteed traffic, plus a second set of bandwidth and burst-size limits for peak traffic. Traffic that conforms to the limits for guaranteed traffic is categorized as green, and nonconforming traffic falls into one of two categories:

- Nonconforming traffic that does not exceed the bandwidth and burst-size limits for peak traffic is categorized as yellow.
- Nonconforming traffic that exceeds the bandwidth and burst-size limits for peak traffic is categorized as red.

A logical interface policer defines traffic rate-limiting rules that you can apply to multiple protocol families on the same logical interface without creating multiple instances of the policer.



**NOTE:** You apply a logical interface policer directly to a logical interface at the logical unit level, and not by referencing the policer in a stateless firewall filter and then applying the filter to the logical interface at the protocol family level.

---

## Topology

In this example, you configure the two-rate three-color policer **trTCM2-cb** as a color-blind logical interface policer and apply the policer to incoming Layer 2 traffic on logical interface **ge-1/3/1.0**.



**NOTE:** When using a three-color policer to rate-limit Layer 2 traffic, color-aware policing can be applied to egress traffic only.

---

The policer defines guaranteed traffic rate limits such that traffic that conforms to the bandwidth limit of 40 Mbps with a 100 KB allowance for traffic bursting (based on the token-bucket formula) is categorized as green. As with any policed traffic, the packets in a green flow are implicitly set to a **low** loss priority and then transmitted.

Nonconforming traffic that falls within the peak traffic limits of a 60 Mbps bandwidth limit and a 200 KB allowance for traffic bursting (based on the token-bucket formula) is categorized as yellow. The packets in a yellow traffic flow are implicitly set to a **medium-high** loss priority and then transmitted.

Nonconforming traffic that exceeds the peak traffic limits are categorized as red. The packets in a red traffic flow are implicitly set to a **high** loss priority. In this example, the

optional policer action for red traffic (**loss-priority high then discard**) is configured, so packets in a red traffic flow are discarded instead of transmitted.

### Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see [“Using the CLI Editor in Configuration Mode” on page 215](#).

To configure this example, perform the following tasks:

- [Configuring the Logical Interfaces on page 159](#)
- [Configuring the Two-Rate Three-Color Policer as a Logical Interface Policer on page 160](#)
- [Applying the Three-Color Policer to the Layer 2 Input at the Logical Interface on page 161](#)

#### CLI Quick Configuration

To quickly configure this example, copy the following configuration commands into a text file, remove any line breaks, and then paste the commands into the CLI at the **[edit]** hierarchy level.

```
set interfaces ge-1/3/1 vlan-tagging
set interfaces ge-1/3/1 unit 0 vlan-id 100
set interfaces ge-1/3/1 unit 0 family inet address 10.10.10.1/30
set interfaces ge-1/3/1 unit 1 vlan-id 101
set interfaces ge-1/3/1 unit 1 family inet address 20.20.20.1/30 arp 20.20.20.2 mac
  00:00:11:22:33:44
set firewall three-color-policer trTCM2-cb logical-interface-policer
set firewall three-color-policer trTCM2-cb two-rate color-blind
set firewall three-color-policer trTCM2-cb two-rate committed-information-rate 40m
set firewall three-color-policer trTCM2-cb two-rate committed-burst-size 100k
set firewall three-color-policer trTCM2-cb two-rate peak-information-rate 60m
set firewall three-color-policer trTCM2-cb two-rate peak-burst-size 200k
set firewall three-color-policer trTCM2-cb action loss-priority high then discard
set interfaces ge-1/3/1 unit 0 layer2-policer input-three-color trTCM2-cb
```

#### Configuring the Logical Interfaces

#### Step-by-Step Procedure

To configure the logical interfaces:

1. Enable configuration of the interface.  
  
[edit]  
user@host# edit interfaces ge-1/3/1
2. Configure single tagging.  
  
[edit interfaces ge-1/3/1]  
user@host# set vlan-tagging
3. Configure logical interface ge-1/3/1.0.  
  
[edit interfaces ge-1/3/1]  
user@host# set unit 0 vlan-id 100  
user@host# set unit 0 family inet address 10.10.10.1/30
4. Configure logical interface ge-1/3/1.0.  
  
[edit interfaces ge-1/3/1]

```

user@host# set unit 1 vlan-id 101
user@host# set unit 1 family inet address 20.20.20.1/30 arp 20.20.20.2 mac
00:00:11:22:33:44

```

**Results** Confirm the configuration of the logical interfaces by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```

[edit]
user@host# show interfaces
ge-1/3/1 {
  vlan-tagging;
  unit 0 {
    vlan-id 100;
    family inet {
      address 10.10.10.1/30;
    }
  }
  unit 1 {
    vlan-id 101;
    family inet {
      address 20.20.20.1/30 {
        arp 20.20.20.2 mac 00:00:11:22:33:44;
      }
    }
  }
}

```

### *Configuring the Two-Rate Three-Color Policer as a Logical Interface Policer*

**Step-by-Step Procedure** To configure the two-rate three-color policer as a logical interface policer:

1. Enable configuration of a three-color policer.

```

[edit]
user@host# edit firewall three-color-policer trTCM2-cb

```

2. Specify that the policer is a logical interface (aggregate) policer.

```

[edit firewall three-color-policer trTCM2-cb]
user@host# set logical-interface-policer

```

A logical interface policer rate-limits traffic based on a percentage of the media rate of the physical interface underlying the logical interface to which the policer is applied, and the policer is applied directly to the interface rather than referenced by a firewall filter.

3. Specify that the policer is two-rate and color-blind.

```

[edit firewall three-color-policer trTCM2-cb]
user@host# set two-rate color-blind

```

A color-aware three-color policer takes into account any coloring markings that might have been set for a packet by another traffic policer configured at a previous network node, and any preexisting color markings are used in determining the appropriate policing action for the packet.



Because you are applying this three-color policer applied to input at Layer 2, you must configure the policer to be color-blind.

4. Specify the policer traffic limits used to classify a green traffic flow.

```
[edit firewall three-color-policer trTCM2-cb]
user@host# set two-rate committed-information-rate 40m
user@host# set two-rate committed-burst-size 100k
```

5. Specify the additional policer traffic limits used to classify a yellow or red traffic flow.

```
[edit firewall three-color-policer trTCM2-cb]
user@host# set two-rate peak-information-rate 60m
user@host# set two-rate peak-burst-size 200k
```

6. (Optional) Specify the configured policer action for packets in a red traffic flow.

```
[edit firewall three-color-policer trTCM2-cb]
user@host# set action loss-priority high then discard
```

In color-aware mode, the three-color policer configured action can increase the packet loss priority (PLP) level 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.

**Results** Confirm the configuration of the three-color policer by entering the **show firewall** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show firewall
three-color-policer trTCM2-cb {
  logical-interface-policer;
  action {
    loss-priority high then discard;
  }
  two-rate {
    color-blind;
    committed-information-rate 40m;
    committed-burst-size 100k;
    peak-information-rate 60m;
    peak-burst-size 200k;
  }
}
```

#### *Applying the Three-Color Policer to the Layer 2 Input at the Logical Interface*

#### **Step-by-Step Procedure**

To apply the three-color policer to the Layer 2 input at the logical interface:

1. Enable application of Layer 2 logical interface policers.

```
[edit]
user@host# edit interfaces ge-1/3/1 unit 0
```

2. Apply the three-color logical interface policer to a logical interface input.

```
[edit interfaces ge-1/3/1 unit 0]
```

```
user@host# set layer2-policer input-three-color trTCM2-cb
```

