

VYATTA, INC.

| **Vyatta System**

Policy and QoS

REFERENCE GUIDE

Routing Policies

Quality of Service



Vyatta
Suite 200
1301 Shoreway Road
Belmont, CA 94002
vyatta.com
650 413 7200
1 888 VYATTA 1 (US and Canada)

COPYRIGHT

Copyright © 2005–2009 Vyatta, Inc. All rights reserved.

Vyatta reserves the right to make changes to software, hardware, and documentation without notice. For the most recent version of documentation, visit the Vyatta web site at vyatta.com.

PROPRIETARY NOTICES

Vyatta is a registered trademark of Vyatta, Inc.

VMware, VMware ESX, and VMware server are trademarks of VMware, Inc.

All other trademarks are the property of their respective owners.

ISSUE DATE: February 2009

DOCUMENT REVISION: VC5 v03

RELEASED WITH: VC5.0.2

PART NO. A0-0120-10-0002

Table of Contents

Quick Reference to Commands	vii
Quick List of Examples	xii
Preface	xiv
Intended Audience	xv
Organization of This Guide	xv
Document Conventions	xvi
Advisory Paragraphs	xvi
Typographic Conventions	xvi
Vyatta Publications	xvii
Chapter 1 Routing Policies	1
Routing Policy Commands	2
policy access-list <list-num>	6
policy access-list <list-num> description <desc>	7
policy access-list <list-num> rule <rule-num>	8
policy access-list <list-num> rule <rule-num> action	9
policy access-list <list-num> rule <rule-num> description <desc>	11
policy access-list <list-num> rule <rule-num> destination	12
policy access-list <list-num> rule <rule-num> source	14
policy as-path-list <list-name>	16
policy as-path-list <list-name> description <desc>	17
policy as-path-list <list-name> rule <rule-num>	18
policy as-path-list <list-name> rule <rule-num> action	19
policy as-path-list <list-name> rule <rule-num> description <desc>	21
policy as-path-list <list-name> rule <rule-num> regex <regex>	22
policy community-list <list-num>	24
policy community-list <list-num> description <desc>	25
policy community-list <list-num> rule <rule-num>	26
policy community-list <list-num> rule <rule-num> action	27

policy community-list <list-num> rule <rule-num> description <desc>	29
policy community-list <list-num> rule <rule-num> regex <regex>	30
policy prefix-list <list-name>	32
policy prefix-list <list-name> description <desc>	33
policy prefix-list <list-name> rule <rule-num>	34
policy prefix-list <list-name> rule <rule-num> action	35
policy prefix-list <list-name> rule <rule-num> description <desc>	37
policy prefix-list <list-name> rule <rule-num> ge <value>	38
policy prefix-list <list-name> rule <rule-num> le <value>	40
policy prefix-list <list-name> rule <rule-num> prefix <ipv4net>	42
policy route-map <map-name>	44
policy route-map <map-name> description <desc>	45
policy route-map <map-name> rule <rule-num>	46
policy route-map <map-name> rule <rule-num> action	47
policy route-map <map-name> rule <rule-num> call <target>	49
policy route-map <map-name> rule <rule-num> continue <target-num>	50
policy route-map <map-name> rule <rule-num> description <desc>	51
policy route-map <map-name> rule <rule-num> match as-path <list-name>	52
policy route-map <map-name> rule <rule-num> match community	54
policy route-map <map-name> rule <rule-num> match interface <ethx>	56
policy route-map <map-name> rule <rule-num> match ip address	58
policy route-map <map-name> rule <rule-num> match ip nexthop	60
policy route-map <map-name> rule <rule-num> match ip route-source	62
policy route-map <map-name> rule <rule-num> match metric <metric>	64
policy route-map <map-name> rule <rule-num> match origin	66
policy route-map <map-name> rule <rule-num> match peer <ipv4>	68
policy route-map <map-name> rule <rule-num> match tag <tag>	70
policy route-map <map-name> rule <rule-num> on-match	72
policy route-map <map-name> rule <rule-num> set aggregator	74
policy route-map <map-name> rule <rule-num> set as-path-prepend <prepend>	76
policy route-map <map-name> rule <rule-num> set atomic-aggregate	77
policy route-map <map-name> rule <rule-num> set comm-list	78
policy route-map <map-name> rule <rule-num> set community	80
policy route-map <map-name> rule <rule-num> set ip-next-hop <ipv4>	82
policy route-map <map-name> rule <rule-num> set local-preference <local-pref>	83
policy route-map <map-name> rule <rule-num> set metric <metric>	84
policy route-map <map-name> rule <rule-num> set metric-type <type>	85
policy route-map <map-name> rule <rule-num> set origin	87
policy route-map <map-name> rule <rule-num> set originator-id <ipv4>	89
policy route-map <map-name> rule <rule-num> set tag <tag>	90
policy route-map <map-name> rule <rule-num> set weight <weight>	91
show ip access-list	92
show ip as-path-access-list	93
show ip community-list	94

show ip extcommunity-list	95
show ip prefix-list	96
show ip protocol	98
show route-map	100
Chapter 2 Quality of Service	102
QoS Configuration	103
QoS Overview	103
QoS Mechanisms	103
Drop Tail	104
Fair Queue	104
Rate Limiting	104
Traffic Shaping	104
Traffic Limiting	104
QoS Configuration Example	104
QoS Commands	108
interfaces adsl <adslx> pvc <pvc-id> bridged-ethernet qos-policy out <policy-name>	112
interfaces adsl <adslx> pvc <pvc-id> classical-ipoa qos-policy out <policy-name>	114
interfaces adsl <adslx> pvc <pvc-id> pppoa <num> qos-policy out <policy-name>	116
interfaces adsl <adslx> pvc <pvc-id> pppoe <num> qos-policy out <policy-name>	118
interfaces bonding <bondx> qos-policy out <policy-name>	120
interfaces ethernet <ethx> pppoe <num> qos-policy out <policy-name>	121
interfaces ethernet <ethx> qos-policy	123
interfaces ethernet <ethx> vif <vlan-id> qos-policy out <policy-name>	125
interfaces serial <wanx> qos-policy	127
qos-policy drop-tail <policy-name>	129
qos-policy drop-tail <policy-name> queue-limit <limit>	130
qos-policy fair-queue <policy-name>	131
qos-policy fair-queue <policy-name> description <desc>	133
qos-policy fair-queue <policy-name> hash-interval <seconds>	134
qos-policy fair-queue <policy-name> queue-limit <limit>	136
qos-policy rate-limit <policy-name>	138
qos-policy rate-limit <policy-name> bandwidth	140
qos-policy rate-limit <policy-name> burst	142
qos-policy rate-limit <policy-name> description <desc>	144
qos-policy rate-limit <policy-name> latency	145
qos-policy traffic-limiter <policy-name>	147
qos-policy traffic-limiter <policy-name> class <class>	148
qos-policy traffic-limiter <policy-name> class <class> bandwidth	150
qos-policy traffic-limiter <policy-name> class <class> description <desc>	152
qos-policy traffic-limiter <policy-name> class <class> match <match-name>	154
qos-policy traffic-limiter <policy-name> class <class> match <match-name> description <desc>	156

qos-policy traffic-limiter <policy-name> class <class> match <match-name> ip destination	158
qos-policy traffic-limiter <policy-name> class <class> match <match-name> ip dscp <value>	160
qos-policy traffic-limiter <policy-name> class <class> match <match-name> ip protocol <proto>	162
qos-policy traffic-limiter <policy-name> class <class> match <match-name> ip source	164
qos-policy traffic-limiter <policy-name> class <class> match <match-name> vif <vlan-id>	166
qos-policy traffic-limiter <policy-name> class <class> priority <priority>	168
qos-policy traffic-limiter <policy-name> description <desc>	170
qos-policy traffic-shaper <policy-name>	171
qos-policy traffic-shaper <policy-name> bandwidth	173
qos-policy traffic-shaper <policy-name> class <class>	175
qos-policy traffic-shaper <policy-name> class <class> bandwidth	177
qos-policy traffic-shaper <policy-name> class <class> burst	179
qos-policy traffic-shaper <policy-name> class <class> ceiling	181
qos-policy traffic-shaper <policy-name> class <class> description <desc>	183
qos-policy traffic-shaper <policy-name> class <class> match <match-name>	185
qos-policy traffic-shaper <policy-name> class <class> match <match-name> description <desc>	187
qos-policy traffic-shaper <policy-name> class <class> match <match-name> interface <interface>	189
qos-policy traffic-shaper <policy-name> class <class> match <match-name> ip destination	191
qos-policy traffic-shaper <policy-name> class <class> match <match-name> ip dscp <value>	193
qos-policy traffic-shaper <policy-name> class <class> match <match-name> ip protocol <proto>	195
qos-policy traffic-shaper <policy-name> class <class> match <match-name> ip source	197
qos-policy traffic-shaper <policy-name> class <class> match <match-name> vif <vlan-id>	199
qos-policy traffic-shaper <policy-name> class <class> priority <priority>	201
qos-policy traffic-shaper <policy-name> class <class> queue-limit <limit>	203
qos-policy traffic-shaper <policy-name> class <class> queue-type <type>	205
qos-policy traffic-shaper <policy-name> class <class> set-dscp <value>	207
qos-policy traffic-shaper <policy-name> default	209
qos-policy traffic-shaper <policy-name> default bandwidth	210
qos-policy traffic-shaper <policy-name> default burst	212
qos-policy traffic-shaper <policy-name> default ceiling	214
qos-policy traffic-shaper <policy-name> default priority <priority>	216
qos-policy traffic-shaper <policy-name> default queue-limit <limit>	218
qos-policy traffic-shaper <policy-name> default queue-type <type>	220
qos-policy traffic-shaper <policy-name> default set-dscp <value>	222
qos-policy traffic-shaper <policy-name> description <desc>	224
show queueing	225
Glossary of Acronyms	227

Quick Reference to Commands

Use this section to help you quickly locate a command.