**Results** Confirm the configuration of the logical interfaces by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this procedure to correct the configuration.

```
[edit]
user@host# show interfaces
ge-1/3/1 {
  vlan-tagging;
  unit 0 {
    vlan-id 100;
    layer2-policer {
      input-three-color trTCM2-cb;
    }
    family inet {
      address 10.10.10.1/30;
    }
  }
  unit 1 {
    vlan-id 101;
    family inet {
      address 20.20.20.1/30 {
        arp 20.20.20.2 mac 00:00:11:22:33:44;
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

---

### Verification

Confirm that the configuration is working properly.

- [Displaying Traffic Statistics and Policers for the Logical Interface on page 162](#)
- [Displaying Statistics for the Policer on page 163](#)

#### *Displaying Traffic Statistics and Policers for the Logical Interface*

**Purpose** Verify the traffic flow through the logical interface and that the policer is evaluated when packets are received on the logical interface.

**Action** Use the **show interfaces** operational mode command for logical interface **ge-1/3/1.0**, and include the **detail** or **extensive** option. The command output section for **Traffic statistics** lists the number of bytes and packets received and transmitted on the logical interface, and the **Protocol inet** section contains a **Policer** field that would list the policer **trTCM2-cb** as an input or output policer as follows:

- Input: trTCM2-cb-ge-1/3/1.0-log\_int-i
- Output: trTCM2-cb-ge-1/3/1.0-log\_int-o

The **log\_int-i** suffix denotes a logical interface policer applied to input traffic, while the **log\_int-o** suffix denotes a logical interface policer applied to output traffic. In this example, the logical interface policer is applied to in the input direction only.

#### *Displaying Statistics for the Policer*

**Purpose** Verify the number of packets evaluated by the policer.

**Action** Use the **show policer** operational mode command and optionally specify the name of the policer. The command output displays the number of packets evaluated by each configured policer (or the specified policer), in each direction. For the policer **trTCM2-cb**, the input and output policer names are displayed as follows:

- **trTCM2-cb-ge-1/3/1.0-log\_int-i**
- **trTCM2-cb-e-1/3/1.0-log\_int-o**

The **log\_int-i** suffix denotes a logical interface policer applied to input traffic, while the **log\_int-o** suffix denotes a logical interface policer applied to output traffic. In this example, the logical interface policer is applied to input traffic only.

- Related Documentation**
- [Statement Hierarchy for Configuring Policers on page 13](#)
  - [Guidelines for Applying Traffic Policers on page 24](#)
  - [layer2-policer on page 189](#)
  - [logical-interface-policer on page 190](#)
  - [policer \(Configuring\) on page 201](#)
  - [three-color-policer \(Configuring\) on page 207](#)



# Policer Configuration Statements

## action

---

**Syntax**    action {  
                  loss-priority high then discard;  
                  }

**Hierarchy Level**    [edit firewall [three-color-policer name](#)],  
                          [edit logical-systems *logical-system-name* firewall [three-color-policer name](#)]

**Release Information**    Statement introduced in Junos OS Release 8.2.  
                              Logical systems support introduced in Junos OS Release 9.3.

**Description**    Discard traffic on a logical interface using tricolor marking policing.



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

**Options**    The statements are explained separately.

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

**Related Documentation**

- [Three-Color Policer Configuration Overview on page 19](#)
- [Basic Single-Rate Three-Color Policers on page 111](#)
- [Basic Two-Rate Three-Color Policers on page 117](#)
- [Two-Color and Three-Color Logical Interface Policers on page 125](#)
- [Two-Color and Three-Color Physical Interface Policers on page 137](#)
- [Two-Color and Three-Color Policers at Layer 2 on page 154](#)
- [loss-priority high then discard on page 192](#)

## aggregate (Hierarchical Policer)


---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>aggregate {<br/>    if-exceeding {<br/>        bandwidth-limit <i>bandwidth</i>;<br/>        burst-size-limit <i>burst</i>;<br/>    }<br/>    then {<br/>        discard;<br/>    }<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit firewall <a href="#">hierarchical-policer</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b>              | On M40e, M120, and M320 edge routers with Flexible PIC Concentrator (FPC) input as FFPC and FPC output as SFPC, and on MX Series, T320, T640, and T1600 edge routers with Enhanced Intelligent Queuing (IQE) PICs, configure an aggregate hierarchical policer.                                                                                                                                                                                                                                                                                           |
| <b>Options</b>                  | Options are described separately.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Hierarchical Policer Configuration Overview on page 22</a></li><li>• <a href="#">Hierarchical Policers on page 147</a></li><li>• <a href="#">bandwidth-limit (Hierarchical Policer) on page 167</a></li><li>• <a href="#">burst-size-limit (Hierarchical Policer) on page 172</a></li><li>• <a href="#">hierarchical-policer on page 184</a></li><li>• <a href="#">if-exceeding (Hierarchical Policer) on page 185</a></li><li>• <a href="#">premium (Hierarchical Policer) on page 205</a></li></ul> |

## bandwidth-limit (Hierarchical Policer)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>bandwidth-limit <i>bps</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit firewall <a href="#">hierarchical-policer aggregate if-exceeding</a> ],<br>[edit firewall <a href="#">hierarchical-policer premium if-exceeding</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b>              | For M40e, M120, and M320 (with FFPC and SFPC) edge routers and T320, T640, and T1600 core routers with Enhanced Intelligent Queuing (IQE) PICs, configure the maximum average bandwidth for premium or aggregate traffic in a hierarchical policer.                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Options</b>                  | <p><b><i>bps</i></b>—You can specify the number of bits per second either as a decimal number or as a decimal number followed by the abbreviation <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000).</p> <p><b>Range:</b> 32,000 through 50,000,000,000</p>                                                                                                                                                                                                                                                                                                                                                                                    |
| <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="#">Hierarchical Policer Configuration Overview on page 22</a></li> <li>• <a href="#">Policer Bandwidth and Burst-Size Limits on page 25</a></li> <li>• <a href="#">Policer Color-Marking and Actions on page 26</a></li> <li>• <a href="#">Single Token Bucket Algorithm on page 28</a></li> <li>• <a href="#">Calculation of Policer Burst-Size Limit on page 33</a></li> <li>• <a href="#">aggregate (Hierarchical Policer) on page 166</a></li> <li>• <a href="#">burst-size-limit (Hierarchical Policer) on page 172</a></li> <li>• <a href="#">premium (Hierarchical Policer) on page 205</a></li> </ul> |

## bandwidth-limit (Policer)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>bandwidth-limit <i>bps</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit firewall <code>policer <i>policer-name</i> if-exceeding</code> ],<br>[edit logical-systems <code>logical-system-name <i>policer</i> <i>policer-name</i> if-exceeding</code> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | <p>For a single-rate two-color policer, configure the bandwidth limit as a number of bits per second. Single-rate two-color policing uses the single token bucket algorithm to measure traffic-flow conformance to a two-color policer rate limit.</p> <p>Traffic at the interface that conforms to the bandwidth limit is categorized green. Traffic that exceeds the specified rate is also categorized as green provided that sufficient tokens remain in the single token bucket. Packets in a green flow are implicitly marked with <b>low</b> packet loss priority (PLP) and then passed through the interface.</p> <p>Traffic that exceeds the specified rate when insufficient tokens remain in the single token bucket is categorized red. Depending on the configuration of the two-color policer, packets in a red traffic flow might be implicitly discarded; or the packets might be re-marked with a specified forwarding class, a specified PLP, or both, and then passed through the interface.</p> <div style="margin-top: 20px;">  <p><b>NOTE:</b> This statement specifies the bandwidth limit as an absolute number of bits per second. Alternatively, for single-rate two-color policers only, you can use the <code>bandwidth-percent <i>percentage</i></code> statement to specify the bandwidth limit as a percentage of either the physical interface port speed or the configured logical interface shaping rate.</p> </div> <p>Single-rate two-color policing allows bursts of traffic for short periods, whereas single-rate and two-rate three-color policing allows more sustained bursts of traffic.</p> <p>Hierarchical policing is a form of two-color policing that applies different policing actions based on whether the packets are classified for expedited forwarding (EF) or for a lower priority. You apply a hierarchical policer to ingress Layer 2 traffic to allow bursts of EF traffic for short period and bursts of non-EF traffic for short periods, with EF traffic always taking precedence over non-EF traffic.</p> |
| <b>Options</b>                  | <p><b><i>bps</i></b>—You can specify the number of bits per second either as a decimal number or as a decimal number followed by the abbreviation <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000).</p> <p><b>Range:</b> (M Series, MX Series, and T Series routers) 8000 through 50,000,000,000</p> <p><b>Default:</b> None.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |



- Related Documentation**
- [Two-Color Policer Configuration Overview on page 15](#)
  - [Policer Bandwidth and Burst-Size Limits on page 25](#)
  - [Policer Color-Marking and Actions on page 26](#)
  - [Single Token Bucket Algorithm on page 28](#)
  - [Calculation of Policer Burst-Size Limit on page 33](#)
  - [bandwidth-percent on page 170](#)
  - [burst-size-limit \(Policer\) on page 173](#)

## bandwidth-percent

|                            |                                                                                                                                                                                                                                               |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>bandwidth-percent <i>percentage</i>;</code>                                                                                                                                                                                             |
| <b>Hierarchy Level</b>     | [edit firewall <code>policer <i>policer-name</i> if-exceeding</code> ],<br>[edit logical-systems <code>logical-system-name <i>policer</i> <i>policer-name</i> if-exceeding</code> ]                                                           |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                             |
| <b>Description</b>         | For a single-rate two-color policer, configure the bandwidth limit as a percentage value. Single-rate two-color policing uses the <i>single token bucket algorithm</i> to measure traffic-flow conformance to a two-color policer rate limit. |

Traffic at the interface that conforms to the bandwidth limit is categorized green. Traffic that exceeds the specified rate is also categorized as green provided that sufficient tokens remain in the single token bucket. Packets in a green flow are implicitly marked with **low** packet loss priority and then passed through the interface.

Traffic that exceeds the specified rate when insufficient tokens remain in the single token bucket is categorized red. Depending on the configuration of the two-color policer, packets in a red traffic flow might be implicitly discarded; or the packets might be re-marked with a specified forwarding class, a specified PLP, or both, and then passed through the interface.



**NOTE:** This statement specifies the bandwidth limit as a percentage of either the physical interface port speed or the configured logical interface shaping rate. Alternatively, you can use the `bandwidth-limit bps` statement to specify the bandwidth limit as an absolute number of bits per second.

The function of the bandwidth limit is extended by the burst size (configured using the `burst-size-limit bytes` statement) to allow bursts of traffic up to a limit based on the overall traffic load:

- When a single-rate two-color policer is applied to the input or output traffic at an interface, the initial capacity for traffic bursting is equal to the number of bytes specified by this statement.
- During periods of relatively low traffic (traffic that arrives at or departs from the interface at overall rates below the token arrival rate), unused tokens accumulate in the bucket, but only up to the configured token bucket depth.

Single-rate two-color policing allows bursts of traffic for short periods, whereas single-rate and two-rate three-color policing allows more sustained bursts of traffic.

Hierarchical policing is a form of two-color policing that applies different policing actions based on whether the packets are classified for expedited forwarding (EF) or for a lower priority. You apply a hierarchical policer to ingress Layer 2 traffic to allow bursts of EF

traffic for short period and bursts of non-EF traffic for short periods, with EF traffic always taking precedence over non-EF traffic.

**Options** *percentage*—Traffic rate as a percentage of either the physical interface media rate or the logical interface configured shaping rate. You can configure a shaping rate on a logical interface by using class-of-service statement.



**NOTE:** You cannot rate-limit based on bandwidth percentage for aggregate, tunnel, and software interfaces. The bandwidth percentage policer cannot be used for forwarding table filters. Bandwidth percentage policers can only be used for interface-specific filters.

**Range:** 0 through 100

**Default:** None.

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

**Related Documentation**

- [Two-Color Policer Configuration Overview on page 15](#)
- [Policer Bandwidth and Burst-Size Limits on page 25](#)
- [Policer Color-Marking and Actions on page 26](#)
- [Single Token Bucket Algorithm on page 28](#)
- [Calculation of Policer Burst-Size Limit on page 33](#)
- [Bandwidth Policers on page 55](#)
- [bandwidth-limit \(Policer\) on page 168](#)
- [burst-size-limit \(Policer\) on page 173](#)

## burst-size-limit (Hierarchical Policer)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>burst-size-limit <i>bytes</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | [edit firewall <a href="#">hierarchical-policer aggregate if-exceeding</a> ],<br>[edit firewall <a href="#">hierarchical-policer premium if-exceeding</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | For M40e, M120, and M320 (with FFPC and SFPC) edge routers and T320, T640, and T1600 core routers with Enhanced Intelligent Queuing (IQE) PICs, configure the burst-size limit for premium or aggregate traffic in a hierarchical policer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <b><i>bytes</i></b> —Burst-size limit in bytes. The minimum recommended value is the maximum transmission unit (MTU) of the IP packets being policed. You can specify the value either as a complete decimal number or as a decimal number followed by the abbreviation <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000).<br><b>Range:</b> 1500 through 2,147,450,880                                                                                                                                                                                                                                                                                                                           |
| <b>Required Privilege Level</b> | <b>firewall</b> —To view this statement in the configuration.<br><b>firewall-control</b> —To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Hierarchical Policer Configuration Overview on page 22</a></li><li>• <a href="#">Policer Bandwidth and Burst-Size Limits on page 25</a></li><li>• <a href="#">Policer Color-Marking and Actions on page 26</a></li><li>• <a href="#">Single Token Bucket Algorithm on page 28</a></li><li>• <a href="#">Calculation of Policer Burst-Size Limit on page 33</a></li><li>• <a href="#">Hierarchical Policers on page 147</a></li><li>• <a href="#">aggregate (Hierarchical Policer) on page 166</a></li><li>• <a href="#">bandwidth-limit (Hierarchical Policer) on page 167</a></li><li>• <a href="#">premium (Hierarchical Policer) on page 205</a></li></ul> |

## burst-size-limit (Policer)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>burst-size-limit bytes;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>     | [edit firewall <b>policer</b> <i>policer-name</i> <b>if-exceeding</b> ],<br>[edit logical-systems <i>logical-system-name</i> <b>policer</b> <i>policer-name</i> <b>if-exceeding</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b>         | <p>For a single-rate two-color policer, configure the burst size as a number of bytes. The burst size allows for short periods of traffic bursting (back-to-back traffic at average rates that exceed the configured bandwidth limit). Single-rate two-color policing uses the <i>single token bucket algorithm</i> to measure traffic-flow conformance to a two-color policer rate limit.</p> <p>Traffic at the interface that conforms to the bandwidth limit is categorized green. Traffic that exceeds the specified rate is also categorized as green provided that sufficient tokens remain in the single token bucket. Packets in a green flow are implicitly marked with <b>low</b> packet loss priority and then passed through the interface.</p> <p>Traffic that exceeds the specified rate when insufficient tokens remain in the single token bucket is categorized red. Depending on the configuration of the two-color policer, packets in a red traffic flow might be implicitly discarded; or the packets might be re-marked with a specified forwarding class, a specified PLP, or both, and then passed through the interface.</p> <p>The burst size extends the function of the bandwidth limit (configured using either the <b>bandwidth-limit bps</b> statement or the <b>bandwidth-percent percentage</b> statement) to allow bursts of traffic up to a limit based on the overall traffic load:</p> <ul style="list-style-type: none"> <li>• When a single-rate two-color policer is applied to the input or output traffic at an interface, the initial capacity for traffic bursting is equal to the number of bytes specified by this statement.</li> <li>• During periods of relatively low traffic (traffic that arrives at or departs from the interface at overall rates below the token arrival rate), unused tokens accumulate in the bucket, but only up to the configured token bucket depth.</li> </ul> <p>Single-rate two-color policing allows bursts of traffic for short periods, whereas single-rate and two-rate three-color policing allows more sustained bursts of traffic.</p> <p>Hierarchical policing is a form of two-color policing that applies different policing actions based on whether the packets are classified for expedited forwarding (EF) or for a lower priority. You apply a hierarchical policer to ingress Layer 2 traffic to allow bursts of EF traffic for short period and bursts of non-EF traffic for short periods, with EF traffic always taking precedence over non-EF traffic.</p> |
| <b>Options</b>             | <b>bytes</b> —Burst size limit in bytes. The minimum recommended value is the maximum transmission unit (MTU) of the IP packets being policed. You can specify the value either as a complete decimal number or as a decimal number followed by the abbreviation <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |


**Range:** 1500 through 100,000,000,000

**Default:** None


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

- Related Documentation**
- [Two-Color Policer Configuration Overview on page 15](#)
  - [Policer Bandwidth and Burst-Size Limits on page 25](#)
  - [Policer Color-Marking and Actions on page 26](#)
  - [Single Token Bucket Algorithm on page 28](#)
  - [Calculation of Policer Burst-Size Limit on page 33](#)
  - [bandwidth-limit \(Policer\) on page 168](#)
  - [bandwidth-percent on page 170](#)

## color-aware

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | color-aware;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit firewall <b>three-color-policer</b> <i>policer-name</i> <b>single-rate</b> ],<br>[edit firewall <b>three-color-policer</b> <i>policer-name</i> <b>two-rate</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | <p>For a three-color policer, configure the way preclassified packets are metered. In color-aware mode, the local router can assign a higher packet loss priority, but cannot assign a lower packet loss priority.</p> <p>For example, suppose an upstream router assigned medium-high packet loss priority to a packet because the packet exceeded the committed information rate on the upstream router interface.</p> <ul style="list-style-type: none"> <li>• If the local router applies color-aware policing to the packet, the router <i>cannot</i> change the packet loss priority to low, even if the packet conforms to the configured committed information route on the local router interface.</li> <li>• If the local router applies color-blind policing to the packet, the router <i>can</i> change the packet loss priority to low if the packet conforms to the configured committed information route on the local router interface.</li> </ul> <div style="margin-top: 20px;">  <p><b>NOTE:</b> A color-aware policer cannot be applied to Layer 2 traffic.</p> </div> |
| <b>Default</b>                  | If you omit the <b>color-aware</b> statement, the default behavior is color-aware mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Three-Color Policer Configuration Overview on page 19</a></li> <li>• <a href="#">Color Modes for Three-Color Policers on page 109</a></li> <li>• <a href="#">color-blind on page 176</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## color-blind

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | color-blind;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Hierarchy Level</b>          | [edit firewall <b>three-color-policer</b> <i>policer-name</i> <b>single-rate</b> ],<br>[edit firewall <b>three-color-policer</b> <i>policer-name</i> <b>two-rate</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b>              | <p>For a three-color policer, configure the way preclassified packets are metered. In color-blind mode, the local router ignores the preclassification of packets and can assign a higher or lower packet loss priority.</p> <p>For example, suppose an upstream router assigned medium-high packet loss priority to a packet because the packet exceeded the committed information rate on the upstream router interface.</p> <ul style="list-style-type: none"> <li>• If the local router applies color-aware policing to the packet, the router <i>cannot</i> change the packet loss priority to low, even if the packet conforms to the configured committed information rate on the local router interface.</li> </ul> <div style="margin-top: 10px;">  <p><b>NOTE:</b> A color-aware policer cannot be applied to Layer 2 traffic.</p> </div> <ul style="list-style-type: none"> <li>• If the local router applies color-blind policing to the packet, the router <i>can</i> change the packet loss priority to low if the packet conforms to the configured committed information rate on the local router interface.</li> </ul> |
| <b>Default</b>                  | If you omit the <b>color-blind</b> statement, the default behavior is color-aware mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Three-Color Policer Configuration Overview on page 19</a></li> <li>• <a href="#">Color Modes for Three-Color Policers on page 109</a></li> <li>• <a href="#">color-aware on page 175</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |



## committed-burst-size

|                            |                                                                                                                                                                        |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>committed-burst-size bytes;</code>                                                                                                                               |
| <b>Hierarchy Level</b>     | [edit firewall <b>three-color-policer</b> <i>policer-name</i> <b>single-rate</b> ],<br>[edit firewall <b>three-color-policer</b> <i>policer-name</i> <b>two-rate</b> ] |
| <b>Release Information</b> | Statement introduced in Junos OS Release 7.4.                                                                                                                          |
| <b>Description</b>         | For a three-color policer, configure the committed burst size (CBS) as a number of bytes.                                                                              |



**NOTE:** When you include the **committed-burst-size** statement in the configuration, you must also include the **committed-information-rate** statement at the same hierarchy level.

In three-color policing, a committed information rate (CIR) defines the guaranteed bandwidth for traffic arriving at or departing from the interface under normal line conditions. A flow of traffic at an average rate that conforms to the CIR is categorized green.

During periods of average traffic rates below the CIR, any unused bandwidth capacity accumulates up to a maximum amount defined by the CBS. Short periods of bursting traffic (back-to-back traffic at average rates that exceed the CIR) are also categorized as green provided that unused bandwidth capacity is available.

Traffic that exceeds both the CIR and the CBS is considered nonconforming.

Single-rate three-color policers use a *dual token bucket algorithm* to measure traffic against a single rate limit. Nonconforming traffic is categorized as yellow or red, based on the **excess-burst-size** statement included in the policer configuration.

Two-rate three-color policers use a *dual-rate dual token bucket algorithm* to measure traffic against two rate limits. Nonconforming traffic is categorized as yellow or red based on the **peak-information-rate** and **peak-burst-rate** statements included in the policer configuration.

|                                 |                                                                                                                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Options</b>                  | <b>bytes</b> —Number of bytes. You can specify a value in bytes either as a complete decimal number or as a decimal number followed by the abbreviation <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000).<br><b>Range:</b> 1500 through 100,000,000,000 bytes |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Three-Color Policer Configuration Overview on page 19</a></li> <li>• <a href="#">Policer Bandwidth and Burst-Size Limits on page 25</a></li> </ul>                                                                         |

- [Policer Color-Marking and Actions on page 26](#)
- [Dual Token Bucket Algorithms on page 30](#)
- [Calculation of Policer Burst-Size Limit on page 33](#)
- [committed-information-rate on page 179](#)
- [excess-burst-size on page 181](#)
- [peak-burst-size on page 195](#)
- [peak-information-rate on page 197](#)

## committed-information-rate

|                            |                                                                                                                                                                                                                                                            |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>committed-information-rate <i>bps</i>;</code>                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>     | [edit firewall <a href="#">three-color-policer</a> <i>policer-name</i> <a href="#">single-rate</a> ],<br>[edit firewall <a href="#">three-color-policer</a> <i>policer-name</i> <a href="#">two-rate</a> ]                                                 |
| <b>Release Information</b> | Statement introduced in Junos OS Release 7.4.                                                                                                                                                                                                              |
| <b>Description</b>         | For a three-color policer, configure the committed information rate as a number of bits per second. The committed information rate (CIR) is the guaranteed bandwidth for traffic arriving at or departing from the interface under normal line conditions. |



**NOTE:** When you include the `committed-information-rate` statement in the configuration, you must also include the `committed-burst-size` statement at the same hierarchy level.

In three-color policing, a CIR defines the guaranteed bandwidth for traffic arriving at or departing from the interface under normal line conditions. A flow of traffic at an average rate that conforms to the CIR is categorized green.

During periods of average traffic rates below the CIR, any unused bandwidth capacity accumulates up to a maximum amount defined by the committed burst size (CBS). Short periods of bursting traffic (back-to-back traffic at averages rates that exceed the CIR) are also categorized as green provided that unused bandwidth capacity is available.

Traffic that exceeds both the CIR and the CBS is considered nonconforming.


Single-rate three-color policers use a *dual token bucket algorithm* to measure traffic against a single rate limit. Nonconforming traffic is categorized as yellow or red, based on the `excess-burst-size` statement included in the policer configuration.

Two-rate three-color policers use a *dual-rate dual token bucket algorithm* to measure traffic against two rate limits. Nonconforming traffic is categorized as yellow or red based on the `peak-information-rate` and `peak-burst-rate` statements included in the policer configuration.

|                                 |                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Options</b>                  | <code><i>bps</i></code> —Number of bits per second. You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation <code>k</code> (1000), <code>m</code> (1,000,000), or <code>g</code> (1,000,000,000).<br><b>Range:</b> 32,000 through 40,000,000,000 bps |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">Three-Color Policer Configuration Overview on page 19</a></li> <li><a href="#">Policer Bandwidth and Burst-Size Limits on page 25</a></li> </ul>                                                                                                                             |

- [Policer Color-Marking and Actions on page 26](#)
- [Dual Token Bucket Algorithms on page 30](#)
- [Calculation of Policer Burst-Size Limit on page 33](#)
- [committed-burst-size on page 177](#)
- [excess-burst-size on page 181](#)
- [peak-burst-size on page 195](#)
- [peak-information-rate on page 197](#)

## excess-burst-size

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>excess-burst-size bytes;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit firewall <b>three-color-policer</b> <i>policer-name</i> <b>single-rate</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>              | <p>For a single-rate three-color policer, configure the excess burst size (EBS) as a number of bytes. The EBS allows for moderate periods of bursting traffic that exceeds both the committed information rate (CIR) and the committed burst size (CBS).</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> <b>NOTE:</b> When you include the <code>excess-burst-size</code> statement in the configuration, you must also include the <code>committed-burst-size</code> and <code>committed-information-rate</code> statements at the same hierarchy level.</p> </div> <p>Traffic that exceeds both the CIR and the CBS is considered nonconforming.</p> <p>Single-rate three-color policing uses a <i>dual token bucket algorithm</i> to measure traffic against a single rate limit. Nonconforming traffic is categorized as yellow or red based on the <b>excess-burst-size</b> statement included in the policer configuration.</p> <p>During periods of traffic that conforms to the CIR, any unused portion of the guaranteed bandwidth capacity accumulates in the first token bucket, up to the maximum number of bytes defined by the CBS. If any accumulated bandwidth capacity overflows the first bucket, the excess accumulates in a second token bucket, up to the maximum number of bytes defined by the EBS.</p> <p>A nonconforming traffic flow is categorized yellow if its size conforms to bandwidth capacity accumulated in the first token bucket. Packets in a yellow flow are marked with <b>medium-high</b> packet loss priority (PLP) and then passed through the interface.</p> <p>A nonconforming traffic flow is categorized red if its size exceeds the bandwidth capacity accumulated in the second token bucket. Packets in a red traffic flow are marked with <b>high</b> PLP and then either passed through the interface or optionally discarded.</p> |
| <b>Options</b>                  | <p><b>bytes</b>—Number of bytes. You can specify a value in bytes either as a complete decimal number or as a decimal number followed by the abbreviation <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000).</p> <p><b>Range:</b> 1500 through 100,000,000,000 bytes</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <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="#">Three-Color Policer Configuration Overview on page 19</a></li> <li>• <a href="#">Policer Bandwidth and Burst-Size Limits on page 25</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

- [Policer Color-Marking and Actions on page 26](#)
- [Dual Token Bucket Algorithms on page 30](#)
- [Calculation of Policer Burst-Size Limit on page 33](#)
- [committed-burst-size on page 177](#)
- [committed-information-rate on page 179](#)

---

## filter-specific

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | filter-specific;                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Hierarchy Level</b>          | [edit firewall family inet <a href="#">prefix-action name</a> ],<br>[edit firewall <a href="#">policer policer-name</a> ],<br>[edit logical-systems <i>logical-system-name</i> firewall <a href="#">policer policer-name</a> ],<br>[edit logical-systems <i>logical-system-name</i> firewall family inet <a href="#">prefix-action name</a> ]                                                                                                 |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Logical systems support introduced in Junos OS Release 9.3.                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | Set the prefix-specific action or policer to operate in <i>filter-specific</i> mode, meaning that a single policer and counter are shared by all filter terms that reference the prefix-specific action or policer. By default, the prefix-specific action or policer operates in <i>term-specific</i> mode, meaning that a separate policer and counter are used for each filter term that references the prefix-specific action or policer. |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Filter-Specific Policer Overview on page 64</a></li><li>• <a href="#">Prefix-Specific Counting and Policing Overview on page 71</a></li><li>• <a href="#">Filter-Specific Counter and Policer Set Overview on page 74</a></li></ul>                                                                                                                                                       |

## forwarding-class (Firewall Filter Action)

---

|                                 |                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>forwarding-class <i>class-name</i>;</code>                                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit firewall family <i>family-name</i> filter <i>filter-name</i> term <i>term-name</i> then],<br>[edit logical-systems <i>logical-system-name</i> firewall family <i>family-name</i> filter <i>filter-name</i> term <i>term-name</i> then]                                                                                       |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                  |
| <b>Description</b>              | Set the forwarding class of incoming packets.                                                                                                                                                                                                                                                                                      |
| <b>Options</b>                  | <i>class-name</i> —Name of the forwarding class.                                                                                                                                                                                                                                                                                   |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• “Standard Firewall Filter Nonterminating Actions” in the <a href="#">Junos OS Firewall Filter and Policer Configuration Guide</a></li><li>• <a href="#">Policer Color-Marking and Actions on page 26</a></li><li>• <a href="#">Multifield Classification Overview on page 87</a></li></ul> |

## hierarchical-policer