interfaces adsl <adslx> pvc <pvc-id> bridged-ethernet qos-policy out <policy-name>	112
interfaces adsl <adslx> pvc <pvc-id> classical-ipoa qos-policy out <policy-name>	114
interfaces adsl <adslx> pvc <pvc-id> pppoa <num> qos-policy out <policy-name>	116
interfaces adsl <adslx> pvc <pvc-id> pppoe <num> qos-policy out <policy-name>	118
interfaces bonding <bondx> qos-policy out <policy-name>	120
interfaces ethernet <ethx> pppoe <num> qos-policy out <policy-name>	121
interfaces ethernet <ethx> qos-policy	123
interfaces ethernet <ethx> vif <vlan-id> qos-policy out <policy-name>	125
interfaces serial <wanx> qos-policy	127
policy access-list <list-num>	6
policy access-list <list-num> description <desc>	7
policy access-list <list-num> rule <rule-num>	8
policy access-list <list-num> rule <rule-num> action	9
policy access-list <list-num> rule <rule-num> description <desc>	11
policy access-list <list-num> rule <rule-num> destination	12
policy access-list <list-num> rule <rule-num> source	14
policy as-path-list <list-name>	16
policy as-path-list <list-name> description <desc>	17
policy as-path-list <list-name> rule <rule-num>	18
policy as-path-list <list-name> rule <rule-num> action	19
policy as-path-list <list-name> rule <rule-num> description <desc>	21
policy as-path-list <list-name> rule <rule-num> regex <regex>	22
policy community-list <list-num>	24
policy community-list <list-num> description <desc>	25
policy community-list <list-num> rule <rule-num>	26
policy community-list <list-num> rule <rule-num> action	27
policy community-list <list-num> rule <rule-num> description <desc>	29
policy community-list <list-num> rule <rule-num> regex <regex>	30
policy prefix-list <list-name>	32
policy prefix-list <list-name> description <desc>	33
policy prefix-list <list-name> rule <rule-num>	34
policy prefix-list <list-name> rule <rule-num> action	35

policy prefix-list <list-name> rule <rule-num> description <desc>	37
policy prefix-list <list-name> rule <rule-num> ge <value>	38
policy prefix-list <list-name> rule <rule-num> le <value>	40
policy prefix-list <list-name> rule <rule-num> prefix <ipv4net>	42
policy route-map <map-name>	44
policy route-map <map-name> description <desc>	45
policy route-map <map-name> rule <rule-num>	46
policy route-map <map-name> rule <rule-num> action	47
policy route-map <map-name> rule <rule-num> call <target>	49
policy route-map <map-name> rule <rule-num> continue <target-num>	50
policy route-map <map-name> rule <rule-num> description <desc>	51
policy route-map <map-name> rule <rule-num> match as-path <list-name>	52
policy route-map <map-name> rule <rule-num> match community	54
policy route-map <map-name> rule <rule-num> match interface <ethx>	56
policy route-map <map-name> rule <rule-num> match ip address	58
policy route-map <map-name> rule <rule-num> match ip nexthop	60
policy route-map <map-name> rule <rule-num> match ip route-source	62
policy route-map <map-name> rule <rule-num> match metric <metric>	64
policy route-map <map-name> rule <rule-num> match origin	66
policy route-map <map-name> rule <rule-num> match peer <ipv4>	68
policy route-map <map-name> rule <rule-num> match tag <tag>	70
policy route-map <map-name> rule <rule-num> on-match	72
policy route-map <map-name> rule <rule-num> set aggregator	74
policy route-map <map-name> rule <rule-num> set as-path-prepend <prepend>	76
policy route-map <map-name> rule <rule-num> set atomic-aggregate	77
policy route-map <map-name> rule <rule-num> set comm-list	78
policy route-map <map-name> rule <rule-num> set community	80
policy route-map <map-name> rule <rule-num> set ip-next-hop <ipv4>	82
policy route-map <map-name> rule <rule-num> set local-preference <local-pref>	83
policy route-map <map-name> rule <rule-num> set metric <metric>	84
policy route-map <map-name> rule <rule-num> set metric-type <type>	85
policy route-map <map-name> rule <rule-num> set origin	87
policy route-map <map-name> rule <rule-num> set originator-id <ipv4>	89
policy route-map <map-name> rule <rule-num> set tag <tag>	90
policy route-map <map-name> rule <rule-num> set weight <weight>	91
qos-policy drop-tail <policy-name>	129
qos-policy drop-tail <policy-name> queue-limit <limit>	130
qos-policy fair-queue <policy-name>	131
qos-policy fair-queue <policy-name> description <desc>	133
qos-policy fair-queue <policy-name> hash-interval <seconds>	134
qos-policy fair-queue <policy-name> queue-limit <limit>	136
qos-policy rate-limit <policy-name>	138
qos-policy rate-limit <policy-name> bandwidth	140
qos-policy rate-limit <policy-name> burst	142

qos-policy rate-limit <policy-name> description <desc>	144
qos-policy rate-limit <policy-name> latency	145
qos-policy traffic-limiter <policy-name>	147
qos-policy traffic-limiter <policy-name> class <class>	148
qos-policy traffic-limiter <policy-name> class <class> bandwidth	150
qos-policy traffic-limiter <policy-name> class <class> description <desc>	152
qos-policy traffic-limiter <policy-name> class <class> match <match-name>	154
qos-policy traffic-limiter <policy-name> class <class> match <match-name> description <desc>	156
qos-policy traffic-limiter <policy-name> class <class> match <match-name> ip destination	158
qos-policy traffic-limiter <policy-name> class <class> match <match-name> ip dscp <value>	160
qos-policy traffic-limiter <policy-name> class <class> match <match-name> ip protocol <proto>	162
qos-policy traffic-limiter <policy-name> class <class> match <match-name> ip source	164
qos-policy traffic-limiter <policy-name> class <class> match <match-name> vif <vlan-id>	166
qos-policy traffic-limiter <policy-name> class <class> priority <priority>	168
qos-policy traffic-limiter <policy-name> description <desc>	170
qos-policy traffic-shaper <policy-name>	171
qos-policy traffic-shaper <policy-name> bandwidth	173
qos-policy traffic-shaper <policy-name> class <class>	175
qos-policy traffic-shaper <policy-name> class <class> bandwidth	177
qos-policy traffic-shaper <policy-name> class <class> burst	179
qos-policy traffic-shaper <policy-name> class <class> ceiling	181
qos-policy traffic-shaper <policy-name> class <class> description <desc>	183
qos-policy traffic-shaper <policy-name> class <class> match <match-name>	185
qos-policy traffic-shaper <policy-name> class <class> match <match-name> description <desc>	187
qos-policy traffic-shaper <policy-name> class <class> match <match-name> interface <interface>	189
qos-policy traffic-shaper <policy-name> class <class> match <match-name> ip destination	191
qos-policy traffic-shaper <policy-name> class <class> match <match-name> ip dscp <value>	193
qos-policy traffic-shaper <policy-name> class <class> match <match-name> ip protocol <proto>	195
qos-policy traffic-shaper <policy-name> class <class> match <match-name> ip source	197
qos-policy traffic-shaper <policy-name> class <class> match <match-name> vif <vlan-id>	199
qos-policy traffic-shaper <policy-name> class <class> priority <priority>	201
qos-policy traffic-shaper <policy-name> class <class> queue-limit <limit>	203
qos-policy traffic-shaper <policy-name> class <class> queue-type <type>	205
qos-policy traffic-shaper <policy-name> class <class> set-dscp <value>	207
qos-policy traffic-shaper <policy-name> default	209
qos-policy traffic-shaper <policy-name> default bandwidth	210
qos-policy traffic-shaper <policy-name> default burst	212
qos-policy traffic-shaper <policy-name> default ceiling	214
qos-policy traffic-shaper <policy-name> default priority <priority>	216
qos-policy traffic-shaper <policy-name> default queue-limit <limit>	218
qos-policy traffic-shaper <policy-name> default queue-type <type>	220
qos-policy traffic-shaper <policy-name> default set-dscp <value>	222
qos-policy traffic-shaper <policy-name> description <desc>	224
show ip access-list	92

show ip as-path-access-list	93
show ip community-list	94
show ip extcommunity-list	95
show ip prefix-list	96
show ip protocol	98
show queueing	225
show route-map	100

Quick List of Examples

Use this list to help you locate examples you'd like to try or look at.

Example 1-1	"show ip access-list": Displaying IP access lists	92
Example 1-2	"show ip as-path-access-list": Displaying as-path access lists	93
Example 1-3	"show ip community-list": Displaying community lists	94
Example 1-4	"show ip extcommunity-list": Displaying extended IP community lists	95
Example 1-5	"show ip prefix-list": Displaying prefix lists	96
Example 1-6	"show ip protocol": Displaying IP route maps by protocol	98
Example 1-7	"show route-map": Displaying route map information	100
Example 2-2	"show queueing": Displaying all QoS policies.	225
Example 2-3	"show queueing ethernet eth0": Displaying QoS policies on a specific interface.	226

Preface

This guide describes commands for routing policies and for quality of service (QoS) on the Vyatta system.

This preface provides information about using this guide. The following topics are covered:

- Intended Audience
- Organization of This Guide
- Document Conventions
- Vyatta Publications

Intended Audience

This guide is intended for experienced system and network administrators. Depending on the functionality to be used, readers should have specific knowledge in the following areas:

- Networking and data communications
- TCP/IP protocols
- General router configuration
- Routing protocols
- Network administration
- Network security

Organization of This Guide

This guide has the following aid to help you find the information you are looking for:

- **Quick Reference to Commands**

Use this section to help you quickly locate a command.

- **Use this list to help you locate examples you'd like to try or look at.**

Use this list to help you locate examples you'd like to try or look at.

This guide has the following chapters:

Chapter	Description	Page
Chapter 1: Routing Policies	This chapter describes commands for implementing routing policies on the Vyatta system.	1
Chapter 2: Quality of Service	This chapter describes commands for implementing quality of service (QoS) on the Vyatta system.	102
Glossary of Acronyms		227

Document Conventions

This guide contains advisory paragraphs and uses typographic conventions.

Advisory Paragraphs

This guide uses the following advisory paragraphs:

Warnings alert you to situations that may pose a threat to personal safety, as in the following example:



WARNING *Risk of injury. Switch off power at the main breaker before attempting to connect the remote cable to the service power at the utility box.*

Cautions alert you to situations that might cause harm to your system or damage to equipment, or that may affect service, as in the following example:



CAUTION *Risk of loss of service. Restarting a running system will interrupt service.*

Notes provide information you might need to avoid problems or configuration errors:

NOTE *You must create and configure network interfaces before enabling them for routing protocols.*

Typographic Conventions

This document uses the following typographic conventions:

<code>Courier</code>	Examples, command-line output, and representations of configuration nodes.
<code>boldface Courier</code>	In an example, your input: something you type at a command line.
<code>boldface</code>	In-line commands, keywords, and file names .
<i>italics</i>	Arguments and variables, where you supply a value.
<key>	A key on your keyboard. Combinations of keys are joined by plus signs (“+”). An example is <Ctrl>+<Alt>+.
[<i>arg1</i> <i>arg2</i>]	Enumerated options for completing a syntax. An example is [enable disable].

<i>num1–numN</i>	A inclusive range of numbers. An example is 1–65535, which means 1 through 65535.
<i>arg1..argN</i>	A range of enumerated values. An example is eth0..eth3, which means eth0, eth1, eth2, and eth3.
<i>arg [arg ...]</i> <i>arg,[arg,...]</i>	A value that can optionally represent a list of elements (a space-separated list in the first case, and a comma-separated list in the second case).

Vyatta Publications

More information about the Vyatta system is available in the Vyatta technical library, and on www.vyatta.com and www.vyatta.org.

Full product documentation is provided in the Vyatta technical library. To see what documentation is available for your release, see the *Vyatta Documentation Map*. This guide is posted with every release of Vyatta software and provides a great starting point for finding what you need.

Chapter 1: Routing Policies

This chapter describes commands for implementing routing policies on the Vyatta system.

This chapter presents the following topics:

- Routing Policy Commands

Routing Policy Commands

This chapter contains the following commands.

Configuration Commands

Access Lists

policy access-list <list-num>	Defines an access list.
policy access-list <list-num> description <desc>	Allows you to specify a brief description for an access list.
policy access-list <list-num> rule <rule-num>	Creates a rule for an access list.
policy access-list <list-num> rule <rule-num> action	Specifies the action to be taken for packets matching an access list rule.
policy access-list <list-num> rule <rule-num> description <desc>	Allows you to specify a brief description for an access list rule.
policy access-list <list-num> rule <rule-num> destination	Defines match criteria for an access list rule based on destination.
policy access-list <list-num> rule <rule-num> source	Defines match criteria for an access list rule based on source.

AS Path Lists

policy as-path-list <list-name>	Defines an autonomous system (AS) path list.
policy as-path-list <list-name> description <desc>	Allows you to specify a brief description for an AS path list.
policy as-path-list <list-name> rule <rule-num>	Creates a rule for an AS path list.
policy as-path-list <list-name> rule <rule-num> action	Specifies the action to be taken for packets matching an AS path list rule.
policy as-path-list <list-name> rule <rule-num> description <desc>	Allows you to specify a brief description for an AS path list rule.
policy as-path-list <list-name> rule <rule-num> regex <regex>	Defines match criteria for an AS path list rule based on a regular expression.

Community Lists

policy community-list <list-num>	Defines a BGP community list.
policy community-list <list-num> description <desc>	Allows you to specify a brief description for a community list.
policy community-list <list-num> rule <rule-num>	Creates a rule for a community list.

policy community-list <list-num> rule <rule-num> action	Specifies the action to be taken for packets matching a community list rule.
policy community-list <list-num> rule <rule-num> description <desc>	Allows you to specify a brief description for a community list rule.
policy community-list <list-num> rule <rule-num> regex <regex>	Defines match criteria for a community list rule based on a regular expression.

Prefix Lists

policy prefix-list <list-name>	Defines a prefix list.
policy prefix-list <list-name> description <desc>	Allows you to specify a brief description for a prefix list.
policy prefix-list <list-name> rule <rule-num>	Creates a rule for a prefix list.
policy prefix-list <list-name> rule <rule-num> action	Specifies the action to be taken for packets matching a prefix list rule.
policy prefix-list <list-name> rule <rule-num> description <desc>	Allows you to specify a brief description for a prefix list rule.
policy prefix-list <list-name> rule <rule-num> ge <value>	Defines match criteria for a prefix list rule based on a "greater-than-or-equal-to" numeric comparison.
policy prefix-list <list-name> rule <rule-num> le <value>	Defines a match criterion based on a "less-than-or-equal-to" numeric comparison for a prefix list rule.
policy prefix-list <list-name> rule <rule-num> prefix <ipv4net>	Defines match criteria for a prefix list rule based on an IPv4 network.

Route Maps

policy route-map <map-name>	Defines a route map for policy-based routing.
policy route-map <map-name> description <desc>	Allows you to specify a brief description for a route map.
policy route-map <map-name> rule <rule-num>	Creates a rule for a route map.
policy route-map <map-name> rule <rule-num> action	Specifies the action to be taken for packets matching a route map rule.
policy route-map <map-name> rule <rule-num> call <target>	Calls to another route map.
policy route-map <map-name> rule <rule-num> continue <target-num>	Calls to another rule within the current route map.
policy route-map <map-name> rule <rule-num> description <desc>	Allows you to specify a brief description for a route map rule.

policy route-map <map-name> rule <rule-num> match as-path <list-name>	Defines a match condition for a route map based on an AS path list
policy route-map <map-name> rule <rule-num> match community	Defines a match condition for a route map based on BGP communities.
policy route-map <map-name> rule <rule-num> match interface <ethx>	Defines a match condition for a route map based on the first-hop interface.
policy route-map <map-name> rule <rule-num> match ip address	Defines a match condition for a route map based on IP address.
policy route-map <map-name> rule <rule-num> match ip nexthop	Defines a match condition for a route map based on the next-hop address.
policy route-map <map-name> rule <rule-num> match ip route-source	Defines a match condition for a route map based on the address from where a route is advertised.
policy route-map <map-name> rule <rule-num> match metric <metric>	Defines a match condition for a route map based on the route's metric.
policy route-map <map-name> rule <rule-num> match origin	Defines a match condition for a route map based on the route's origin.
policy route-map <map-name> rule <rule-num> match peer <ipv4>	Defines a match condition for a route map based on peer IP address.
policy route-map <map-name> rule <rule-num> match tag <tag>	Defines a match condition for a route map based on OSPF tag.
policy route-map <map-name> rule <rule-num> on-match	Specifies an alternative exit policy for a route map.
policy route-map <map-name> rule <rule-num> set aggregator	Modifies the BGP aggregator attribute of a route.
policy route-map <map-name> rule <rule-num> set as-path-prepend <prepend>	Sets or prepends to the AS path of the route.
policy route-map <map-name> rule <rule-num> set atomic-aggregate	Sets the BGP atomic-aggregate attribute in a route.
policy route-map <map-name> rule <rule-num> set comm-list	Modifies the BGP community list in a route.
policy route-map <map-name> rule <rule-num> set community	Modifies the BGP communities attribute in a route.
policy route-map <map-name> rule <rule-num> set ip-next-hop <ipv4>	Modifies the next hop destination of a route.
policy route-map <map-name> rule <rule-num> set local-preference <local-pref>	Modifies the BGP local-pref attribute in a route.
policy route-map <map-name> rule <rule-num> set metric <metric>	Modifies the metric of a route.

policy route-map <map-name> rule <rule-num> set metric-type <type>	Specifies the OSPF external metric-type for a route.
policy route-map <map-name> rule <rule-num> set metric-type <type>	Modifies the BGP origin code of a route.
policy route-map <map-name> rule <rule-num> set originator-id <ipv4>	Modifies the BGP originator ID attribute of a route.
policy route-map <map-name> rule <rule-num> set tag <tag>	Modifies the OSPF tag value of a route.
policy route-map <map-name> rule <rule-num> set weight <weight>	Modifies the BGP weight of a route.

Operational Commands

show ip access-list	Displays all IP access lists.
show ip as-path-access-list	Displays all as-path access lists.
show ip community-list	Displays all IP community lists.
show ip extcommunity-list	Displays all extended IP community lists.
show ip prefix-list	Displays IP prefix lists.
show ip protocol	Displays IP route maps per protocol.
show route-map	Displays route map information.

policy access-list <list-num>

Defines an access list.

Syntax

```
set policy access-list list-num  
delete policy access-list list-num  
show policy access-list list-num
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
    access-list u32 {}  
}
```

Parameters

<i>list-num</i>	Mandatory. Multi-node. A numeric identifier for the access list. Access list numbers can take the following values: 1 to 99: IP standard access list 100 to 199: IP extended access list 1300 to 1999: IP standard access list (expanded range) 2000 to 2699: IP extended access list (expanded range) You can create multiple access lists by creating multiple policy access-list configuration nodes.
-----------------	--

Default

None.

Usage Guidelines

Use the **set** form of this command to create an access list.

Use the **delete** form of this command to remove an access list.

Use the **show** form of this command to display access list configuration.

policy access-list <list-num> description <desc>

Allows you to specify a brief description for an access list.

Syntax

set policy access-list *list-num* **description** *desc*

delete policy access-list *list-num* **description**

show policy access-list *list-num* **description**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  access-list u32 {  
    description: text  
  }  
}
```

Parameters

<i>list-num</i>	Mandatory. The number of a defined access list.
<i>desc</i>	Mandatory. A brief text description for the access list.

Default

None.

Usage Guidelines

Use the **set** form of this command to create a description for an access list.

Use the **delete** form of this command to remove an access list description.

Use the **show** form of this command to display the description for an access list.

policy access-list <list-num> rule <rule-num>

Creates a rule for an access list.

Syntax

```
set policy access-list list-num rule rule-num
delete policy access-list list-num rule rule-num
show policy access-list list-num rule rule-num
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {
  access-list u32 {
    rule u32 {}
  }
}
```

Parameters

<i>list-num</i>	Mandatory. The number of a defined access list.
<i>rule-num</i>	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1 to 4294967295. You can define multiple rules by creating multiple rule configuration nodes.

Default

None.

Usage Guidelines

Use the **set** form of this command to create an access list rule.

Use the **delete** form of this command to remove an access list rule.

Use the **show** form of this command to display configuration settings for an access list rule.

policy access-list <list-num> rule <rule-num> action

Specifies the action to be taken for packets matching an access list rule.

Syntax

set policy access-list *list-num* **rule** *rule-num* **action** {**deny** | **permit**}

delete policy access-list *list-num* **rule** *rule-num* **action**

show policy access-list *list-num* **rule** *rule-num* **action**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  access-list u32 {  
    rule u32 {  
      action {  
        deny  
        permit  
      }  
    }  
  }  
}
```

Parameters

<i>list-num</i>	Mandatory. The number of a defined access list.
<i>rule-num</i>	Mandatory. The number of a defined access list rule.
deny	Optional. Packets matching this rule are silently dropped.
permit	Optional. Packets matching this rule are forwarded.

Default

Packets matching this rule are forwarded.

Usage Guidelines

Use the **set** form of this command to define the action taken when received packets satisfy the match criteria for this rule.

If the action for a rule is **deny**, packets meeting the match criteria of the rule are silently dropped. If the action for the rule is **permit**, packets meeting the match criteria of the rule are forwarded.

Use the **delete** form of this command to restore the default action for packets satisfying the match criteria.

Use the **show** form of this command to display action settings for this rule.

policy access-list <list-num> rule <rule-num> description <desc>

Allows you to specify a brief description for an access list rule.

Syntax

```
set policy access-list list-num rule rule-num description desc  
delete policy access-list list-num rule rule-num description  
show policy access-list list-num rule rule-num description
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
    access-list u32 {  
        rule u32 {  
            description: text  
        }  
    }  
}
```

Parameters

<i>list-num</i>	Mandatory. The number of a defined access list.
<i>rule-num</i>	Mandatory. The number of a defined access list rule.
<i>desc</i>	Mandatory. A brief text description for the access list rule.

Default

None.

Usage Guidelines

Use the **set** form of this command to create a description for an access list rule.

Use the **delete** form of this command to remove an access list rule description.

Use the **show** form of this command to display an access list rule description.

policy access-list <list-num> rule <rule-num> destination

Defines match criteria for an access list rule based on destination.

Syntax

set policy access-list *list-num* **rule** *rule-num* **destination** { **any** | **host** *ipv4* | **inverse-mask** *ipv4* | **network** *ipv4net* }

delete policy access-list *list-num* **rule** *rule-num* **destination**

show policy access-list *list-num* **rule** *rule-num* **destination**

Command Mode

Configuration mode.

Configuration Statement

```
policy {
  access-list u32 {
    rule u32 {
      destination {
        any
        host: ipv4
        inverse-mask: ipv4
        network: ipv4net
      }
    }
  }
}
```

Parameters

<i>list-num</i>	Mandatory. The number of a defined access list.
<i>rule-num</i>	Mandatory. The number of a defined access list.
any	Match packets destined for any destination. Exactly one of any , host , inverse-mask , and network is mandatory.
host <i>ipv4</i>	Match packets destined for the specified IPv4 host. Exactly one of any , host , inverse-mask , and network is mandatory.
inverse-mask <i>ipv4</i>	Match packets destined for the network specified by the mask. Exactly one of any , host , inverse-mask , and network is mandatory.

network <i>ipv4net</i>	Match packets coming from the specified network. The format is <i>ip-address/prefix</i> . Exactly one of any , host , inverse-mask , and network is mandatory.
-------------------------------	--

Default

None.

Usage Guidelines

Use the **set** form of this command to specify the destination match criteria for this access list rule.

Use the **delete** form of this command to remove configured destination match criteria for this rule. If no match criteria are specified, no packet filtering on destination will take place; that is, packets to all destinations are permitted.

Use the **show** form of this command to display configuration settings for access list rule destination packet filtering.

policy access-list <list-num> rule <rule-num> source

Defines match criteria for an access list rule based on source.

Syntax

set policy access-list *list-num* **rule** *rule-num* **source** { **any** | **host** *ipv4* | **inverse-mask** *ipv4* | **network** *ipv4net* }

delete policy access-list *list-num* **rule** *rule-num* **source**

show policy access-list *list-num* **rule** *rule-num* **source**

Command Mode

Configuration mode.