```
Syntax hierarchical-policer policer-name {
    aggregate {
        if-exceeding {
            bandwidth-limit bps;
            burst-size-limit bytes;
        }
        then {
            discard;
        }
    }
    premium {
        if-exceeding {
            bandwidth-limit bps;
            burst-size-limit bytes;
        }
        then {
            discard;
        }
    }
}
```

**Hierarchy Level** [edit firewall]

**Release Information** Statement introduced in Junos OS Release 9.5.

**Description** On M40e, M120, and M320 edge routers with Flexible PIC Concentrator (FPC) input as FFPC and FPC output as SFPC, and on MX Series, T320, T640, and T1600 edge routers with Enhanced Intelligent Queuing (IQE) PICs, specify a hierarchical policer.

**Options** *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 (" ").

The remaining statements are explained separately.

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

**Related Documentation**

- [Hierarchical Policer Configuration Overview on page 22](#)
- [Hierarchical Policers on page 147](#)
- [aggregate \(Hierarchical Policer\) on page 166](#)
- [bandwidth-limit \(Hierarchical Policer\) on page 167](#)
- [burst-size-limit \(Hierarchical Policer\) on page 172](#)
- [if-exceeding \(Hierarchical Policer\) on page 185](#)
- [premium \(Hierarchical Policer\) on page 205](#)



## if-exceeding (Hierarchical Policer)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | if-exceeding {<br><a href="#">bandwidth-limit</a> <i>bps</i> ;<br><a href="#">burst-size-limit</a> <i>bytes</i> ;<br>}                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit firewall <a href="#">hierarchical-policer aggregate</a> ],<br>[edit firewall <a href="#">hierarchical-policer premium</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>              | For M40e, M120, and M320 (with FFPC and SFPC) edge routers and T320, T640, and T1600 core routers with Enhanced Intelligent Queuing (IQE) PICs, specify bandwidth and burst limits for a premium or aggregate component of a hierarchical policer.                                                                                                                                                                                                                                                                                                             |
| <b>Options</b>                  | The remaining statements are explained separately.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Hierarchical Policer Configuration Overview on page 22</a></li> <li>• <a href="#">Hierarchical Policers on page 147</a></li> <li>• <a href="#">aggregate (Hierarchical Policer) on page 166</a></li> <li>• <a href="#">bandwidth-limit (Hierarchical Policer) on page 167</a></li> <li>• <a href="#">burst-size-limit (Hierarchical Policer) on page 172</a></li> <li>• <a href="#">hierarchical-policer on page 184</a></li> <li>• <a href="#">premium (Hierarchical Policer) on page 205</a></li> </ul> |

## if-exceeding (Policer)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>if-exceeding {<br/>    (bandwidth-limit <i>bps</i>   bandwidth-percent <i>number</i>);<br/>    burst-size-limit <i>bytes</i>;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | [edit firewall <b>policer</b> <i>policer-name</i> ],<br>[edit logical-systems <i>logical-system-name</i> firewall <b>policer</b> <i>policer-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Logical systems support introduced in Junos OS Release 9.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | Configure rate limits for a single-rate two-color policer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Options</b>                  | The remaining statements are explained separately.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Two-Color Policer Configuration Overview on page 15</a></li><li>• <a href="#">Hierarchical Policer Configuration Overview on page 22</a></li><li>• <a href="#">Basic Single-Rate Two-Color Policers on page 39</a></li><li>• <a href="#">Bandwidth Policers on page 55</a></li><li>• <a href="#">Filter-Specific Counters and Policers on page 64</a></li><li>• <a href="#">Prefix-Specific Counting and Policing Actions on page 71</a></li><li>• <a href="#">Multifield Classification on page 87</a></li><li>• <a href="#">Policer Overhead to Account for Rate Shaping in the Traffic Manager on page 99</a></li><li>• <a href="#">Hierarchical Policers on page 147</a></li></ul> |

## input-hierarchical-policer

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>input-hierarchical-policer <i>policer-name</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> <a href="#">layer2-policer</a> ],<br>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> <a href="#">layer2-policer</a> ],<br>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <a href="#">layer2-policer</a> ]<br>[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 9.5.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | Apply a hierarchical policer to the Layer 2 input traffic for all protocol families at the physical or logical interface.                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <i>policer-name</i> —Name of the hierarchical policer.                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Hierarchical Policers on page 147</a></li> <li>• <a href="#">layer2-policer on page 189</a></li> </ul>                                                                                                                                                                                                                                                                                                      |

## input-policer

|                                 |                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>input-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> ],<br>[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.                                                                                                                                                                                                                                                                                                                       |
| <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>                  | <i>policer-name</i> —Name of the single-rate two-color policer.                                                                                                                                                                                                                                                                                                     |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Two-Color and Three-Color Policers at Layer 2 on page 154</a></li> <li>• <a href="#">input-three-color on page 188</a></li> <li>• <a href="#">layer2-policer on page 189</a></li> <li>• <a href="#">logical-interface-policer on page 190</a></li> <li>• <a href="#">output-policer on page 193</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> ],<br>[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.                                                                                                                                                                                                                                                                                                                 |
| <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-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 or two-rate three-color policer.                                                                                                                                                                                                                                                                          |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Two-Color and Three-Color Policers at Layer 2 on page 154</a></li><li>• <a href="#">input-policer on page 187</a></li><li>• <a href="#">layer2-policer on page 189</a></li><li>• <a href="#">logical-interface-policer on page 190</a></li><li>• <a href="#">output-three-color on page 194</a></li></ul> |

## layer2-policer

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | layer2-policer { ... }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> ],<br>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ],<br>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> ]<br>[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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b>              | <p>Apply a traffic policer to Layer 2 traffic at a supported interface.</p> <p>Apply a two-color or three-color logical interface policer to the Layer 2 input or output traffic at the logical interface. The following interfaces are supported:</p> <ul style="list-style-type: none"> <li>• 1-Gigabit Ethernet interfaces on M Series, MX Series, and T Series routers</li> <li>• 10-Gigabit Ethernet IQ2 and IQ2E interfaces on M Series, MX Series, and T Series routers</li> </ul> <p>Apply a hierarchical policer to the Layer 2 input traffic for all protocol families at the physical or logical interface. The following interfaces are supported:</p> <ul style="list-style-type: none"> <li>• SONET interfaces hosted on M40e, M120, and M320 edge routers with incoming Flexible PIC Concentrators (FPCs) as SFPC and outgoing FPCs as FFPC</li> <li>• Interfaces on MX Series, T320, T640, and T1600 core routers with Enhanced Intelligent Queuing (IQE) PICs</li> </ul> |
| <b>Options</b>                  | The statements are explained separately.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Hierarchical Policers on page 147</a></li> <li>• <a href="#">input-hierarchical-policer on page 187</a></li> <li>• <a href="#">Two-Color and Three-Color Policers at Layer 2 on page 154</a></li> <li>• <a href="#">input-policer on page 187</a></li> <li>• <a href="#">input-three-color on page 188</a></li> <li>• <a href="#">output-policer on page 193</a></li> <li>• <a href="#">output-three-color on page 194</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## logical-bandwidth-policer

---

|                                 |                                                                                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | logical-bandwidth-policer;                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit firewall <a href="#">policer</a> <i>policer-name</i> ],<br>[edit logical-systems <i>logical-system-name</i> firewall <a href="#">policer</a> <i>policer-name</i> ]                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.2.<br>Logical systems support introduced in Junos OS Release 9.3.                                                                                                                                                                 |
| <b>Description</b>              | For a policer with a bandwidth limit configured as a percentage (using the <a href="#">bandwidth-percent</a> statement), specify that the percentage be based on the shaping rate defined on the logical interface, rather than on the media rate of the physical interface. |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Bandwidth Policers on page 55</a></li><li>• <a href="#">bandwidth-percent on page 170</a></li><li>• interface-specific statement in the <i>Junos OS Firewall Filter and Policer Configuration Guide</i></li></ul>        |

## logical-interface-policer

---

|                                 |                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | logical-interface-policer;                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit firewall <a href="#">policer</a> <i>policer-name</i> ],<br>[edit firewall <a href="#">three-color-policer</a> <i>name</i> ],<br>[edit logical-systems <i>logical-system-name</i> firewall <a href="#">policer</a> <i>policer-name</i> ],<br>[edit logical-systems <i>logical-system-name</i> firewall <a href="#">three-color-policer</a> <i>name</i> ] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Support at the [edit firewall <a href="#">three-color-policer</a> <i>name</i> ] hierarchy level introduced in Junos OS Release 8.2.<br>Logical systems support introduced in Junos OS Release 9.3.                                                                                                       |
| <b>Description</b>              | Configure a logical interface (aggregate) policer.                                                                                                                                                                                                                                                                                                            |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Two-Color and Three-Color Logical Interface Policers on page 125</a></li></ul>                                                                                                                                                                                                                            |

## loss-priority (Firewall Filter Action)

|                                 |                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <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> then],<br>[edit logical-systems <i>logical-system-name</i> firewall family <i>family-name</i> filter <i>filter-name</i> term <i>term-name</i> then]                                                                                           |
| <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.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• “Standard Firewall Filter Nonterminating Actions” in the <a href="#">Junos OS Firewall Filter and Policer Configuration Guide</a></li> <li>• <a href="#">Policer Color-Marking and Actions on page 26</a></li> <li>• <a href="#">Multifield Classification Overview on page 87</a></li> </ul> |

## loss-priority high then discard (Three-Color Policer)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | loss-priority high then discard;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | [edit firewall <a href="#">three-color-policer policer-name action</a> ],<br>[edit logical-systems <i>logical-system-name</i> firewall <a href="#">three-color-policer policer-name action</a> ]                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 8.2.<br>Logical systems support introduced in Junos OS Release 9.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | <p>For packets with high loss priority, discard the packets. The loss priority setting is implicit and is not configurable. Include this statement if you do not want the local router to forward packets that have high packet loss priority.</p> <p>For single-rate three-color policers, the Junos OS assigns high loss priority to packets that exceed the committed information rate and the excess burst size.</p> <p>For two-rate three-color policers, the Junos OS assigns high loss priority to packets that exceed the peak information rate and the peak burst size.</p>                   |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Three-Color Policer Configuration Overview on page 19</a></li><li>• <a href="#">Basic Single-Rate Three-Color Policers on page 111</a></li><li>• <a href="#">Basic Two-Rate Three-Color Policers on page 117</a></li><li>• <a href="#">Two-Color and Three-Color Logical Interface Policers on page 125</a></li><li>• <a href="#">Two-Color and Three-Color Physical Interface Policers on page 137</a></li><li>• <a href="#">Two-Color and Three-Color Policers at Layer 2 on page 154</a></li><li>• <a href="#">action on page 165</a></li></ul> |



## 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> ],<br>[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.                                                                                                                                                                                                                                                                                                                       |
| <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>                  | <i>policer-name</i> —Name of the single-rate two-color policer.                                                                                                                                                                                                                                                                                                     |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Two-Color and Three-Color Policers at Layer 2 on page 154</a></li> <li>• <a href="#">input-policer on page 187</a></li> <li>• <a href="#">layer2-policer on page 189</a></li> <li>• <a href="#">logical-interface-policer on page 190</a></li> <li>• <a href="#">output-three-color on page 194</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> ],<br>[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.                                                                                                                                                                                                                                                                                                                 |
| <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-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 or two-rate three-color policer.                                                                                                                                                                                                                                                                          |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Two-Color and Three-Color Policers at Layer 2 on page 154</a></li><li>• <a href="#">input-three-color on page 188</a></li><li>• <a href="#">layer2-policer on page 189</a></li><li>• <a href="#">logical-interface-policer on page 190</a></li><li>• <a href="#">output-policer on page 193</a></li></ul> |

## peak-burst-size

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>peak-burst-size bytes;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit firewall <b>three-color-policer</b> <i>policer-name</i> <b>two-rate</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | For a two-rate three-color policer, configure the peak burst size (PBS) as a number of bytes. The PBS defines the maximum number of bytes of unused peak bandwidth capacity that can be accumulated. The accumulated bandwidth allows for moderate periods of bursting traffic that exceeds the peak information rate (PIR) and the committed burst size (CBS).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                                 | <div>  <p><b>NOTE:</b> When you include the <b>peak-burst-size</b> statement in the configuration, you must also include the <b>committed-burst-size</b> and <b>peak-information-rate</b> statements at the same hierarchy level.</p> </div> <p>Two-rate three-color policers use a <i>dual-rate dual token bucket algorithm</i> to measure traffic against two rate limits.</p> <ul style="list-style-type: none"> <li>A traffic flow is categorized green if it conforms to both the committed information rate (CIR) and the CBS-bounded accumulation of available committed bandwidth capacity.</li> <li>A traffic flow is categorized yellow if exceeds the CIR and CBS but conforms to the PIR. Packets in a yellow flow are marked with <b>medium-high</b> packet loss priority (PLP) and then passed through the interface.</li> <li>A traffic flow is categorized red if exceeds the PIR and the PBS-bounded accumulation of available peak bandwidth capacity. Packets in a red traffic flow are marked with <b>high</b> PLP and then either passed through the interface or optionally discarded.</li> </ul> |
| <b>Options</b>                  | <p><b>bytes</b>—Number of bytes. You can specify a value in bytes either as a complete decimal number or as a decimal number followed by the abbreviation <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000).</p> <p><b>Range:</b> 1500 through 100,000,000,000 bytes</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <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="#">Three-Color Policer Configuration Overview on page 19</a></li> <li><a href="#">Policer Bandwidth and Burst-Size Limits on page 25</a></li> <li><a href="#">Policer Color-Marking and Actions on page 26</a></li> <li><a href="#">Dual Token Bucket Algorithms on page 30</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

- [Calculation of Policer Burst-Size Limit on page 33](#)
- [committed-burst-size on page 177](#)
- [committed-information-rate on page 179](#)
- [excess-burst-size on page 181](#)
- [peak-information-rate on page 197](#)

## peak-information-rate

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>peak-information-rate <i>bps</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit firewall <b>three-color-policer</b> <i>policer-name</i> <b>two-rate</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | For a two-rate three-color policer, configure the peak information rate (PIR) as a number of bits per second. The PIR is the maximum rate for traffic arriving at or departing from the interface under peak line conditions. Traffic that exceeds the committed information rate (CIR) and the committed burst size (CBS) is metered to the PIR.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                                 | <div>  <p><b>NOTE:</b> When you include the <b>peak-information-rate</b> statement in the configuration, you must also include the <b>committed-information-rate</b> and <b>peak-burst-size</b> statements at the same hierarchy level.</p> </div> <p>Two-rate three-color policers use a <i>dual-rate dual token bucket algorithm</i> to measure traffic against two rate limits.</p> <ul style="list-style-type: none"> <li>• A traffic flow is categorized green if it conforms to both the CIR and the CBS-bounded accumulation of available committed bandwidth capacity.</li> <li>• A traffic flow is categorized yellow if exceeds the CIR and CBS but conforms to the PIR. Packets in a yellow flow are marked with <b>medium-high</b> packet loss priority (PLP) and then passed through the interface.</li> <li>• A traffic flow is categorized red if exceeds the PIR and the PBS-bounded accumulation of available peak bandwidth capacity. Packets in a red traffic flow are marked with <b>high</b> PLP and then either passed through the interface or optionally discarded.</li> </ul> |
| <b>Options</b>                  | <p><b>bps</b>—Number of bits per second. You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000).</p> <p><b>Range:</b> 32,000 through 40,000,000,000 bps</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <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="#">Three-Color Policer Configuration Overview on page 19</a></li> <li>• <a href="#">Policer Bandwidth and Burst-Size Limits on page 25</a></li> <li>• <a href="#">Policer Color-Marking and Actions on page 26</a></li> <li>• <a href="#">Dual Token Bucket Algorithms on page 30</a></li> <li>• <a href="#">Calculation of Policer Burst-Size Limit on page 33</a></li> <li>• <a href="#">committed-burst-size on page 177</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

- [committed-information-rate on page 179](#)
- [excess-burst-size on page 181](#)
- [peak-burst-size on page 195](#)

---

## physical-interface-filter


---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | physical-interface-filter;                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit firewall family <i>family-name</i> filter <i>filter-name</i> ],<br>[edit logical-systems <i>logical-system-name</i> firewall family <i>family-name</i> filter <i>filter-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> firewall family <i>family-name</i> filter <i>filter-name</i> ],<br>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> firewall family <i>family-name</i> filter <i>filter-name</i> ] |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.6.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | Configure a physical interface filter. Use this statement to reference a physical interface policer for the specified protocol family.                                                                                                                                                                                                                                                                                                                                              |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Two-Color and Three-Color Physical Interface Policers on page 137</a></li><li>• <a href="#">physical-interface-policer on page 199</a></li><li>• <a href="#">policer (Configuring) on page 201</a></li></ul>                                                                                                                                                                                                                    |

## physical-interface-policer

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | physical-interface-policer;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | <p>[edit firewall <a href="#">policer</a> <i>policer-name</i>],</p> <p>[edit firewall <a href="#">three-color-policer</a> <i>policer-name</i>],</p> <p>[edit logical-system <i>logical-system-name</i> firewall <a href="#">policer</a> <i>policer-name</i>],</p> <p>[edit logical-system <i>logical-system-name</i> <a href="#">three-color-policer</a> <i>policer-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> firewall <a href="#">policer</a> <i>policer-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> firewall <a href="#">three-color-policer</a> <i>policer-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> firewall <a href="#">policer</a> <i>policer-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> firewall <a href="#">three-color-policer</a> <i>policer-name</i>]</p> |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b>              | Configure an aggregate policer for a physical interface. A physical interface policer applies to all the logical interfaces and protocol families configured on a physical interface. As a result, a single physical interface policer can be applied to multiple routing instances because this policer includes all the logical interfaces configured on the physical interface even if they belong to different routing instances.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <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="#">Two-Color and Three-Color Physical Interface Policers on page 137</a></li> <li>• <a href="#">physical-interface-filter on page 198</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## policer (Applying to a Logical Interface)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> policer {     input <i>policer-name</i>;     output <i>policer-name</i>; } </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | <pre> [edit interfaces <i>interface-name</i> unit <i>unit-number</i>], [edit interfaces <i>interface-name</i> unit <i>unit-number</i> family <i>family</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>unit-number</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>unit-number</i>   family <i>family</i>] </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | <p>Apply a single-rate two-color policer—except for a physical interface policer—to Layer 3 input or output traffic at a logical interface.</p> <ul style="list-style-type: none"> <li>To rate-limit all traffic types, regardless of the protocol family, you can apply a logical interface policer at the logical unit level of a supported interface.</li> <li>To rate-limit traffic of a specific protocol family, you can apply a basic two-color policer, a bandwidth policer, or a logical interface policer at the protocol family level of a supported interface.</li> </ul> <div style="margin-top: 10px;">  <p><b>NOTE:</b> You cannot apply a physical interface policer as part of the interface configuration. You can apply a physical interface policer by referencing the policer from a physical interface filter term.</p> </div> |
| <b>Options</b>                  | <p><b>input <i>policer-name</i></b>—Name of one policer to evaluate packets received on the interface.</p> <p><b>output <i>policer-name</i></b>—Name of one policer to evaluate packets transmitted on the interface.</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>• <a href="#">Single-Rate Two-Color Policer Overview on page 39</a></li> <li>• <a href="#">Bandwidth Policer Overview on page 56</a></li> <li>• <a href="#">Logical Interface (Aggregate) Policer Overview on page 125</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |



## policer (Configuring)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <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-interface-policer;     physical-interface-policer;     then {         <i>policer-action</i>;     } } </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit firewall],<br>[edit logical-systems <i>logical-system-name</i> firewall]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Logical systems support introduced in Junos OS Release 9.3.<br><b>physical-interface-policer</b> statement introduced in Junos OS Release 9.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | Configure policer rate limits and actions. When included at the <b>[edit 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.                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Options</b>                  | <p><b><i>policer-action</i></b>—One or more actions to take:</p> <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> </ul> <p><b><i>policer-name</i></b>—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 (" ").</p> <p><b>then</b>—Actions to take on matching packets.</p> <p>The remaining statements are explained separately.</p> |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Statement Hierarchy for Configuring Policers on page 13</a></li> <li>• <a href="#">Single-Rate Two-Color Policer Overview on page 39</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

- [Bandwidth Policer Overview on page 56](#)
- [Physical Interface Policer Overview on page 137](#)
- [Logical Interface \(Aggregate\) Policer Overview on page 125](#)

## **policer (Firewall Filter Action)**

---

|                                 |                                                                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>policer <i>policer-name</i>;</code>                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit firewall family <i>family-name</i> filter <i>filter-name</i> term <i>term-name</i> then],<br>[edit logical-systems <i>logical-system-name</i> firewall family <i>family-name</i> filter <i>filter-name</i> term <i>term-name</i> then]                      |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Logical systems support introduced in Junos OS Release 9.3.                                                                                                                                                  |
| <b>Description</b>              | For T Series routers and M320 routers with Enhanced II Flexible PIC Concentrators (FPCs) and the T640 Core Router with Enhanced Scaling FPC4, apply a tricolor marking policer.                                                                                   |
| <b>Options</b>                  | <i>policer-name</i> —Name of a single-rate two-color policer to use to rate-limit traffic.                                                                                                                                                                        |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• “Standard Firewall Filter Nonterminating Actions” in the <a href="#">Junos OS Firewall Filter and Policer Configuration Guide</a></li><li>• <a href="#">Two-Color Policer Configuration Overview on page 15</a></li></ul> |