Configuration Statement

```
policy {
  access-list u32 {
    rule u32 {
      source {
        any
        host: ipv4
        inverse-mask: ipv4
        network: ipv4net
      }
    }
  }
}
```

Parameters

<i>list-num</i>	Mandatory. The number of a defined access list.
<i>rule-num</i>	Mandatory. The number of a defined access list rule.
any	Match packets coming from any source. Exactly one of any , host , inverse-mask , and network is mandatory.
host <i>ipv4</i>	Match packets coming from the specified IPv4 host. Exactly one of any , host , inverse-mask , and network is mandatory.
inverse-mask <i>ipv4</i>	Match packets coming from the network specified by the mask. Exactly one of any , host , inverse-mask , and network is mandatory.

network <i>ipv4net</i>	Match packets coming from the specified network. The format is <i>ip-address/prefix</i> . Exactly one of any , host , inverse-mask , and network is mandatory.
-------------------------------	--

Default

None.

Usage Guidelines

Use the **set** form of this command to specify the source match criteria for this access list rule.

Use the **delete** form of this command to remove the configured source match criteria for this rule. If no match criteria are specified, no packet filtering on source will take place; that is, packets from all sources are permitted.

Use the **show** form of this command to display configuration settings for access list rule source packet filtering.

policy as-path-list <list-name>

Defines an autonomous system (AS) path list.

Syntax

```
set policy as-path-list list-name
delete policy as-path-list list-name
show policy as-path-list list-name
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {
    as-path-list text {}
}
```

Parameters

<i>list-name</i>	Mandatory. Multi-node. A text identifier for the AS path list. You can create multiple AS path lists by creating multiple policy as-path-list configuration nodes.
------------------	--

Default

None.

Usage Guidelines

Use the **set** form of this command to define an autonomous system (AS) path list for use in policy-based routing.

Use the **delete** form of this command to remove an AS path list.

Use the **show** form of this command to display AS path list configuration.

policy as-path-list <list-name> description <desc>

Allows you to specify a brief description for an AS path list.

Syntax

```
set policy as-path-list list-name description desc  
delete policy as-path-list list-name description  
show policy as-path-list list-name description
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  as-path-list text {  
    description: text  
  }  
}
```

Parameters

<i>list-name</i>	Mandatory. The name of a defined AS path list.
<i>desc</i>	Mandatory. A brief text description for the AS path list.

Default

None.

Usage Guidelines

Use the **set** form of this command to specify a description for an AS path list.

Use the **delete** form of this command to remove an AS path list description.

Use the **show** form of this command to display an AS path list description.

policy as-path-list <list-name> rule <rule-num>

Creates a rule for an AS path list.

Syntax

```
set policy as-path-list list-name rule rule-num
delete policy as-path-list list-name rule rule-num
show policy as-path-list list-name rule rule-num
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {
  as-path-list text {
    rule u32 {}
  }
}
```

Parameters

<i>list-name</i>	Mandatory. The name of a defined AS path list.
<i>rule-num</i>	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1 to 4294967295. You can define multiple rules by creating multiple rule configuration nodes.

Default

None.

Usage Guidelines

Use the **set** form of this command to create an AS path list rule.

Use the **delete** form of this command to remove an AS path list rule.

Use the **show** form of this command to display configuration settings for an AS path list rule.

policy as-path-list <list-name> rule <rule-num> action

Specifies the action to be taken for packets matching an AS path list rule.

Syntax

set policy as-path-list *list-name* **rule** *rule-num* **action** { **deny** | **permit** }

delete policy as-path-list *list-name* **rule** *rule-num* **action**

show policy as-path-list *list-name* **rule** *rule-num* **action**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  as-path-list text {  
    rule u32 {  
      action {  
        deny  
        permit  
      }  
    }  
  }  
}
```

Parameters

<i>list-name</i>	Mandatory. The name of a defined AS path list.
<i>rule-num</i>	Mandatory. The number of a defined AS path list rule.
deny	Optional. Packets matching this rule are silently dropped.
permit	Optional. Packets matching this rule are forwarded.

Default

Packets matching this rule are forwarded.

Usage Guidelines

Use the **set** form of this command to define the action taken when received packets satisfy the match criteria for this rule.

If the action for a rule is **deny**, packets meeting the match criteria of the rule are silently dropped. If the action for the rule is **permit**, destination-based routing is performed; that is, packets are sent using the normal forwarding channels.

Use the **delete** form of this command to restore the default action for packets satisfying the match criteria.

Use the **show** form of this command to display action settings for this rule.

policy as-path-list <list-name> rule <rule-num> description <desc>

Allows you to specify a brief description for an AS path list rule.

Syntax

```
set policy as-path-list list-name rule rule-num description desc  
delete policy as-path-list list-name rule rule-num description  
show policy as-path-list list-name rule rule-num description
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  as-path-list text {  
    rule u32 {  
      description: text  
    }  
  }  
}
```

Parameters

<i>list-name</i>	Mandatory. The name of a defined AS path list.
<i>rule-num</i>	Mandatory. The number of a defined AS path list rule.
<i>desc</i>	Mandatory. A brief text description for the AS path list rule.

Default

None.

Usage Guidelines

Use the **set** form of this command to specify a description for an AS path list.

Use the **delete** form of this command to remove an AS path list description.

Use the **show** form of this command to display an AS path list description.

policy as-path-list <list-name> rule <rule-num> regex <regex>

Defines match criteria for an AS path list rule based on a regular expression.

Syntax

set policy as-path-list *list-name* **rule** *rule-num* **regex** *regex*

delete policy as-path-list *list-name* **rule** *rule-num* **regex**

show policy as-path-list *list-name* **rule** *rule-num* **regex**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  as-path-list text {  
    rule u32 {  
      regex: text  
    }  
  }  
}
```

Parameters

<i>list-name</i>	Mandatory. The name of a defined AS path list.
<i>rule-num</i>	Mandatory. The number of a defined AS path list rule.
<i>regex</i>	Mandatory. A POSIX-style regular expression representing an AS path list.

Default

If no regular expression is defined, all packets are considered to match the rule.

Usage Guidelines

Use the **set** form of this command to define the match criteria to be used to determine forwarding policy based on AS paths.

Packets are matched based on whether the AS paths listed in the packet match the regular expression defined using this command. Depending on the action defined for the rule using the **policy as-path-list <list-name> rule <rule-num> action** command (see page 19), matched packets are either permitted or denied.

Use the **delete** form of this command to remove the regular expression entry. If no regular expression is defined, all packets are considered to match the rule.

Use the **show** form of this command to display the regular expression entry.

policy community-list <list-num>

Defines a BGP community list.

Syntax

```
set policy community-list list-num
delete policy community-list list-num
show policy community-list list-num
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {
    community-list: u32 {}
}
```

Parameters

<i>list-num</i>	Mandatory. Multi-node. A numeric identifier for the community list. You can create multiple community lists by creating multiple policy community-list configuration nodes.
-----------------	---

Default

None.

Usage Guidelines

Use the **set** form of this command to create a BGP community list for use in policy-based routing.

Use the **delete** form of this command to remove a community list.

Use the **show** form of this command to display community list configuration.

policy community-list <list-num> description <desc>

Allows you to specify a brief description for a community list.

Syntax

set policy community-list *list-num* **description** *desc*

delete policy community-list *list-num* **description**

show policy community-list *list-num* **description**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
    community-list u32 {  
        description: text  
    }  
}
```

Parameters

<i>list-num</i>	Mandatory. The number of a defined community list.
<i>desc</i>	Mandatory. A brief text description for the community list.

Default

None.

Usage Guidelines

Use the **set** form of this command to create a description for a community list.

Use the **delete** form of this command to remove a community list description.

Use the **show** form of this command to display the description for a community list.

policy community-list <list-num> rule <rule-num>

Creates a rule for a community list.

Syntax

```
set policy community-list list-num rule rule-num
delete policy community-list list-num rule rule-num
show policy community-list list-num rule rule-num
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {
  community-list u32 {
    rule u32 {}
  }
}
```

Parameters

<i>list-num</i>	Mandatory. The number of a defined community list.
<i>rule-num</i>	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1 to 4294967295. You can define multiple rules by creating multiple rule configuration nodes.

Default

None.

Usage Guidelines

Use the **set** form of this command to create a community list rule.

Use the **delete** form of this command to remove a community list rule.

Use the **show** form of this command to display configuration settings for a community list rule.

policy community-list <list-num> rule <rule-num> action

Specifies the action to be taken for packets matching a community list rule.

Syntax

set policy community-list *list-num* **rule** *rule-num* **action** { **deny** | **permit** }

delete policy community-list *list-num* **rule** *rule-num* **action**

show policy community-list *list-num* **rule** *rule-num* **action**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  community-list u32 {  
    rule u32 {  
      action {  
        deny  
        permit  
      }  
    }  
  }  
}
```

Parameters

<i>list-num</i>	Mandatory. The number of a defined community list.
<i>rule-num</i>	Mandatory. The number of a defined community list rule.
deny	Optional. Packets matching this rule are silently dropped.
permit	Optional. Packets matching this rule are forwarded.

Default

Packets matching this rule are forwarded.

Usage Guidelines

Use the **set** form of this command to define the action taken when received packets satisfy the match criteria for this rule.

If the action for a rule is **deny**, packets meeting the match criteria of the rule are silently dropped. If the action for the rule is **permit**, destination-based routing is performed; that is, packets are sent using the normal forwarding channels.

Use the **delete** form of this command to restore the default action for packets satisfying the match criteria.

Use the **show** form of this command to display action settings for this rule.

policy community-list <list-num> rule <rule-num> description <desc>

Allows you to specify a brief description for a community list rule.

Syntax

```
set policy community-list list-num rule rule-num description desc  
delete policy community-list list-num rule rule-num description  
show policy community-list list-num rule rule-num description
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
    community-list u32 {  
        rule u32 {  
            description: text  
        }  
    }  
}
```

Parameters

<i>list-num</i>	Mandatory. The number of a defined community list.
<i>rule-num</i>	Mandatory. The number of a defined community list rule.
<i>desc</i>	Mandatory. A brief text description for the community list rule.

Default

None.

Usage Guidelines

Use the **set** form of this command to create a description for a community list rule.

Use the **delete** form of this command to remove a community list rule description.

Use the **show** form of this command to display the description for a community list rule.

policy community-list <list-num> rule <rule-num> regex <regex>

Defines match criteria for a community list rule based on a regular expression.

Syntax

set policy community-list *list-num* **rule** *rule-num* **regex** *regex*

delete policy community-list *list-num* **rule** *rule-num* **regex**

show policy community-list *list-num* **rule** *rule-num* **regex**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
    community-list u32 {  
        rule u32 {  
            regex: text  
        }  
    }  
}
```

Parameters

<i>list-num</i>	Mandatory. The number of a defined community list.
<i>rule-num</i>	Mandatory. The number of a defined community list rule.
<i>regex</i>	Mandatory. A POSIX-style regular expression representing a BGP community list.

Default

If no regular expression is defined, all packets are considered to match the rule.

Usage Guidelines

Use the **set** form of this command to define the match criteria to be used to determine forwarding policy based on BGP community.

Packets are matched based on whether the communities listed in the packet match the regular expression defined using this command. Depending on the action defined for the rule using the **policy community-list <list-num> rule <rule-num> action** command (see page 27), matched packets are either permitted or denied.

Use the **delete** form of this command to remove the regular expression entry. If no regular expression is defined, all packets are considered to match the rule.

Use the **show** form of this command to display the regular expression entry.

policy prefix-list <list-name>

Defines a prefix list.

Syntax

```
set policy prefix-list list-name  
delete policy prefix-list list-name  
show policy prefix-list list-name
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
    prefix-list text {}  
}
```

Parameters

<i>list-name</i>	Mandatory. Multi-node. A text identifier for the prefix list. You can create multiple prefix lists by creating multiple policy prefix-list configuration nodes.
------------------	---

Default

None.

Usage Guidelines

Use the **set** form of this command to create a prefix list for use in policy-based routing.

Use the **delete** form of this command to remove a prefix list.

Use the **show** form of this command to display prefix list configuration.

policy prefix-list <list-name> description <desc>

Allows you to specify a brief description for a prefix list.

Syntax

```
set policy prefix-list list-name description desc  
delete policy prefix-list list-name description  
show policy prefix-list list-name description
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
    prefix-list text {  
        description: text  
    }  
}
```

Parameters

<i>list-name</i>	Mandatory. The name of a defined prefix list.
<i>desc</i>	Mandatory. A brief text description for the prefix list.

Default

None.

Usage Guidelines

Use the **set** form of this command to create a description for a prefix list.

Use the **delete** form of this command to remove a prefix list description.

Use the **show** form of this command to display the description for a prefix list.

policy prefix-list <list-name> rule <rule-num>

Creates a rule for a prefix list.

Syntax

```
set policy prefix-list list-name rule rule-num
delete policy prefix-list list-name rule rule-num
show policy prefix-list list-name rule rule-num
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {
  prefix-list text {
    rule u32 {}
  }
}
```

Parameters

<i>list-name</i>	Mandatory. The name of a defined prefix list.
<i>rule-num</i>	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1 to 4294967295. You can define multiple rules by creating multiple rule configuration nodes.

Default

None.

Usage Guidelines

Use the **set** form of this command to create a prefix list rule.

Use the **delete** form of this command to remove a prefix list rule.

Use the **show** form of this command to display configuration settings for a prefix list rule.

policy prefix-list <list-name> rule <rule-num> action

Specifies the action to be taken for packets matching a prefix list rule.

Syntax

set policy prefix-list *list-name* **rule** *rule-num* **action** { **deny** | **permit** }

delete policy prefix-list *list-name* **rule** *rule-num* **action**

show policy prefix-list *list-name* **rule** *rule-num* **action**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  prefix-list text {  
    rule u32 {  
      action {  
        deny  
        permit  
      }  
    }  
  }  
}
```

Parameters

<i>list-name</i>	Mandatory. The name of a defined prefix list.
<i>rule-num</i>	Mandatory. The number of a defined prefix list rule.
deny	Optional. Packets matching this rule are silently dropped.
permit	Optional. Packets matching this rule are forwarded.

Default

Packets matching this rule are forwarded.

Usage Guidelines

Use the **set** form of this command to define the action taken when received packets satisfy the match criteria for this rule.

If the action for a rule is **deny**, packets meeting the match criteria of the rule are silently dropped. If the action for the rule is **permit**, destination-based routing is performed; that is, packets are sent using the normal forwarding channels.

Use the **delete** form of this command to restore the default action for packets satisfying the match criteria.

Use the **show** form of this command to display action settings for this rule.

policy prefix-list <list-name> rule <rule-num> description <desc>

Allows you to specify a brief description for a prefix list rule.

Syntax

set policy prefix-list *list-name* **rule** *rule-num* **description** *desc*

delete policy prefix-list *list-name* **rule** *rule-num* **description**

show policy prefix-list *list-name* **rule** *rule-num* **description**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  prefix-list text {  
    rule u32 {  
      description: text  
    }  
  }  
}
```

Parameters

<i>list-name</i>	Mandatory. The name of a defined prefix list.
<i>rule-num</i>	Mandatory. The number of a defined prefix list rule.
<i>desc</i>	Mandatory. A brief text description for the prefix list rule.

Default

None.

Usage Guidelines

Use the **set** form of this command to create a description for a prefix list rule.

Use the **delete** form of this command to remove a prefix list rule description.

Use the **show** form of this command to display the description for a prefix list rule.

policy prefix-list <list-name> rule <rule-num> ge <value>

Defines match criteria for a prefix list rule based on a “greater-than-or-equal-to” numeric comparison.

Syntax

set policy prefix-list *list-name* **rule** *rule-num* **ge** *value*

delete policy prefix-list *list-name* **rule** *rule-num* **ge**

show policy prefix-list *list-name* **rule** *rule-num* **ge**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  prefix-list text {  
    rule u32 {  
      ge: 0-32  
    }  
  }  
}
```

Parameters

<i>list-name</i>	Mandatory. The name of a defined prefix list.
<i>rule-num</i>	Mandatory. The number of a defined prefix list rule.
<i>value</i>	Mandatory. A number representing a network prefix. Network prefixes greater than or equal to this number will match this rule. The range of values is 0 to 32.

Default

If no prefix is specified, all network prefixes are considered to match the rule.

Usage Guidelines

Use the **set** form of this command to specify a network prefix for determining routing. The network prefixes of incoming packets are compared with this value; if the prefix is greater than or equal to the specified prefix, the rule is matched and the action specified for the rule is taken.

Exactly one comparison (**ge**, **le**, or **prefix**) may be specified for a prefix list rule.

Use the **delete** form of this command to remove the specified “ge” prefix. If no prefix is specified, all network prefixes are considered to match the rule.

Use the **show** form of this command to display the value specified as “ge” prefix.

policy prefix-list <list-name> rule <rule-num> le <value>

Defines a match criterion based on a “less-than-or-equal-to” numeric comparison for a prefix list rule.

Syntax

set policy prefix-list *list-name* **rule** *rule-num* **le** *value*

delete policy prefix-list *list-name* **rule** *rule-num* **le**

show policy prefix-list *list-name* **rule** *rule-num* **le**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  prefix-list text {  
    rule u32 {  
      le: 0-32  
    }  
  }  
}
```

Parameters

<i>list-name</i>	Mandatory. The name of a defined prefix list.
<i>rule-num</i>	Mandatory. The number of a defined prefix list rule.
<i>value</i>	Mandatory. A number representing a network prefix. Network prefixes less than or equal to this number will match this rule. The range of values is 0 to 32.

Default

If no prefix is specified, all network prefixes are considered to match the rule.

Usage Guidelines

Use the **set** form of this command to specify a network prefix for determining routing policy. The network prefixes of incoming packets are compared with this value; if the prefix is less than or equal to the specified prefix, the rule is matched and the action specified for the rule is taken.

Exactly one comparison (**ge**, **le**, or **prefix**) may be specified for a prefix list rule.

Use the **delete** form of this command to remove the specified “le” prefix. If no prefix is specified, all network prefixes are considered to match the rule.

Use the **show** form of this command to display the value specified as “le” prefix.

policy prefix-list <list-name> rule <rule-num> prefix <ipv4net>

Defines match criteria for a prefix list rule based on an IPv4 network.

Syntax

set policy prefix-list *list-name* **rule** *rule-number* **prefix** *ipv4net*

delete policy prefix-list *list-name* **rule** *rule-num* **prefix**

show policy prefix-list *list-name* **rule** *rule-num* **prefix**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  prefix-list text {  
    rule u32 {  
      prefix: ipv4net  
    }  
  }  
}
```

Parameters

<i>list-name</i>	Mandatory. The name of a defined prefix list.
<i>rule-num</i>	Mandatory. The number of a defined prefix list rule.
<i>ipv4net</i>	Mandatory. An IPv4 network. Networks exactly matching this network will match this rule. The format is <i>ip-address/prefix</i> .

Default

If no network is specified, all networks are considered to match the rule.

Usage Guidelines

Use the **set** form of this command to specify a network for determining routing policy. The network specified in incoming packets are compared with this value; if it exactly matches the network specified in this command, the rule is matched and the action specified for the rule is taken.

Exactly one comparison (**ge**, **le**, or **prefix**) may be specified for a prefix list rule.

Use the **delete** form of this command to remove the specified “ge” prefix. If no prefix is specified, all network prefixes are considered to match the rule.

Use the **show** form of this command to display the value specified as “ge” prefix.

policy route-map <map-name>

Defines a route map for policy-based routing.

Syntax

```
set policy route-map map-name
delete policy route-map map-name
show policy route-map map-name
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {
    route-map text {}
}
```

Parameters

<i>map-name</i>	Mandatory. Multi-node. A text identifier for the route map. You can create multiple route maps by creating multiple policy route-map configuration nodes.
-----------------	---

Default

None.

Usage Guidelines

Use the **set** form of this command to create a route map for policy-based routing.

Use the **delete** form of this command to remove a route map.

Use the **show** form of this command to display route map configuration.

policy route-map <map-name> description <desc>

Allows you to specify a brief description for a route map.

Syntax

```
set policy route-map map-name description desc  
delete policy route-map map-name description  
show policy route-map map-name description
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
    route-map text {  
        description: text  
    }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>desc</i>	Mandatory. A brief text description for the route map.

Default

None.

Usage Guidelines

Use the **set** form of this command to create a description for a route map.

Use the **delete** form of this command to remove a route map policy description.

Use the **show** form of this command to display the description for a route map.

policy route-map <map-name> rule <rule-num>

Creates a rule for a route map.

Syntax

```
set policy route-map map-name rule rule-num  
delete policy route-map map-name rule rule-num  
show policy route-map map-name rule rule-num
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
    route-map text {  
        rule u32 {}  
    }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1 to 4294967295. You can define multiple rules by creating multiple rule configuration nodes.

Default

None.

Usage Guidelines

Use the **set** form of this command to create a route map rule.

Use the **delete** form of this command to remove a route map rule.

Use the **show** form of this command to display configuration settings for a route map rule.

policy route-map <map-name> rule <rule-num> action

Specifies the action to be taken for packets matching a route map rule.

Syntax

set policy route-map *map-name* **rule** *rule-num* **action** {deny | permit}

delete policy route-map *map-name* **rule** *rule-num* **action**

show policy route-map *map-name* **rule** *rule-num* **action**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      action {  
        deny  
        permit  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
deny	Optional. Packets matching this rule are silently dropped.
permit	Optional. Packets matching this rule are forwarded.

Default

Routes are denied.

Usage Guidelines

Use the **set** form of this command to define the action taken when received packets satisfy the match criteria for this rule.

If the action for a rule is **deny**, packets meeting the match criteria of the rule are silently dropped. If the action for the rule is **permit**, destination-based routing is performed; that is, packets are sent using the normal forwarding channels.

The default action of a route map is to deny; that is if no entries satisfy the match criteria the route is denied. To change this behavior, specify an empty **permit** rule as the last entry in the route map.

Use the **delete** form of this command to restore the default action for packets satisfying the match criteria.

Use the **show** form of this command to display action settings for this rule.

policy route-map <map-name> rule <rule-num> call <target>

Calls to another route map.

Syntax

set policy route-map *map-name* **rule** *rule-num* **call** *target*

delete policy route-map *map-name* **rule** *rule-num* **call**

show policy route-map *map-name* **rule** *rule-num*

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
    route-map text {  
        rule u32 {  
            call: text  
        }  
    }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
<i>target</i>	Mandatory. The identifier of the route map being called.

Default

None.

Usage Guidelines

Use the **set** form of this command to call to another route map.