## prefix-action (Configuring)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>prefix-action <i>prefix-action-name</i> {     count;     destination-prefix-length <i>prefix-length</i>;     filter-specific;     policer <i>policer-name</i>;     source-prefix-length <i>prefix-length</i>;     subnet-prefix-length <i>prefix-length</i>; }</pre>                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | <pre>[edit firewall family inet], [edit logical-systems <i>logical-system-name</i> firewall family inet]</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Logical systems support introduced in Junos OS Release 9.3.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | Configure a prefix-specific action.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Options</b>                  | <p><b>count</b>—Enable counter.</p> <p><b>destination-prefix-length <i>prefix-length</i></b>—Destination prefix length.<br/> <b>Range:</b> 0 through 32</p> <p><b>filter-specific</b>—Create the prefix-specific set of policers and counters as a filter-specific set. If this option is not specified, the prefix-specific set of policers and counters are created as term-specific.</p> <p><b>policer <i>policer-name</i></b>—Policer name.</p> <p><b>source-prefix-length <i>prefix-length</i></b>—Source prefix length.<br/> <b>Range:</b> 0 through 32</p> <p><b>subnet-prefix-length <i>prefix-length</i></b>—Subnet prefix length.<br/> <b>Range:</b> 0 through 32</p> |
| <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="#">Prefix-Specific Counting and Policing Actions on page 71</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## prefix-action (Firewall Filter Action)

---

|                              |                                                                                                                                                                                                                                                                        |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                | <code>prefix-action <i>prefix-action-name</i>;</code>                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>       | [edit firewall family inet filter <i>filter-name</i> term <i>term-name</i> then],<br>[edit logical-systems <i>logical-system-name</i> firewall family inet filter <i>filter-name</i> term <i>term-name</i> then]                                                       |
| <b>Release Information</b>   | Statement introduced before Junos OS Release 7.4.<br>Logical systems support introduced in Junos OS Release 9.3.                                                                                                                                                       |
| <b>Description</b>           | Reference a prefix-specific action.                                                                                                                                                                                                                                    |
| <b>Options</b>               | <i>prefix-action-name</i> —Name of a prefix-specific action to use to rate-limit traffic.                                                                                                                                                                              |
| <b>Related Documentation</b> | <ul style="list-style-type: none"><li>• “Standard Firewall Filter Nonterminating Actions” in the <a href="#">Junos OS Firewall Filter and Policer Configuration Guide</a></li><li>• <a href="#">Prefix-Specific Counting and Policing Actions on page 71</a></li></ul> |

## premium (Hierarchical Policer)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> premium {   if-exceeding {     bandwidth-limit <i>bandwidth</i>;     burst-size-limit <i>burst</i>;   }   then {     discard;   } } </pre>                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit firewall <a href="#">hierarchical-policer</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | On M40e, M120, and M320 edge routers with FPC input as FFPC and FPC output as SFPC, and on MX Series, T320, T640, and T1600 edge routers with Enhanced Intelligent Queuing (IQE) PICs, specify a premium level for a hierarchical policer.                                                                                                                                                                                                                                                                                                                          |
| <b>Options</b>                  | The remaining statements are explained separately.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Hierarchical Policer Configuration Overview on page 22</a></li> <li>• <a href="#">Hierarchical Policers on page 147</a></li> <li>• <a href="#">aggregate (Hierarchical Policer) on page 166</a></li> <li>• <a href="#">bandwidth-limit (Hierarchical Policer) on page 167</a></li> <li>• <a href="#">burst-size-limit (Hierarchical Policer) on page 172</a></li> <li>• <a href="#">hierarchical-policer on page 184</a></li> <li>• <a href="#">if-exceeding (Hierarchical Policer) on page 185</a></li> </ul> |

## single-rate

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>single-rate {<br/>  (color-aware   color-blind);<br/>  committed-information-rate <i>bps</i>;<br/>  committed-burst-size <i>bytes</i>;<br/>  excess-burst-size <i>bytes</i>;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | [edit firewall <a href="#">three-color-policer</a> <i>policer-name</i> ],<br>[edit logical-systems <i>logical-system-name</i> firewall <a href="#">three-color-policer</a> <i>policer-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Logical systems support introduced in Junos OS Release 9.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b>              | <p>Configure a single-rate three-color policer in which marking is based on the committed information rate (CIR), committed burst size (CBS), and excess burst size (EBS).</p> <p>Packets that conform to the CIR or the CBS are assigned low loss priority (green). Packets that exceed the CIR and the CBS but are within the EBS are assigned medium-high loss priority (yellow). Packets that exceed the EBS are assigned high loss priority (red).</p> <p>Green and yellow packets are always forwarded; this action is not configurable. You can configure red packets to be discarded. By default, red packets are forwarded.</p> |
| <b>Options</b>                  | The remaining statements are explained separately.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Three-Color Policer Configuration Overview on page 19</a></li><li>• <a href="#">color-aware on page 175</a></li><li>• <a href="#">color-blind on page 176</a></li><li>• <a href="#">two-rate on page 209</a></li></ul>                                                                                                                                                                                                                                                                                                                                                               |

## three-color-policer (Configuring)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> three-color-policer <i>policer-name</i> {     action {         loss-priority high then discard;     }     logical-interface-policer;     physical-interface-policer;     single-rate {         (color-aware   color-blind);         committed-information-rate <i>bps</i>;         committed-burst-size <i>bytes</i>;         excess-burst-size <i>bytes</i>;     }     two-rate {         (color-aware   color-blind);         committed-information-rate <i>bps</i>;         committed-burst-size <i>bytes</i>;         peak-information-rate <i>bps</i>;         peak-burst-size <i>bytes</i>;     } } </pre>                                 |
| <b>Hierarchy Level</b>          | [edit firewall],<br>[edit logical-systems <i>logical-system-name</i> firewall]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br><b>action</b> statement introduced in Junos OS Release 8.2.<br>Logical systems support introduced in Junos OS Release 9.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | Configure a three-color policer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Options</b>                  | <p><b><i>policer-name</i></b>—Name of the three-color policer. Reference this name when you apply the policer to an interface.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Statement Hierarchy for Configuring Policers on page 13</a></li> <li>• <a href="#">Three-Color Policer Configuration Guidelines on page 109</a></li> <li>• <a href="#">Basic Single-Rate Three-Color Policers on page 111</a></li> <li>• <a href="#">Basic Two-Rate Three-Color Policers on page 117</a></li> <li>• <a href="#">Two-Color and Three-Color Logical Interface Policers on page 125</a></li> <li>• <a href="#">Two-Color and Three-Color Physical Interface Policers on page 137</a></li> <li>• <a href="#">Two-Color and Three-Color Policers at Layer 2 on page 154</a></li> </ul> |

## three-color-policer (Firewall Filter Action)

---

|                                 |                                                                                                                                                                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>three-color-policer {<br/>    (single-rate   two-rate) <i>policer-name</i>;<br/>}</pre>                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit firewall family <i>family-name</i> filter <i>filter-name</i> term <i>term-name</i> then],<br>[edit logical-systems <i>logical-system-name</i> firewall family <i>family-name</i> filter <i>filter-name</i> term <i>term-name</i> then]                        |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br><b>single-rate</b> statement added in Junos OS Release 8.2.<br>Logical systems support introduced in Junos OS Release 9.3.                                                                                     |
| <b>Description</b>              | For T Series routers and M320 routers with Enhanced II Flexible PIC Concentrators (FPCs) and the T640 Core 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.<br><br><b>two-rate</b> —Named tricolor policer is a two-rate policer.<br><br><b><i>policer-name</i></b> —Name of three-color policer to use to rate-limit traffic.                             |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• “Standard Firewall Filter Nonterminating Actions” in the <a href="#">Junos OS Firewall Filter and Policer Configuration Guide</a></li><li>• <a href="#">Three-Color Policer Configuration Overview</a> on page 19</li></ul> |



## two-rate

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>two-rate {   (color-aware   color-blind);   committed-information-rate <i>bps</i>;   committed-burst-size <i>bytes</i>;   peak-information-rate <i>bps</i>;   peak-burst-size <i>bytes</i>; }</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | <pre>[edit firewall <b>three-color-policer</b> <i>policer-name</i>], [edit logical-systems <i>logical-system-name</i> firewall <b>three-color-policer</b> <i>policer-name</i>]</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Logical systems support introduced in Junos OS Release 9.3.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | <p>Configure a two-rate three-color policer in which marking is based on the committed information rate (CIR), committed burst size (CBS), peak information rate (PIR), and peak burst size (PBS).</p> <p>Packets that conform to the CIR or the CBS are assigned low loss priority (green). Packets that exceed the CIR and the CBS but are within the PIR or the PBS are assigned medium-high loss priority (yellow). Packets that exceed the PIR and the PBS are assigned high loss priority (red).</p> <p>Green and yellow packets are always forwarded; this action is not configurable. You can configure red packets to be discarded. By default, red packets are forwarded.</p> <p>The remaining statements are explained separately.</p> |
| <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="#">Three-Color Policer Configuration Overview on page 19</a></li> <li>• <a href="#">color-aware on page 175</a></li> <li>• <a href="#">color-blind on page 176</a></li> <li>• <a href="#">single-rate on page 206</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                |



## PART 3

# Administration

- [Traffic Policing Standards on page 213](#)
- [Traffic Policing Reference on page 215](#)
- [Firewall Filter and Policer Operational Mode Commands on page 219](#)



## CHAPTER 10

# Traffic Policing Standards

- [Supported Standards for Policing on page 213](#)

### Supported Standards for Policing

---

Three-color policers are part of an assured forwarding (AF) per-hop-behavior (PHB) classification system for a Differentiated Services (DiffServ) environment, which is described and defined in the following RFCs:

- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC 2475, *An Architecture for Differentiated Service*
- RFC 2597, *Assured Forwarding PHB Group*
- RFC 2598, *An Expedited Forwarding PHB*
- RFC 2698, *A Two Rate Three Color Marker*

In a DiffServ environment, the most significant 6 bits of the type-of-service (ToS) octet in the IP header contain a value called the *Differentiated Services code point* (DSCP). Within the DSCP field, the most significant 3 bits are interpreted as the *IP precedence* field, which can be used to select different per-hop forwarding treatments for the packet.

#### Related Documentation

- [Traffic Policing Overview on page 3](#)
- [Traffic Policer Types on page 7](#)
- [Order of Policer and Firewall Filter Operations on page 10](#)
- [Two-Color Policer Configuration Overview on page 15](#)
- [Three-Color Policer Configuration Overview on page 19](#)
- [Hierarchical Policer Configuration Overview on page 22](#)



## CHAPTER 11

# Traffic Policing Reference

- Using the CLI Editor in Configuration Mode on page 215

## Using the CLI Editor in Configuration Mode

This topic describes some of the basic commands that you must use to enter configuration mode in the command-line interface (CLI) editor, navigate through the configuration hierarchy, get help, and commit or revert the changes that you make during the configuration session. For more information about the commands described here, see the *Junos OS CLI User Guide*.

| Task                                                                                                                                                                                                                                                                                          | Command/Statement                        | Example                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>Edit Your Configuration</b>                                                                                                                                                                                                                                                                |                                          |                                                                                                                                      |
| Enter configuration mode.<br><br>When you first log in to the device, the device is in operational mode. You must explicitly enter configuration mode. When you do, the CLI prompt changes from <b>user@host&gt;</b> to <b>user@host#</b> and the hierarchy level appears in square brackets. | <b>configure</b>                         | <b>user@host&gt; configure</b><br><br>[edit]<br>user@host#                                                                           |
| Create a statement hierarchy.<br><br>You can use the <b>edit</b> command to simultaneously create a hierarchy and move to that new level in the hierarchy. You cannot use the <b>edit</b> command to change the value of identifiers.                                                         | <b>edit <i>hierarchy-level value</i></b> | [edit]<br>user@host# <b>edit security zones security-zone myzone</b><br><br>[edit security zones security-zone myzone]<br>user@host# |
| Create a statement hierarchy and set identifier values.<br><br>The <b>set</b> command is similar to <b>edit</b> except that your current level in the hierarchy does not change.                                                                                                              | <b>set <i>hierarchy-level value</i></b>  | [edit]<br>user@host# <b>set security zones security-zone myzone</b><br><br>[edit]<br>user@host#                                      |

## Navigate the Hierarchy

| Task                                                                                                                                                                                                                                                                                                                                                                                                               | Command/Statement                        | Example                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Navigate down to an existing hierarchy level.                                                                                                                                                                                                                                                                                                                                                                      | <code>edit <i>hierarchy-level</i></code> | [edit]<br>user@host# <code>edit security zones</code><br><br>[edit security zones]<br>user@host#                                                       |
| Navigate up one level in the hierarchy.                                                                                                                                                                                                                                                                                                                                                                            | <code>up</code>                          | [edit security zones]<br>user@host# <code>up</code><br><br>[edit security]<br>user@host#                                                               |
| Navigate to the top of the hierarchy.                                                                                                                                                                                                                                                                                                                                                                              | <code>top</code>                         | [edit security zones]<br>user@host# <code>top</code><br><br>[edit]<br>user@host#                                                                       |
| <b>Commit or Revert Changes</b>                                                                                                                                                                                                                                                                                                                                                                                    |                                          |                                                                                                                                                        |
| Commit your configuration.                                                                                                                                                                                                                                                                                                                                                                                         | <code>commit</code>                      | [edit]<br>user@host# <code>commit</code><br><br>commit complete                                                                                        |
| Roll back changes from the current session.<br><br>Use the <b>rollback</b> command to revert all changes from the current configuration session. When you run the <b>rollback</b> command before exiting your session or committing changes, the software loads the most recently committed configuration onto the device. You must enter the <b>rollback</b> statement at the <b>edit</b> level in the hierarchy. | <code>rollback</code>                    | [edit]<br>user@host# <code>rollback</code><br><br>load complete                                                                                        |
| <b>Exit Configuration Mode</b>                                                                                                                                                                                                                                                                                                                                                                                     |                                          |                                                                                                                                                        |
| Commit the configuration and exit configuration mode.                                                                                                                                                                                                                                                                                                                                                              | <code>commit and-quit</code>             | [edit]<br>user@host# <code>commit and-quit</code><br><br>user@host>                                                                                    |
| Exit configuration mode without committing your configuration.<br><br>You must navigate to the top of the hierarchy using the <b>up</b> or <b>top</b> commands before you can exit configuration mode.                                                                                                                                                                                                             | <code>exit</code>                        | [edit]<br>user@host# <code>exit</code><br><br>The configuration has been changed but not committed<br>Exit with uncommitted changes?<br>[yes,no] (yes) |
| <b>Get Help</b>                                                                                                                                                                                                                                                                                                                                                                                                    |                                          |                                                                                                                                                        |



| Task                                                             | Command/Statement | Example                                                                                                                                                                                                                |
|------------------------------------------------------------------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display a list of valid options for the current hierarchy level. | ?                 | <pre>[edit ] user@host# edit security zones ?  Possible completions: &lt;[Enter]&gt; Execute this command &gt; functional-zone Functional zone &gt; security-zone Security zones   Pipe through a command [edit]</pre> |




## CHAPTER 12

# Firewall Filter and Policer Operational Mode Commands

## clear firewall

---

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                    | clear firewall (all   counter <i>counter-name</i>   filter <i>filter-name</i>   logical-system <i>logical-system-name</i> )                                                                                                                                                                                                                                                                                                                      |
| <b>Syntax (EX Series Switch)</b> | clear firewall (all   counter <i>counter-name</i>   filter <i>filter-name</i> )                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>       | Command introduced before Junos OS Release 7.4.<br>Command introduced in Junos OS Release 9.0 for EX Series switches.<br><b>logical-system</b> option introduced in Junos OS Release 9.3.                                                                                                                                                                                                                                                        |
| <b>Description</b>               | Clear statistics about configured firewall filters.<br><br><div> <b>NOTE:</b> The <b>clear firewall</b> command cannot be used to clear the Routing Engine filter counters on a backup Routing Engine that is enabled for GRES.</div>                                                                                                                           |
| <b>Options</b>                   | <p>all—Clear the packet and byte counts for all filters.</p> <p>counter <i>counter-name</i>—Clear the packet and byte counts for a filter counter that has been configured with the counter firewall filter action.</p> <p>filter <i>filter-name</i>—Clear the packet and byte counts for the specified firewall filter.</p> <p>logical-system <i>logical-system-name</i>—Clear the packet and byte counts for the specified logical system.</p> |
| <b>Required Privilege Level</b>  | clear                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>     | <ul style="list-style-type: none"><li>• <a href="#">show firewall on page 221</a></li></ul>                                                                                                                                                                                                                                                                                                                                                      |
| <b>List of Sample Output</b>     | <a href="#">clear firewall all on page 220</a>                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Output Fields</b>             | When you enter this command, you are provided feedback on the status of your request.                                                                                                                                                                                                                                                                                                                                                            |

## Sample Output

clear firewall all    user@host> clear firewall all

## show firewall

---

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                    | <pre>show firewall &lt;filter <i>filter-name</i>&gt; &lt;counter <i>counter-name</i>&gt; &lt;log&gt; &lt;logical-system (all   <i>logical-system-name</i>)&gt; &lt;terse&gt;</pre>                                                                                                                                                                                                                                                                                                                                                               |
| <b>Syntax (EX Series Switch)</b> | <pre>show firewall &lt;filter <i>filter-name</i>&gt; &lt;counter <i>counter-name</i>&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>       | <p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p><b>logical-system</b> option introduced in Junos OS Release 9.3.</p> <p><b>terse</b> option introduced in Junos OS Release 9.4.</p>                                                                                                                                                                                                                                                                          |
| <b>Description</b>               | Display statistics about configured firewall filters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Options</b>                   | <p><b>none</b>—(Optional) Display statistics about configured firewall filters.</p> <p><b>filter <i>filter-name</i></b>—(Optional) Name of a configured filter.</p> <p><b>counter <i>counter-name</i></b>—(Optional) Name of a filter counter.</p> <p><b>logical-system (all   <i>logical-system-name</i>)</b>—(Optional) Perform this operation on all logical systems or on a particular system.</p> <p><b>log</b>—(Optional) Display log entries for firewall filters.</p> <p><b>terse</b>—(Optional) Display firewall filter names only.</p> |
| <b>Required Privilege Level</b>  | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>     | <ul style="list-style-type: none"> <li>• <a href="#">clear firewall on page 220</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>List of Sample Output</b>     | <p><a href="#">show firewall filter on page 223</a></p> <p><a href="#">show firewall filter (Dynamic Input Filter) on page 223</a></p> <p><a href="#">show firewall (Logical Systems) on page 223</a></p>                                                                                                                                                                                                                                                                                                                                        |
| <b>Output Fields</b>             | <p><a href="#">Table 10 on page 222</a> lists the output fields for the <b>show firewall</b> command. Output fields are listed in the approximate order in which they appear.</p>                                                                                                                                                                                                                                                                                                                                                                |

Table 10: show firewall Output Fields

| Field Name      | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Filter</b>   | <p>Name of a filter that has been configured with the <b>filter</b> statement at the <b>[edit firewall]</b> hierarchy level.</p> <p>When an interface-specific filter is displayed, the name of the filter is followed by the full interface name and by either <b>-i</b> for an input filter or <b>-o</b> for an output filter.</p> <p>When dynamic filters are displayed, the name of the filter is followed by the full interface name and by either <b>-in</b> for an input filter or <b>-out</b> for an output filter. When a logical system-specific filter is displayed, the name of the filter is prefixed with two underscore (__) characters and the name of the logical system (for example, __ls1/filter1).</p> |
| <b>Counters</b> | <p>Display filter counter information:</p> <ul style="list-style-type: none"> <li>• <b>Name</b>—Name of a filter counter that has been configured with the <b>counter</b> firewall filter action.</li> <li>• <b>Bytes</b>—Number of bytes that match the filter term under which the <b>counter</b> action is specified.</li> <li>• <b>Packets</b>—Number of packets that matched the filter term under which the <b>counter</b> action is specified.</li> </ul>                                                                                                                                                                                                                                                            |
| <b>Policers</b> | <p>Display policer information:</p> <ul style="list-style-type: none"> <li>• <b>Name</b>—Name of policer.</li> <li>• <b>Bytes</b>—(I-chip DPCs only) Number of bytes that match the filter term under which the policer action is specified. This is only the number out-of-specification (out-of-spec) byte counts, not all the bytes in all packets policed by the policer.</li> <li>• <b>Packets</b>—Number of packets that matched the filter term under which the policer action is specified. This is only the number of out-of-specification (out-of-spec) packet counts, not all packets policed by the policer.</li> </ul>                                                                                         |

## Sample Output

```

show firewall filter user@host> show firewall filter test
Filter: test
Counters:
Name                               Bytes          Packets
Counter-1                          0              0
Counter-2                          0              0
Policers:
Name                               Bytes          Packets
Policer-1                         2770           70

show firewall filter user@host> show firewall filter dfwd-ge-5/0/0.1-in
(Dynamic Input Filter) Filter: dfwd-ge-5/0/0.1-in
Counters:
Name                               Bytes          Packets
c1-ge-5/0/0.1-in                  0              0

show firewall (Logical user@host>show firewall
Systems)
Filter: __lr1/test
Counters:
Name                               Bytes          Packets
icmp                              420            5
Filter: __default_bpdu_filter__
Filter: __lr1/inet_filter1
Counters:
Name                               Bytes          Packets
inet_tcp_count                     0              0
inet_udp_count                     0              0
Filter: __lr1/inet_filter2
Counters:
Name                               Bytes          Packets
inet_icmp_count                    0              0
inet_pim_count                     0              0
Filter: __lr2/inet_filter1
Counters:
Name                               Bytes          Packets
inet_tcp_count                     0              0
inet_udp_count                     0              0

```

## show firewall filter version

|                                 |                                                                                                                                                                                                                                                                    |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show firewall filter version <filter-name>                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Command introduced in Junos OS Release 10.2R2.                                                                                                                                                                                                                     |
| <b>Description</b>              | Display the version number of the installed firewall filter in the Routing Engine.                                                                                                                                                                                 |
| <b>Options</b>                  | <p>none—(Optional) Display the version number of all installed firewall filters.</p> <p>filter-name—(Optional) Name of a configured filter. If you specify the name of a filter, only the version number of that filter is displayed.</p>                          |
| <b>Additional Information</b>   | The initial version number is 1. This number increments by one when you modify the firewall filter settings or an associated prefix action. The maximum version number is 4,294,967,295. When the version number reaches 4,294,967,295, this number is reset to 1. |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                               |
| <b>List of Sample Output</b>    | <a href="#">show firewall filter version on page 224</a>                                                                                                                                                                                                           |
| <b>Output Fields</b>            | <a href="#">Table 11 on page 224</a> lists the output fields for the <b>show firewall filter version</b> command. Output fields are listed in the approximate order in which they appear.                                                                          |

Table 11: show firewall filter version Output Fields

| Field Name | Field Description                                                                                                         |
|------------|---------------------------------------------------------------------------------------------------------------------------|
| Filter     | Name of a filter that has been configured with the <b>filter</b> statement at the <b>[edit firewall]</b> hierarchy level. |
| Version    | Display the version number of the firewall filter.                                                                        |

### Sample Output

```

show firewall filter user@host> show firewall filter version
version             Filter version information :
                   Filter                                     Version
                   test                                      10

```



## show firewall log

|                                  |                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                    | show firewall log<br><detail><br><interface <i>interface-name</i> ><br><logical-system ( <i>logical-system-name</i>   all)>                                                                                                                                                                                                                                      |
| <b>Syntax (EX Series Switch)</b> | show firewall log<br><detail><br><interface <i>interface-name</i> >                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>       | Command introduced before Junos OS Release 7.4.<br>Command introduced in Junos OS Release 9.0 for EX Series switches.<br><b>logical-system</b> option introduced in Junos OS Release 9.3.                                                                                                                                                                        |
| <b>Description</b>               | Display log information about firewall filters.                                                                                                                                                                                                                                                                                                                  |
| <b>Options</b>                   | none—Display log information about firewall filters.<br><br>detail—(Optional) Display detailed information.<br><br>interface <i>interface-name</i> —(Optional) Display log information about a specific interface.<br><br>logical-system ( <i>logical-system-name</i>   all)—(Optional) Perform this operation on all logical systems or on a particular system. |
| <b>Required Privilege Level</b>  | view                                                                                                                                                                                                                                                                                                                                                             |
| <b>List of Sample Output</b>     | <a href="#">show firewall log on page 226</a><br><a href="#">show firewall log detail on page 226</a>                                                                                                                                                                                                                                                            |
| <b>Output Fields</b>             | <a href="#">Table 12 on page 225</a> lists the output fields for the <b>show firewall log</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                   |

**Table 12: show firewall log Output Fields**

| Field Name         | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Time of Log</b> | Time that the event occurred.                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Filter</b>      | <p>Name of a filter that has been configured with the <b>filter</b> statement at the <b>[edit firewall]</b> hierarchy level.</p> <ul style="list-style-type: none"> <li>A hyphen (-) indicates that the packet was handled by the Packet Forwarding Engine.</li> <li>A space (no hyphen) indicates the packet was handled by the Routing Engine.</li> <li>The notation <b>pfe</b> indicates packets logged by the Packet Forwarding Engine hardware filters.</li> </ul> |

Table 12: show firewall log Output Fields (*continued*)

| Field Name          | Field Description                                                                                                    |
|---------------------|----------------------------------------------------------------------------------------------------------------------|
| Filter Action       | Filter action: <ul style="list-style-type: none"> <li>• A—Accept</li> <li>• D—Discard</li> <li>• R—Reject</li> </ul> |
| Name of Interface   | Ingress interface for the packet.                                                                                    |
| Name of protocol    | Packet's protocol name: <b>egp, gre, icmp, ipip, ospf, pim, rsvp, tcp, or udp.</b>                                   |
| Packet length       | Length of the packet.                                                                                                |
| Source address      | Packet's source address.                                                                                             |
| Destination address | Packet's destination address and port.                                                                               |

## Sample Output

### show firewall log