The new route map is called after all **set** actions specified in the route map have been performed. If the called route map returns **permit**, then the matching and exit policies of the route map govern further behavior in the normal way. If the called route-map returns **deny**, processing of the route map completes and the route is denied, regardless of any further matching or exit policies.

Use the **delete** form of this command to remove this statement from the route map.

Use the **show** form of this command to display route map rule configuration settings.

policy route-map <map-name> rule <rule-num> continue <target-num>

Calls to another rule within the current route map.

Syntax

set policy route-map *map-name* **rule** *rule-num* **continue** *target-num*

delete policy route-map *map-name* **rule** *rule-num* **continue**

show policy route-map *map-name* **rule** *rule-num* **continue**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      continue: u32  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
<i>target</i>	Mandatory. The identifier of the route map rule being called.

Default

None.

Usage Guidelines

Use the **set** form of this command to call to another rule within the current route map. The new route map rule is called after all **set** actions specified in the route map rule have been performed.

Use the **delete** form of this command to remove this statement from the route map.

Use the **show** form of this command to display route map rule configuration settings.

policy route-map <map-name> rule <rule-num> description <desc>

Allows you to specify a brief description for a route map rule.

Syntax

```
set policy route-map map-name rule rule-num description desc  
delete policy route-map map-name rule rule-num description  
show policy route-map map-name rule rule-num description
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
    route-map text {  
        rule u32 {  
            description: text  
        }  
    }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
<i>desc</i>	Mandatory. A brief text description for the route map rule.

Default

None.

Usage Guidelines

- Use the **set** form of this command to create a description for a route map rule.
- Use the **delete** form of this command to remove a route map rule description.
- Use the **show** form of this command to display the description for a route map rule.

policy route-map <map-name> rule <rule-num> match as-path <list-name>

Defines a match condition for a route map based on an AS path list

Syntax

set policy route-map *map-name* **rule** *rule-num* **match as-path** *list-name*

delete policy route-map *map-name* **rule** *rule-num* **match as-path**

show policy route-map *map-name* **rule** *rule-num* **match as-path**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      match {  
        as-path: text  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
<i>list-name</i>	Mandatory. Matches the AS paths in the route with those permitted by the specified AS path list. The AS path list must already be defined.

Default

If no AS path match condition is specified, packets are not filtered by AS path.

Usage Guidelines

Use the **set** form of this command to define a match condition for a route map policy based on an AS path list.

Packets are matched based on whether the AS path listed in the route match the AS path defined by this command. Depending on the action defined for the rule using the **policy route-map <map-name> rule <rule-num> action** command (see page 47), matched

packets are either permitted or denied. Based on the forwarding information specified by the **set** statements in the route map rule, permitted packets are forwarded to their various destinations.

If more than one match condition is defined in a route map rule, the packet must match all conditions to count as a match. If no match condition is defined for the route map rule, all packets are considered to match the rule.

Use the **delete** form of this command to remove the AS path match condition.

Use the **show** form of this command to display AS path match condition configuration.

policy route-map <map-name> rule <rule-num> match community

Defines a match condition for a route map based on BGP communities.

Syntax

```
set policy route-map map-name rule rule-num match community { community-list  
list-num | exact-match }
```

```
delete policy route-map map-name rule rule-num match community
```

```
show policy route-map map-name rule rule-num match community
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      match {  
        community {  
          community-list: u32  
          exact-match  
        }  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
community-list <i>list-num</i>	Matches the BGP communities in the route with those permitted by the specified community list. The community list policy must already be defined. Either community-list or exact-match must be specified.
exact-match	BGP communities are to be matched exactly. Either community-list or exact-match must be specified.

Default

If no community list match condition is specified, packets are not filtered by BGP community.

Usage Guidelines

Use the **set** form of this command to define a match condition for a route map policy based on BGP communities.

Packets are matched based on whether the BGP communities listed in the route match the communities defined by this command. Depending on the action defined for the rule using the **policy route-map <map-name> rule <rule-num> action** command (see page 47), matched packets are either permitted or denied. Based on the forwarding information specified by the **set** statements in the route map rule, permitted packets are forwarded to their various destinations.

If more than one match condition is defined in a route map rule, the packet must match all conditions to count as a match. If no match condition is defined for the route map rule, all packets are considered to match the rule.

Use the **delete** form of this command to remove the BGP community match condition.

Use the **show** form of this command to display BGP community match condition configuration.

policy route-map <map-name> rule <rule-num> match interface <ethx>

Defines a match condition for a route map based on the first-hop interface.

Syntax

```
set policy route-map map-name rule rule-num match interface ethx  
delete policy route-map map-name rule rule-num match interface  
show policy route-map map-name rule rule-num match interface
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
    route-map text {  
        rule u32 {  
            match {  
                interface: text  
            }  
        }  
    }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
<i>ethx</i>	Mandatory. Matches first hop interface specified in the route against the interface name.

Default

If no interface match condition is specified, packets are not filtered by interface.

Usage Guidelines

Use the **set** form of this command to define a match condition for a route map policy based on first-hop interface.

Packets are matched based on whether the first-hop interface of the route matches the interface specified by this command. Depending on the action defined for the rule using the **policy route-map <map-name> rule <rule-num> action** command (see page 47), matched packets are either permitted or denied. Based on the forwarding information specified by the **set** statements in the route map rule, permitted packets are forwarded to their various destinations.

If more than one match condition is defined in a route map rule, the packet must match all conditions to count as a match. If no match condition is defined for the route map rule, all packets are considered to match the rule.

Use the **delete** form of this command to remove the interface match condition.

Use the **show** form of this command to display interface match condition configuration.

policy route-map <map-name> rule <rule-num> match ip address

Defines a match condition for a route map based on IP address.

Syntax

set policy route-map *map-name* **rule** *rule-num* **match ip address** {**access-list** *list-num* | **prefix-list** *list-name*}

delete policy route-map *map-name* **rule** *rule-num* **match ip address**

show policy route-map *map-name* **rule** *rule-num* **match ip address**

Command Mode

Configuration mode.

Configuration Statement

```
policy {
  route-map text {
    rule u32 {
      match {
        ip address {
          access-list: u32
          prefix-list: text
        }
      }
    }
  }
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
access-list <i>list-num</i>	Matches the source or destination IP address of the route against those permitted by the specified access list. The access list must already be defined. Either access-list or prefix-list must be specified.
prefix-list <i>list-name</i>	Matches the source or destination network of the route against those permitted by the specified prefix list. The prefix list must already be defined. Either access-list or prefix-list must be specified.

Default

If no IP address match condition is specified, packets are not filtered by IP address.

Usage Guidelines

Use the **set** form of this command to define a match condition for a route map policy based on IP address.

Packets are matched based on whether the source or destination IP address of the route matches an address contained in the specified access list or prefix list. Depending on the action defined for the rule using the **policy route-map <map-name> rule <rule-num> action** command (see page 47), matched packets are either permitted or denied. Based on the forwarding information specified by the **set** statements in the route map rule, permitted packets are forwarded to their various destinations.

If more than one match condition is defined in a route map rule, the packet must match all conditions to count as a match. If no match condition is defined for the route map rule, all packets are considered to match the rule.

Use the **delete** form of this command to remove the IP address match condition.

Use the **show** form of this command to display IP address match condition configuration.

policy route-map <map-name> rule <rule-num> match ip nexthop

Defines a match condition for a route map based on the next-hop address.

Syntax

```
set policy route-map map-name rule rule-num match ip nexthop {access-list list-num |  
prefix-list list-name}
```

```
delete policy route-map map-name rule rule-num match ip nexthop
```

```
show policy route-map map-name rule rule-num match ip nexthop
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      match {  
        ip {  
          nexthop {  
            access-list: u32  
            prefix-list: text  
          }  
        }  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
access-list <i>list-num</i>	Matches the next-hop IP address in the route against those permitted by the specified access list. The access list must already be defined. Either access-list or prefix-list must be specified.

prefix-list <i>list-name</i>	Matches next-hop IP address in the route against those permitted by the specified prefix list. The prefix list must already be defined. Either access-list or prefix-list must be specified.
-------------------------------------	--

Default

If no next-hop match condition is specified, packets are not filtered by next hop.

Usage Guidelines

Use the **set** form of this command to define a match condition for a route map policy based on next-hop IP address.

Packets are matched based on whether the next-hop IP address of the route matches an address contained in the specified access list or prefix list. Depending on the action defined for the rule using the **policy route-map <map-name> rule <rule-num> action** command (see page 47), matched packets are either permitted or denied. Based on the forwarding information specified by the **set** statements in the route map rule, permitted packets are forwarded to their various destinations.

If more than one match condition is defined in a route map rule, the packet must match all conditions to count as a match. If no match condition is defined for the route map rule, all packets are considered to match the rule.

Use the **delete** form of this command to remove the next-hop IP address match condition.

Use the **show** form of this command to display next-hop IP address match condition configuration.

policy route-map <map-name> rule <rule-num> match ip route-source

Defines a match condition for a route map based on the address from where a route is advertised.

Syntax

set policy route-map *map-name* **rule** *rule-num* **match ip route-source** { **access-list** *list-num* | **prefix-list** *list-name* }

delete policy route-map *map-name* **rule** *rule-num* **match ip route-source**

show policy route-map *map-name* **rule** *rule-num* **match ip route-source**

Command Mode

Configuration mode.

Configuration Statement

```
policy {
  route-map text {
    rule u32 {
      match {
        ip {
          route-source {
            access-list: u32
            prefix-list: text
          }
        }
      }
    }
  }
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
access-list <i>list-num</i>	Matches routes advertised from addresses contained in the specified access list. The access list must already be defined. Either access-list or prefix-list must be specified.
prefix-list <i>list-name</i>	Matches routes advertised from addresses contained in the specified prefix list. The prefix list must already be defined. Either access-list or prefix-list must be specified.

Default

If no route source match condition is specified, packets are not filtered by route source.

Usage Guidelines

Use the **set** form of this command to define a match condition for a route map policy based on the address from where routes are advertised (its route source).

Packets are matched based on whether the route source matches an address contained in the specified access list or prefix list. Depending on the action defined for the rule using the **policy route-map <map-name> rule <rule-num> action** command (see page 47), matched packets are either permitted or denied. Based on the forwarding information specified by the **set** statements in the route map rule, permitted packets are forwarded to their various destinations.

If more than one match condition is defined in a route map rule, the packet must match all conditions to count as a match. If no match condition is defined for the route map rule, all packets are considered to match the rule.

Use the **delete** form of this command to remove the route source match condition.

Use the **show** form of this command to display route source match condition configuration.

policy route-map <map-name> rule <rule-num> match metric <metric>

Defines a match condition for a route map based on the route's metric.

Syntax

set policy route-map *map-name* **rule** *rule-num* **match metric** *metric*

delete policy route-map *map-name* **rule** *rule-num* **match metric**

show policy route-map *map-name* **rule** *rule-num* **match metric**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      match {  
        metric: u32  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
<i>metric</i>	Mandatory. A number representing a route metric. This value is matched against the metric in the route.

Default

If no metric match condition is specified, packets are not filtered by metric.

Usage Guidelines

Use the **set** form of this command to define a match condition for a route map policy based route metric.

Packets are matched based on whether the route metric matches that specified by this command. Depending on the action defined for the rule using the **policy route-map <map-name> rule <rule-num> action** command (see page 47), matched packets are

either permitted or denied. Based on the forwarding information specified by the **set** statements in the route map rule, permitted packets are forwarded to their various destinations.