```
user@host>show firewall log
Time      Filter  Action Interface  Protocol  Src Addr  Dest Addr
13:10:12  pfe      D      rlsq0.902   ICMP      180.1.177.2  180.1.177.1
13:10:11  pfe      D      rlsq0.902   ICMP      180.1.177.2  180.1.177.1
```

### show firewall log detail

```
user@host> show firewall log detail
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0Name of protocol: TCP, Packet Length: 50824, Source address:
172.17.22.108:829,
Destination address: 192.168.70.66:513
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0
Name of protocol: TCP, Packet Length: 1020, Source address: 172.17.22.108:829,
Destination address: 192.168.70.66:513
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 172.17.22.108:829,
Destination address: 192.168.70.66:513
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 172.17.22.108:829,
Destination address: 192.168.70.66:513
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 172.17.22.108:829,
Destination address: 192.168.70.66:513
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 172.17.22.108:829,
```

Destination address: 192.168.70.66:513  
.....

## show firewall prefix-action-stats

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show firewall prefix-action-stats filter <i>filter-name</i> prefix-action <i>prefix-action-name</i><br><from <i>number</i> to <i>number</i> ><br><logical-system ( <i>logical-system-name</i>   all)>                                                                                                                                                                                                                                                                                                                                |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.<br><b>logical-system</b> option introduced in Junos OS Release 9.3.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>              | Display prefix action statistics about configured firewall filters.<br><br>If you clear statistics for firewall filters that are applied to Trio-based DPCs and that also use the <b>prefix-action</b> action on matched packets, wait at least 5 seconds before you enter the <b>show firewall prefix-action-stats</b> command. A 5-second pause between issuing the <b>clear firewall</b> and <b>show firewall prefix-action-stats</b> commands avoids a possible timeout of the <b>show firewall prefix-action-stats</b> command. |
| <b>Options</b>                  | filter <i>filter-name</i> —Name of a filter.<br><br>prefix-action <i>prefix-action-name</i> —Name of a prefix action.<br><br>from <i>number</i> to <i>number</i> —(Optional) Starting and ending counter or policer.<br><br>logical-system ( <i>logical-system-name</i>   all)—(Optional) Perform this operation on all logical systems or on a particular system.                                                                                                                                                                   |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear firewall on page 220</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>List of Sample Output</b>    | <a href="#">show firewall prefix-action-stats on page 228</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Output Fields</b>            | <a href="#">Table 13 on page 228</a> lists the output fields for the <b>show firewall prefix-action-stats</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                       |

**Table 13: show firewall prefix-action-stats Output Fields**

| Field Name    | Field Description                                                                                                                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Filter</b> | Filter name.<br><br>Filters configured for logical systems include the name of the filter prefixed with the two underscore characters (__) and the name of the logical system (for example, __ls1/filter1). |

## Sample Output