If more than one match condition is defined in a route map rule, the packet must match all conditions to count as a match. If no match condition is defined for the route map rule, all packets are considered to match the rule.

Use the **delete** form of this command to remove the route source match condition.

Use the **show** form of this command to display route source match condition configuration.

policy route-map <map-name> rule <rule-num> match origin

Defines a match condition for a route map based on the route's origin.

Syntax

set policy route-map *map-name* **rule** *rule-num* **match origin** { **egp** | **igp** | **incomplete** }

delete policy route-map *map-name* **rule** *rule-num* **match origin**

show policy route-map *map-name* **rule** *rule-num* **match origin**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      match {  
        origin {  
          origin-code: [egp|igp|incomplete]  
        }  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
egp:	Matches routes whose origin is an Exterior Gateway Protocol.
igp:	Matches routes whose origin is an Interior Gateway Protocol.
incomplete	Matches routes whose BGP origin code is incomplete.

Default

If no origin match condition is specified, packets are not filtered by BGP origin code.

Usage Guidelines

Use the **set** form of this command to define a match condition for a route map policy based BGP origin.

Packets are matched based on whether the BGP origin code in the route matches that specified by this command. Depending on the action defined for the rule using the **policy route-map <map-name> rule <rule-num> action** command (see page 47), matched packets are either permitted or denied. Based on the forwarding information specified by the **set** statements in the route map rule, permitted packets are forwarded to their various destinations.

If more than one match condition is defined in a route map rule, the packet must match all conditions to count as a match. If no match condition is defined for the route map rule, all packets are considered to match the rule.

Use the **delete** form of this command to remove the origin match condition.

Use the **show** form of this command to display origin match condition configuration.

policy route-map <map-name> rule <rule-num> match peer <ipv4>

Defines a match condition for a route map based on peer IP address.

Syntax

set policy route-map *map-name* **rule** *rule-num* **match peer** *ipv4*

delete policy route-map *map-name* **rule** *rule-num* **match peer**

show policy route-map *map-name* **rule** *rule-num* **match peer**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      match {  
        peer: ipv4  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
<i>ipv4</i>	Mandatory. An IPv4 address. This address is matched against the peer address in the route.

Default

If no peer address match condition is specified, packets are not filtered by peer IP address.

Usage Guidelines

Use the **set** form of this command to define a match condition for a route map policy based peer IP address.

Packets are matched based on whether the address of the peer in the route matches that specified by this command. Depending on the action defined for the rule using the **policy route-map <map-name> rule <rule-num> action** command (see page 47), matched

packets are either permitted or denied. Based on the forwarding information specified by the **set** statements in the route map rule, permitted packets are forwarded to their various destinations.

If more than one match condition is defined in a route map rule, the packet must match all conditions to count as a match. If no match condition is defined for the route map rule, all packets are considered to match the rule.

Use the **delete** form of this command to remove the peer address match condition.

Use the **show** form of this command to display peer address match condition configuration.

policy route-map <map-name> rule <rule-num> match tag <tag>

Defines a match condition for a route map based on OSPF tag.

Syntax

set policy route-map *map-name* **rule** *rule-num* **match tag** *tag*

delete policy route-map *map-name* **rule** *rule-num* **match tag**

show policy route-map *map-name* **rule** *rule-num* **match tag**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      match {  
        tag: u32  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
<i>tag</i>	Mandatory. A 32-bit value representing an OSPF tag. This value is matched against the contents of the OSPF external Link-State Advertisement (LSA) 32-bit tag field in the route.

Default

If no tag match condition is specified, packets are not filtered by tag.

Usage Guidelines

Use the **set** form of this command to define a match condition for a route map policy based on OSPF tag.

Packets are matched based on whether the value of the OSPF external LSA 32-bit tag field in the route matches that specified by this command. Depending on the action defined for the rule using the **policy route-map <map-name> rule <rule-num> action** command (see

page 47), matched packets are either permitted or denied. Based on the forwarding information specified by the **set** statements in the route map rule, permitted packets are forwarded to their various destinations.

If more than one match condition is defined in a route map rule, the packet must match all conditions to count as a match. If no match condition is defined for the route map rule, all packets are considered to match the rule.

Use the **delete** form of this command to remove the OSPF tag match condition.

Use the **show** form of this command to display OSPF tag match condition configuration.

policy route-map <map-name> rule <rule-num> on-match

Specifies an alternative exit policy for a route map.

Syntax

set policy route-map *map-name* **rule** *rule-num* **on-match** {**goto** *rule-num* | **next**}

delete policy route-map *map-name* **rule** *rule-num* **on-match**

show policy route-map *map-name* **rule** *rule-num* **on-match**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      on-match {  
        goto: u32  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
goto <i>rule-num</i>	The number of a defined route map rule. When all matches listed in the route map rule succeed, the current route map rule is exited and this rule is invoked and executed. Note that jumping to a previous route map rule is not permitted.
next	When all matches listed in the route map rule succeed, the current route map rule is exited and the next rule in the sequence is invoked and executed.

Default

None.

Usage Guidelines

Use the **set** form of this command to define an exit policy for a route map entry, by specifying the route map rule to be executed when a match occurs. When all the match conditions specified by the route map rule succeed, the route map rule specified by this command is invoked and executed.

Normally, when a route map is matched, the route map is exited and the route is permitted. This command allows you to specify an alternative exit policy, by directing execution to a specified route map rule or to the next rule in the sequence.

Use the **delete** form of this command to remove the exit policy.

Use the **show** form of this command to display route map exit policy configuration.

policy route-map <map-name> rule <rule-num> set aggregator

Modifies the BGP aggregator attribute of a route.

Syntax

set policy route-map *map-name* **rule** *rule-num* **set aggregator** {**as** *asn* / **ip** *ipv4*}

delete policy route-map *map-name* **rule** *rule-num* **set aggregator**

show policy route-map *map-name* **rule** *rule-num* **set**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      set {  
        aggregator {  
          as: 1-65535  
          ip: ipv4  
        }  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
as <i>asn</i>	Modifies the autonomous system number of the BGP aggregator in the route to the specified value. The range is 1 to 65535.
ip <i>ipv4</i>	Modifies the IP address of the BGP aggregator in the route to the specified IPv4 address.

Default

None.

Usage Guidelines

Use the **set** form of this command to modify the aggregator attribute of a route. When all the match conditions in the route map rule succeed, the aggregator attribute is modified as specified.

Use the **delete** form of this command to delete this statement from the route map rule.

Use the **show** form of this command to display **set** statement configuration for route maps.

policy route-map <map-name> rule <rule-num> set as-path-prepend <prepend>

Sets or prepends to the AS path of the route.

Syntax

set policy route-map *map-name* **rule** *rule-num* **set as-path-prepend** *prepend*

delete policy route-map *map-name* **rule** *rule-num* **set as-path-prepend**

show policy route-map *map-name* **rule** *rule-num* **set**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      set {  
        as-path-prepend: text  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
<i>prepend</i>	Mandatory. A string representing an AS path.

Default

None.

Usage Guidelines

Use the **set** form of this command to prepend a string to the AS path list in a route. When all the match conditions in the route map rule succeed, the specified string is prepended to the AS path in the route.

Use the **delete** form of this command to delete this statement from the route map rule.

Use the **show** form of this command to display **set** statement configuration for route maps.

policy route-map <map-name> rule <rule-num> set atomic-aggregate

Sets the BGP atomic-aggregate attribute in a route.

Syntax

```
set policy route-map map-name rule rule-num set atomic-aggregate
delete policy route-map map-name rule rule-num set atomic-aggregate
show policy route-map map-name rule rule-num set
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {
  route-map text {
    rule u32 {
      set {
        atomic-aggregate
      }
    }
  }
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.

Default

None.

Usage Guidelines

Use the **set** form of this command to set the BGP atomic aggregate attribute in a route. When all the match conditions in the route map rule succeed, the BGP atomic aggregate attribute is modified as specified.

Use the **delete** form of this command to delete this statement from the route map rule.

Use the **show** form of this command to display **set** statement configuration for route maps.

policy route-map <map-name> rule <rule-num> set comm-list

Modifies the BGP community list in a route.

Syntax

```
set policy route-map map-name rule rule-num set comm-list {comm-list list-name /  
delete}
```

```
delete policy route-map map-name rule rule-num set comm-list
```

```
show policy route-map map-name rule rule-num set
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      set {  
        comm-list {  
          comm-list: text  
          delete  
        }  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
comm-list <i>list-name</i>	Removes the communities in the specified community list from the route's community list. The community list must already be defined.
delete	Deletes the route's entire community list.

Default

None.

Usage Guidelines

Use the **set** form of this command to modify the BGP community list in a route. When all the match conditions in the route map rule succeed, the community list is modified as specified.

Use the **delete** form of this command to delete this statement from the route map rule.

Use the **show** form of this command to display **set** statement configuration for route maps.

policy route-map <map-name> rule <rule-num> set community

Modifies the BGP communities attribute in a route.

Syntax

```
set policy route-map map-name rule rule-num set community {community [additive] | none}
```

```
delete policy route-map map-name rule rule-num set community
```

```
show policy route-map map-name rule rule-num set
```

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      set {  
        community: text  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
<i>community</i>	A BGP community. Supported values are a community number in <i>aa:nn</i> format, or the well-known BGP communities local-AS , no-export , no-advertise , or internet .
additive	Appends the specified community to the existing communities in the route.

Default

When the **additive** keyword is not used, the specified community replaces the existing communities in the route.

Usage Guidelines

Use the **set** form of this command to modify the BGP communities attribute in a route. When all the match conditions in the route map rule succeed, the communities attribute is modified as specified.

Use the **delete** form of this command to delete this statement from the route map rule.

Use the **show** form of this command to display **set** statement configuration for route maps.

policy route-map <map-name> rule <rule-num> set ip-next-hop <ipv4>

Modifies the next hop destination of a route.

Syntax

set policy route-map *map-name* **rule** *rule-num* **set ip-next-hop** *ipv4*

delete policy route-map *map-name* **rule** *rule-num* **set ip-next-hop**

show policy route-map *map-name* **rule** *rule-num* **set**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      set {  
        ip-next-hop: ipv4  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
ip-next-hop <i>ipv4</i>	Mandatory. The IPv4 address of the next hop.

Default

None.

Usage Guidelines

Use the **set** form of this command to modify the next hop destination for packets that traverse a route map. When all the match conditions in the route map rule succeed, the next hop of the route is modified as specified.

Use the **delete** form of this command to delete this statement from the route map rule.

Use the **show** form of this command to display **set** statement configuration for route maps.

policy route-map <map-name> rule <rule-num> set local-preference <local-pref>

Modifies the BGP local-pref attribute in a route.

Syntax

set policy route-map *map-name* **rule** *rule-num* **set** local-preference *local-pref*

delete policy route-map *map-name* **rule** *rule-num* **set** local-preference

show policy route-map *map-name* **rule** *rule-num* **set**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      set {  
        local-preference: u32  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
<i>local-pref</i>	Mandatory. The new value for the BGP local preference path attribute.

Default

None.

Usage Guidelines

Use the **set** form of this command to modify the BGP local-pref attribute for packets that traverse a route map. When all the match conditions in the route map rule succeed, the local-pref attribute of the route is modified as specified.

Use the **delete** form of this command to delete this statement from the route map rule.

Use the **show** form of this command to display **set** statement configuration for route maps.

policy route-map <map-name> rule <rule-num> set metric <metric>

Modifies the metric of a route.