```
show firewall prefix-action-stats user@host> show firewall prefix-action-stats filter test prefix-action act1
Filter: __ls2/test
```

## show policer

|                                 |                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show policer<br><policer-name>                                                                                                                                               |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                              |
| <b>Description</b>              | Display the number of policed packets for a given policer or an aggregate policer. An aggregate policer is an aggregate of different policers on the same logical interface. |
| <b>Options</b>                  | none—Display the number of policed packets for all configured policers.<br><br>policer-name—(Optional) Display the number of policed packets for the specified policer.      |
| <b>Required Privilege Level</b> | view                                                                                                                                                                         |
| <b>List of Sample Output</b>    | <a href="#">show policer on page 229</a><br><a href="#">show policer (Aggregate Policer) on page 229</a>                                                                     |
| <b>Output Fields</b>            | <a href="#">Table 14 on page 229</a> lists the output fields for the <b>show policer</b> command. Output fields are listed in the approximate order in which they appear.    |

**Table 14: show policer Output Fields**

| Field Name     | Field Description                                                                                                        |
|----------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>    | Name of the policer.                                                                                                     |
| <b>Bytes</b>   | (For policers applied to logical interfaces on I-chip DPCs only) Total number of bytes policed by the specified policer. |
| <b>Packets</b> | Total number of packets policed by the specified policer.                                                                |

## Sample Output

|                                         |                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>show policer</b>                     | user@host> show policer<br>Policers:<br>Name Bytes Packets<br>__default_arp_policer__ 314520 5242<br>pol-2M-ge-1/2/0.1-inet-i 10372300 103723<br>pol-2M-ge-1/2/0.1-inet6-i 7727800 77278<br>pol-2M-ge-1/2/0.1-mp1s-i 7070336 67984<br>pol-2M-ge-1/2/0.1001-vpls-i 65153700 651537<br>pol-2M-ge-1/2/0.2001-vpls-i 65180900 651809<br>pol-2M-ge-1/2/0.3001-ccc-i 62202144 647939 |
| <b>show policer (Aggregate Policer)</b> | user@host> show policer<br>Policers:<br>Name Packets<br>__default_arp_policer__ 0<br>P1-ae0.0-log_int-o 0<br>P2-ge-7/0/2.0-inet-o 0                                                                                                                                                                                                                                            |

|                       |   |
|-----------------------|---|
| P2-ge-7/0/2.0-inet6-o | 0 |
| __policer_tmpl__-term | 0 |
| __policer_tmpl__-fc0  | 0 |
| __policer_tmpl__-fc0  | 0 |
| __policer_tmpl__-fc1  | 0 |
| __policer_tmpl__-fc0  | 0 |
| __policer_tmpl__-fc1  | 0 |
| __policer_tmpl__-fc2  | 0 |
| __policer_tmpl__-fc0  | 0 |
| __policer_tmpl__-fc1  | 0 |
| __policer_tmpl__-fc2  | 0 |
| __policer_tmpl__-fc3  | 0 |

## PART 4

# Index

- [Index on page 233](#)
- [Index of Statements and Commands on page 239](#)





# Index

## A

|                                       |          |
|---------------------------------------|----------|
| action statement.....                 | 165      |
| aggregate (logical interface) policer |          |
| configuration statement for.....      | 190      |
| example                               |          |
| single-rate two-color.....            | 126      |
| two-rate three-color.....             | 131, 157 |
| overview.....                         | 125      |
| aggregate statement                   |          |
| hierarchical policer.....             | 166      |

## B

|                                 |     |
|---------------------------------|-----|
| bandwidth policer, logical      |     |
| example.....                    | 57  |
| overview.....                   | 56  |
| bandwidth-limit statement       |     |
| hierarchical policer.....       | 167 |
| policer.....                    | 168 |
| bandwidth-percent statement     |     |
| policer.....                    | 170 |
| burst-size-limit statement..... | 173 |
| hierarchical policer.....       | 172 |

## C

|                                           |     |
|-------------------------------------------|-----|
| class-of-service See CoS                  |     |
| clear firewall command.....               | 220 |
| color markings                            |     |
| policers.....                             | 26  |
| color modes for three-color policer.....  | 109 |
| color-aware statement.....                | 175 |
| color-blind statement.....                | 176 |
| committed-burst-size statement.....       | 177 |
| committed-information-rate statement..... | 179 |
| configuration and application overview    |     |
| hierarchical policers.....                | 22  |
| single-rate two-color policers.....       | 15  |
| three-color policers.....                 | 19  |
| CoS                                       |     |
| forwarding classes.....                   | 87  |
| policer actions, overview.....            | 3   |
| RED drop profiles.....                    | 87  |

## D

|                                                      |    |
|------------------------------------------------------|----|
| denial-of-service attacks, preventing.....           | 65 |
| diagnosis                                            |    |
| displaying stateless firewall filter                 |    |
| configurations.....                                  | 69 |
| displaying stateless firewall filter statistics..... | 70 |
| verifying stateless firewall filter DoS              |    |
| protection.....                                      | 69 |
| verifying stateless firewall filter flood            |    |
| protection.....                                      | 69 |
| DoS (denial-of-service) attacks, preventing.....     | 65 |
| dual token bucket algorithms.....                    | 30 |

## E

|                                  |     |
|----------------------------------|-----|
| excess-burst-size statement..... | 181 |
|----------------------------------|-----|

## F

|                                       |            |
|---------------------------------------|------------|
| filter-specific                       |            |
| counting and policing set.....        | 74         |
| policer.....                          | 64         |
| filter-specific policing option       |            |
| configuration scenarios.....          | 81         |
| example.....                          | 74         |
| overview.....                         | 71         |
| filter-specific statement.....        | 182        |
| configuration scenarios.....          | 81         |
| example.....                          | 74         |
| overview.....                         | 64, 71, 74 |
| firewall                              |            |
| filter version                        |            |
| displaying.....                       | 224        |
| statistics                            |            |
| displaying.....                       | 221        |
| firewall filters                      |            |
| log information, displaying.....      | 225        |
| physical interface filters.....       | 198        |
| policed packets, displaying.....      | 229        |
| statistics                            |            |
| clearing.....                         | 220        |
| displaying.....                       | 228        |
| flooding, preventing.....             | 65         |
| forwarding class                      |            |
| policer actions                       |            |
| overview.....                         | 3          |
| forwarding classes.....               | 87         |
| forwarding-class statement            |            |
| stateless firewall filter action..... | 183        |

**H**

|                                             |        |
|---------------------------------------------|--------|
| hierarchical policer                        |        |
| bandwidth limit.....                        | 25     |
| burst-size limit.....                       | 25     |
| color markings and actions.....             | 26     |
| configuration and application overview..... | 22     |
| configuration statement for                 |        |
| aggregate.....                              | 166    |
| premium.....                                | 205    |
| example.....                                | 149    |
| overview.....                               | 7, 147 |
| single token bucket algorithm.....          | 28     |
| hierarchical-policer statement.....         | 184    |

**I**

|                                                            |     |
|------------------------------------------------------------|-----|
| ICMP (Internet Control Message Protocol),<br>policers..... | 65  |
| if-exceeding statement                                     |     |
| hierarchical policer.....                                  | 185 |
| single-rate two-color policer.....                         | 186 |
| input-hierarchical-policer statement.....                  | 187 |
| input-policer statement.....                               | 187 |
| input-three-color statement.....                           | 188 |
| Internet Control Message Protocol policers.....            | 65  |

**L**

|                                       |          |
|---------------------------------------|----------|
| Layer 2 policer                       |          |
| hierarchical policer                  |          |
| configuration overview.....           | 22       |
| example.....                          | 149      |
| overview.....                         | 147      |
| three-color policer                   |          |
| overview.....                         | 156      |
| two-color policer                     |          |
| overview.....                         | 154      |
| layer2-policer statement.....         | 189      |
| hierarchical policing.....            | 22       |
| Layer 2 policer                       |          |
| three-color-policer                   |          |
| example.....                          | 131, 157 |
| logical bandwidth policer             |          |
| example.....                          | 57       |
| overview.....                         | 56       |
| logical interface (aggregate) policer |          |
| configuration statement for.....      | 190      |
| example                               |          |
| single-rate two-color.....            | 126      |
| two-rate three-color.....             | 131, 157 |
| overview.....                         | 125      |

|                                                                                           |     |
|-------------------------------------------------------------------------------------------|-----|
| logical interface-policer statement.....                                                  | 190 |
| logical-bandwidth-policer statement.....                                                  | 190 |
| loopback interface, applying stateless firewall filters<br>to (configuration editor)..... | 65  |
| loss-priority statement                                                                   |     |
| stateless firewall filter action.....                                                     | 191 |

**M**

|                                      |    |
|--------------------------------------|----|
| multifield classification            |    |
| example.....                         | 92 |
| limitations on M Series routers..... | 90 |
| overview.....                        | 87 |
| requirements and restrictions.....   | 89 |

**N**

|                          |     |
|--------------------------|-----|
| naming conventions       |     |
| three-color policer..... | 110 |

**O**

|                                   |     |
|-----------------------------------|-----|
| output-policer statement.....     | 193 |
| output-three-color statement..... | 194 |

**P**

|                                               |     |
|-----------------------------------------------|-----|
| packet loss priority                          |     |
| policer actions                               |     |
| overview.....                                 | 3   |
| peak-burst-size statement.....                | 195 |
| peak-information-rate statement.....          | 197 |
| physical interface policer                    |     |
| configuration statement for.....              | 199 |
| example.....                                  | 139 |
| overview.....                                 | 137 |
| physical-interface-filter statement.....      | 198 |
| physical-interface-policer statement.....     | 199 |
| ping command (stateless firewall filter)..... | 69  |
| explanation.....                              | 69  |
| policer                                       |     |
| and firewall filter                           |     |
| order of operations.....                      | 10  |
| applying to a logical interface.....          | 200 |
| bandwidth limit.....                          | 25  |
| burst size                                    |     |
| calculation of.....                           | 33  |
| burst-size limit.....                         | 25  |
| color markings and actions.....               | 26  |
| filter-specific.....                          | 64  |
| guidelines for applying.....                  | 24  |
| overview.....                                 | 3   |

|                                             |            |  |
|---------------------------------------------|------------|--|
| prefix-specific action                      |            |  |
| configuration scenarios.....                | 81         |  |
| example.....                                | 74         |  |
| overview.....                               | 71         |  |
| statement hierarchy.....                    | 13         |  |
| supported standards.....                    | 213        |  |
| term-specific.....                          | 64         |  |
| traffic-limiting criteria.....              | 25         |  |
| types.....                                  | 7          |  |
| policer actions                             |            |  |
| forwarding class                            |            |  |
| overview.....                               | 3          |  |
| packet loss-priority                        |            |  |
| overview.....                               | 3          |  |
| policer overhead for rate shaping           |            |  |
| example.....                                | 99         |  |
| overview.....                               | 99         |  |
| policer statement                           |            |  |
| configuring.....                            | 201        |  |
| stateless firewall filter action.....       | 202        |  |
| policer, hierarchical                       |            |  |
| and firewall filter                         |            |  |
| order of operations.....                    | 10         |  |
| bandwidth limit.....                        | 25         |  |
| burst size                                  |            |  |
| guidelines for calculating.....             | 33         |  |
| burst-size limit.....                       | 25         |  |
| color markings and actions.....             | 26         |  |
| configuration and application overview..... | 22         |  |
| configuration statement for.....            | 184        |  |
| aggregate.....                              | 166        |  |
| premium.....                                | 205        |  |
| example.....                                | 149        |  |
| overview.....                               | 7, 24, 147 |  |
| single token bucket algorithm.....          | 28         |  |
| policer, Layer 2                            |            |  |
| hierarchical policer                        |            |  |
| configuration overview.....                 | 22         |  |
| example.....                                | 149        |  |
| overview.....                               | 147        |  |
| three-color policer                         |            |  |
| overview.....                               | 156        |  |
| two-color policer                           |            |  |
| overview.....                               | 154        |  |
| policer, multifield classification          |            |  |
| example.....                                | 92         |  |
| limitations on M Series routers.....        | 90         |  |
| overview.....                               | 87         |  |
| requirements and restrictions.....          | 89         |  |
| policer, single-rate three-color            |            |  |
| bandwidth limit.....                        | 25         |  |
| burst size                                  |            |  |
| guidelines for calculating.....             | 33         |  |
| burst-size limit.....                       | 25         |  |
| color markings and actions.....             | 26         |  |
| color modes.....                            | 109        |  |
| configuration and application overview..... | 19         |  |
| dual token bucket algorithm.....            | 30         |  |
| example.....                                | 112        |  |
| logical interface (aggregate)               |            |  |
| overview.....                               | 125        |  |
| naming conventions.....                     | 110        |  |
| overview.....                               | 7, 111     |  |
| physical interface policer                  |            |  |
| overview.....                               | 137        |  |
| supported platforms.....                    | 109        |  |
| policer, single-rate two-color              |            |  |
| bandwidth limit.....                        | 25         |  |
| burst size                                  |            |  |
| guidelines for calculating.....             | 33         |  |
| burst-size limit.....                       | 25         |  |
| color markings and actions.....             | 26         |  |
| configuration and application overview..... | 15         |  |
| example.....                                | 40, 46     |  |
| logical bandwidth                           |            |  |
| example.....                                | 57         |  |
| overview.....                               | 56         |  |
| logical interface (aggregate)               |            |  |
| example.....                                | 126        |  |
| overview.....                               | 125        |  |
| overview.....                               | 7, 39      |  |
| physical interface policer                  |            |  |
| example.....                                | 139        |  |
| overview.....                               | 137        |  |
| prefix-specific action                      |            |  |
| configuration scenarios.....                | 81         |  |
| example.....                                | 74         |  |
| overview.....                               | 71         |  |
| single token bucket algorithm.....          | 28         |  |
| policer, two-rate three-color               |            |  |
| bandwidth limit.....                        | 25         |  |
| burst size                                  |            |  |
| guidelines for calculating.....             | 33         |  |
| burst-size limit.....                       | 25         |  |
| color markings and actions.....             | 26         |  |
| color modes.....                            | 109        |  |
| configuration and application overview..... | 19         |  |
| dual-rate dual token bucket algorithm.....  | 30         |  |

|                                                |          |                                             |            |
|------------------------------------------------|----------|---------------------------------------------|------------|
| example.....                                   | 118      | show policer command.....                   | 229        |
| logical interface (aggregate)                  |          | single token bucket algorithm.....          | 28         |
| example.....                                   | 131, 157 | single-rate statement.....                  | 206        |
| overview.....                                  | 125      | single-rate three-color policer             |            |
| naming conventions.....                        | 110      | and firewall filter                         |            |
| overview.....                                  | 7, 117   | order of operations.....                    | 10         |
| physical interface policer                     |          | bandwidth limit.....                        | 25         |
| overview.....                                  | 137      | burst-size limit.....                       | 25         |
| supported platforms.....                       | 109      | color markings and actions.....             | 26         |
| policers                                       |          | color modes.....                            | 109        |
| for stateless firewall filters.....            | 65       | configuration and application summary.....  | 19         |
| policers, displaying.....                      | 229      | dual token bucket algorithm.....            | 30         |
| prefix-action statement                        |          | example.....                                | 112        |
| configuration scenarios.....                   | 81       | Layer 2 policer                             |            |
| configuring.....                               | 203      | overview.....                               | 156        |
| example.....                                   | 74       | logical interface (aggregate)               |            |
| firewall filter action.....                    | 204      | overview.....                               | 125        |
| overview.....                                  | 71       | naming conventions.....                     | 110        |
| prefix-specific action                         |          | overview.....                               | 7, 24, 111 |
| filter-specific.....                           | 74       | physical interface policer                  |            |
| term-specific.....                             | 74       | overview.....                               | 137        |
| prefix-specific counting and policing          |          | supported platforms.....                    | 109        |
| configuration scenarios.....                   | 81       | single-rate two-color policer               |            |
| example.....                                   | 74       | and firewall filter                         |            |
| overview.....                                  | 71       | order of operations.....                    | 10         |
| premium statement                              |          | at Layer 2                                  |            |
| hierarchical policer.....                      | 205      | overview.....                               | 154        |
| <b>R</b>                                       |          | burst-size limit.....                       | 25         |
| rate-shaping                                   |          | color markings and actions.....             | 26         |
| configuring policer overhead for               |          | configuration and application overview..... | 15         |
| example.....                                   | 99       | example.....                                | 40, 46     |
| overview.....                                  | 99       | logical bandwidth                           |            |
| RED drop profiles.....                         | 87       | example.....                                | 57         |
| Routing Engine                                 |          | overview.....                               | 56         |
| protecting against DoS attacks.....            | 65       | logical interface (aggregate)               |            |
| routing solutions                              |          | example.....                                | 126        |
| protecting against DoS attacks.....            | 65       | overview.....                               | 125        |
| <b>S</b>                                       |          | overview.....                               | 7, 24, 39  |
| sample configurations                          |          | physical interface policer                  |            |
| firewall filter configurations.....            | 69       | example.....                                | 139        |
| show firewall command.....                     | 69, 221  | overview.....                               | 137        |
| show firewall filter protect-RE command.....   | 70       | prefix-specific action                      |            |
| show firewall filter version command.....      | 224      | configuration scenarios.....                | 81         |
| show firewall log command.....                 | 225      | example.....                                | 74         |
| show firewall prefix-action-stats command..... | 228      | overview.....                               | 71         |
| show interfaces lo0 command.....               | 65       | single token bucket algorithm.....          | 28         |
| show interfaces policers command.....          | 126      |                                             |            |

|                                                       |            |
|-------------------------------------------------------|------------|
| standard stateless firewall filters                   |            |
| multifield classification                             |            |
| example.....                                          | 92         |
| limitations on M Series routers.....                  | 90         |
| overview.....                                         | 87         |
| requirements and restrictions.....                    | 89         |
| standards                                             |            |
| supported for policing.....                           | 213        |
| stateless firewall filters                            |            |
| applying to an interface (configuration editor).....  | 65         |
| displaying configurations.....                        | 69         |
| displaying statistics.....                            | 70         |
| policers for.....                                     | 65         |
| protecting the Routing Engine against TCP floods..... | 65         |
| verifying configuration.....                          | 69         |
| verifying flood protection.....                       | 69         |
| statistics                                            |            |
| stateless firewall filters.....                       | 70         |
| supported platforms                                   |            |
| three-color policer.....                              | 109        |
| <b>T</b>                                              |            |
| TCP policers.....                                     | 65         |
| telnet command.....                                   | 69         |
| term-specific                                         |            |
| counting and policing set.....                        | 74         |
| policer.....                                          | 64         |
| three-color policer                                   |            |
| color modes.....                                      | 109        |
| naming conventions.....                               | 110        |
| single-rate                                           |            |
| example.....                                          | 112        |
| overview.....                                         | 111        |
| supported platforms.....                              | 109        |
| two-rate.....                                         | 111, 117   |
| example.....                                          | 118        |
| overview.....                                         | 117        |
| See also policer, single-rate three-color             |            |
| See also policer, two-rate three-color                |            |
| three-color-policer statement.....                    | 207        |
| stateless firewall filter action.....                 | 208        |
| token bucket algorithm                                |            |
| dual bucket.....                                      | 30         |
| dual-rate dual bucket.....                            | 30         |
| single bucket.....                                    | 28         |
| traffic-limiting criteria                             |            |
| policers.....                                         | 25         |
| two-rate statement.....                               | 209        |
| two-rate three-color policer                          |            |
| bandwidth limit.....                                  | 25         |
| burst-size limit.....                                 | 25         |
| color markings and actions.....                       | 26         |
| color modes.....                                      | 109        |
| configuration and application overview.....           | 19         |
| dual-rate dual token bucket algorithm.....            | 30         |
| example.....                                          | 118        |
| Layer 2 policer                                       |            |
| overview.....                                         | 156        |
| logical interface (aggregate)                         |            |
| example.....                                          | 131, 157   |
| overview.....                                         | 125        |
| naming conventions.....                               | 110        |
| overview.....                                         | 7, 24, 117 |
| physical interface policer                            |            |
| overview.....                                         | 137        |
| supported platforms.....                              | 109        |
| two-rate three-color-policer                          |            |
| and firewall filter                                   |            |
| order of operations.....                              | 10         |
| <b>V</b>                                              |            |
| verification                                          |            |
| stateless firewall filter flood protection.....       | 69         |
| stateless firewall filters.....                       | 69         |
| stateless firewall statistics.....                    | 70         |



# Index of Statements and Commands

## A

|                           |     |
|---------------------------|-----|
| action statement.....     | 165 |
| aggregate statement       |     |
| hierarchical policer..... | 166 |

## B

|                                 |     |
|---------------------------------|-----|
| bandwidth-limit statement       |     |
| hierarchical policer.....       | 167 |
| policer.....                    | 168 |
| bandwidth-percent statement     |     |
| policer.....                    | 170 |
| burst-size-limit statement..... | 173 |
| hierarchical policer.....       | 172 |

## C

|                                           |     |
|-------------------------------------------|-----|
| clear firewall command.....               | 220 |
| color-aware statement.....                | 175 |
| color-blind statement.....                | 176 |
| committed-burst-size statement.....       | 177 |
| committed-information-rate statement..... | 179 |

## E

|                                  |     |
|----------------------------------|-----|
| excess-burst-size statement..... | 181 |
|----------------------------------|-----|

## F

|                                       |            |
|---------------------------------------|------------|
| filter-specific statement.....        | 182        |
| overview.....                         | 64, 71, 74 |
| forwarding-class statement            |            |
| stateless firewall filter action..... | 183        |

## H

|                                     |     |
|-------------------------------------|-----|
| hierarchical-policer statement..... | 184 |
|-------------------------------------|-----|

## I

|                                    |     |
|------------------------------------|-----|
| if-exceeding statement             |     |
| hierarchical policer.....          | 185 |
| single-rate two-color policer..... | 186 |

|                                           |     |
|-------------------------------------------|-----|
| input-hierarchical-policer statement..... | 187 |
| input-policer statement.....              | 187 |
| input-three-color statement.....          | 188 |

## L

|                                          |     |
|------------------------------------------|-----|
| layer2-policer statement.....            | 189 |
| hierarchical policing.....               | 22  |
| logical interface-policer statement..... | 190 |
| logical-bandwidth-policer statement..... | 190 |
| loss-priority statement                  |     |
| stateless firewall filter action.....    | 191 |

## O

|                                   |     |
|-----------------------------------|-----|
| output-policer statement.....     | 193 |
| output-three-color statement..... | 194 |

## P

|                                           |     |
|-------------------------------------------|-----|
| peak-burst-size statement.....            | 195 |
| peak-information-rate statement.....      | 197 |
| physical-interface-filter statement.....  | 198 |
| physical-interface-policer statement..... | 199 |
| policer                                   |     |
| applying to a logical interface.....      | 200 |
| policer statement                         |     |
| configuring.....                          | 201 |
| stateless firewall filter action.....     | 202 |
| prefix-action statement                   |     |
| configuring.....                          | 203 |
| firewall filter action.....               | 204 |
| premium statement                         |     |
| hierarchical policer.....                 | 205 |

## S

|                                                |         |
|------------------------------------------------|---------|
| show firewall command.....                     | 69, 221 |
| show firewall filter version command.....      | 224     |
| show firewall log command.....                 | 225     |
| show firewall prefix-action-stats command..... | 228     |
| show interfaces policers command.....          | 126     |
| show policer command.....                      | 229     |
| single-rate statement.....                     | 206     |

## T

|                                       |     |
|---------------------------------------|-----|
| three-color-policer statement.....    | 207 |
| stateless firewall filter action..... | 208 |
| two-rate statement.....               | 209 |