Syntax

set policy route-map *map-name* **rule** *rule-num* **set** metric *metric*

delete policy route-map *map-name* **rule** *rule-num* **set** metric

show policy route-map *map-name* **rule** *rule-num* **set**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      set {  
        metric: text  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
<i>metric</i>	Mandatory. A number representing the new metric to be used in the route.

Default

None.

Usage Guidelines

Use the **set** form of this command to modify the route metric for packets that traverse a route map. When all the match conditions in the route map rule succeed, the route metric is modified as specified.

Use the **delete** form of this command to delete this statement from the route map rule.

Use the **show** form of this command to display **set** statement configuration for route maps.

policy route-map <map-name> rule <rule-num> set metric-type <type>

Specifies the OSPF external metric-type for a route.

Syntax

set policy route-map *map-name* **rule** *rule-num* **set metric-type** *type*

delete policy route-map *map-name* **rule** *rule-num* **set metric-type**

show policy route-map *map-name* **rule** *rule-num* **set**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      set {  
        metric-type: [type-1|type-2]  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
type-1	OSPF external type 1 metric. This metric uses both internal and external costs when calculating the cost to access an external network.
type-2	OSPF external type 2 metric. This metric uses only external cost when calculating the cost to access an external network.

Default

None.

Usage Guidelines

Use this command to specify the metric OSPF should use to calculate the cost of accessing an external network.

Use the **set** form of this command to specify the OSPF external metric type for a route.

Use the **delete** form of this command to delete the metric type.

Use the **show** form of this command to display the metric type.

policy route-map <map-name> rule <rule-num> set origin

Modifies the BGP origin code of a route.

Syntax

set policy route-map *map-name* **rule** *rule-num* **set origin** {*asn* | **egp** | **igp** | **incomplete**}

delete policy route-map *map-name* **rule** *rule-num* **set origin**

show policy route-map *map-name* **rule** *rule-num* **set**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      set {  
        origin [egp|igp|incomplete]  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
<i>asn</i>	An autonomous system number. The range is 1 to 65535.
egp	Sets the BGP origin code to egp (Exterior Gateway Protocol).
igp	Sets the BGP origin code to igp (Interior Gateway Protocol).
incomplete	Sets the BGP origin code to incomplete .

Default

None.

Usage Guidelines

Use the **set** form of this command to set the BGP origin code for packets that traverse a route map. When all the match conditions in the route map rule succeed, the BGP origin code is modified as specified.

Use the **delete** form of this command to delete this statement from the route map rule.

Use the **show** form of this command to display **set** statement configuration for route maps.

policy route-map <map-name> rule <rule-num> set originator-id <ipv4>

Modifies the BGP originator ID attribute of a route.

Syntax

set policy route-map *map-name* **rule** *rule-num* **set** originator-id *ipv4*

delete policy route-map *map-name* **rule** *rule-num* **set** originator-id

show policy route-map *map-name* **rule** *rule-num* **set**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      set {  
        originator-id: ipv4  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
<i>ipv4</i>	Mandatory. The IPv4 address to be used as the new originator ID.

Default

None.

Usage Guidelines

Use the **set** form of this command to set the BGP originator ID for packets that traverse a route map. When all the match conditions in the route map rule succeed, the BGP originator ID is modified as specified.

Use the **delete** form of this command to delete this statement from the route map rule.

Use the **show** form of this command to display **set** statement configuration for route maps.

policy route-map <map-name> rule <rule-num> set tag <tag>

Modifies the OSPF tag value of a route.

Syntax

set policy route-map *map-name* **rule** *rule-num* **set tag** *tag*

delete policy route-map *map-name* **rule** *rule-num* **set tag**

show policy route-map *map-name* **rule** *rule-num* **set**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      set {  
        tag: u32  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
<i>tag</i>	Mandatory. A 32-bit number representing the new value of the OSPF external Link-State Advertisement (LSA) tag field.

Default

None.

Usage Guidelines

Use the **set** form of this command to set the OSPF tag value for packets that traverse a route map. When all the match conditions in the route map rule succeed, the route tag is modified as specified.

Use the **delete** form of this command to delete this statement from the route map rule.

Use the **show** form of this command to display **set** statement configuration for route maps.

policy route-map <map-name> rule <rule-num> set weight <weight>

Modifies the BGP weight of a route.

Syntax

set policy route-map *map-name* **rule** *rule-num* **set weight** *weight*

delete policy route-map *map-name* **rule** *rule-num* **set weight**

show policy route-map *map-name* **rule** *rule-num* **set**

Command Mode

Configuration mode.

Configuration Statement

```
policy {  
  route-map text {  
    rule u32 {  
      set {  
        weight: u32  
      }  
    }  
  }  
}
```

Parameters

<i>map-name</i>	Mandatory. The name of a defined route map.
<i>rule-num</i>	Mandatory. The number of a defined route map rule.
<i>weight</i>	Mandatory. The BGP weight to be recorded in the routing table. The range is 0 to 65535.

Default

None.

Usage Guidelines

Use the **set** form of this command to set the BGP weight for routes. When all the match conditions in the route map rule succeed, the route weight is modified as specified.

Use the **delete** form of this command to delete this statement from the route map rule.

Use the **show** form of this command to display **set** statement configuration for route maps.

show ip access-list

Displays all IP access lists.

Syntax

show ip access-list

Command Mode

Operational mode.

Parameters

None.

Default

None.

Usage Guidelines

Use this command to display IP access lists.

Examples

Example 1-1 shows IP access lists.

Example 1-1 “show ip access-list”: Displaying IP access lists

```
vyatta@vyatta:~$ show ip access-list
ZEBRA:
Standard IP access list 1
    permit any
RIP:
Standard IP access list 1
    permit any
OSPF:
Standard IP access list 1
    permit any
BGP:
Standard IP access list 1
    permit any
vyatta@vyatta:~$
```

show ip as-path-access-list

Displays all as-path access lists.

Syntax

show ip as-path-access-list

Command Mode

Operational mode.

Parameters

None.

Default

None.

Usage Guidelines

Use this command to display as-path access lists.

Examples

Example 1-2 shows as-path access lists.

Example 1-2 “show ip as-path-access-list”: Displaying as-path access lists

```
vyatta@vyatta:~$ show ip as-path-access-list
AS path access list IN
    permit 50:1
vyatta@vyatta:~$
```

show ip community-list

Displays all IP community lists.

Syntax

show ip community-list

Command Mode

Operational mode.

Parameters

None.

Default

None.

Usage Guidelines

Use this command to display community lists.

Examples

Example 1-3 shows community lists.

Example 1-3 “show ip community-list”: Displaying community lists

```
vyatta@vyatta:~$ show ip community-list
Community (expanded) access list 101
    permit AB*
vyatta@vyatta:~$
```

show ip extcommunity-list

Displays all extended IP community lists.

Syntax

show ip extcommunity-list

Command Mode

Operational mode.

Parameters

None.

Default

None.

Usage Guidelines

Use this command to display extended IP community lists.

Examples

Example 1-4 shows extended IP community lists.

Example 1-4 “show ip extcommunity-list”: Displaying extended IP community lists

```
vyatta@vyatta:~$ show ip extcommunity-list
Community (expanded) access list 101
    permit AB*
vyatta@vyatta:~$
```

show ip prefix-list

Displays IP prefix lists.

Syntax

```
show ip prefix-list [detail | summary | list-name [seq seq-num / ipv4net [first-match | longer]]]
```

Command Mode

Operational mode.

Parameters

detail	Displays detailed information for all IP prefix lists.
summary	Displays summary information for all IP prefix lists.
<i>list-name</i>	Displays information about the named IP prefix list.
<i>seq-num</i>	Displays the specified sequence from the named IP prefix list.
<i>ipv4net</i>	Displays the select prefix of the named IP prefix list.
first-match	Displays the first match from the select prefix of the named IP prefix list.
longer	Displays the longer match of the select prefix from the named IP prefix list

Default

None.

Usage Guidelines

Use this command to display prefix lists.

Examples

Example 1-5 shows prefix lists.

Example 1-5 “show ip prefix-list”: Displaying prefix lists

```
vyatta@vyatta:~$ show ip prefix-list
ZEBRA: ip prefix-list ABC: 1 entries
```

```
seq 1 permit 192.168.2.0/24 ge 25
RIP: ip prefix-list ABC: 1 entries
seq 1 permit 192.168.2.0/24 ge 25
OSPF: ip prefix-list ABC: 1 entries
seq 1 permit 192.168.2.0/24 ge 25
BGP: ip prefix-list ABC: 1 entries
seq 1 permit 192.168.2.0/24 ge 25
vyatta@vyatta:~$
```

show ip protocol

Displays IP route maps per protocol.

Syntax

show ip protocol

Command Mode

Operational mode.

Parameters

None.

Default

None.

Usage Guidelines

Use this command to display IP route maps per protocol.

Examples

Example 1-6 shows IP route maps by protocol.

Example 1-6 “show ip protocol”: Displaying IP route maps by protocol

```
vyatta@vyatta:~$ show ip protocol
Protocol      : route-map
-----
system       : none
kernel       : none
connected    : none
static       : none
rip          : none
ripng        : none
ospf         : none
ospf6        : none
isis         : none
bgp          : none
hsls         : none
any          : none
vyatta@vyatta:~$
```

show route-map

Displays route map information.

Syntax

show route-map [map-name]

Command Mode

Operational mode.

Parameters

None.

Default

None.

Usage Guidelines

Use this command to display route map information.

Examples

Example 1-7 shows route map information.

Example 1-7 “show route-map”: Displaying route map information

```
vyatta@vyatta:~$ show route-map
ZEBRA:
route-map MAP1, permit, sequence 1
  Match clauses:
  Set clauses:
  Call clause:
  Action:
    Exit routemap
RIP:
route-map MAP1, permit, sequence 1
  Match clauses:
    interface eth0
  Set clauses:
  Call clause:
  Action:
    Exit routemap
```

```
OSPF:
route-map MAP1, permit, sequence 1
  Match clauses:
    interface eth0
  Set clauses:
  Call clause:
  Action:
    Exit routemap
BGP:
route-map MAP1, permit, sequence 1
  Match clauses:
  Set clauses:
  Call clause:
  Action:
    Exit routemap
vyatta@vyatta:~$
```

Chapter 2: Quality of Service

This chapter describes commands for implementing quality of service (QoS) on the Vyatta system.

This chapter presents the following topics:

- QoS Configuration
- QoS Commands

QoS Configuration

This section presents the following topics:

- QoS Overview
- QoS Mechanisms
- QoS Configuration Example

QoS Overview

By default, all traffic sent out by the Vyatta system is prioritized based on its Type of Service (ToS) field into one of three priority queues. The packets on the highest priority queue are sent out first, followed by those on the next-highest priority queue, followed by those on the lowest priority queue. Within each queue, all packets are sent on a First In First Out (FIFO) basis and receive “best effort” delivery. If traffic arrives on a queue faster than it can be delivered (for example, because of bandwidth limitations) it is buffered within the system. If more data arrives than the system can buffer, the excess is dropped.

Data traffic is divided in this way because providing equal levels of service for all traffic is not always desirable. Some types of traffic, by their nature, should be treated differently than others. For example, voice traffic is very sensitive to delay and, if it is not processed accordingly, may be unintelligible. Data, on the other hand, is sensitive not to delay but to corruption.

Quality of service (QoS) is a feature that enables network administrators to identify different traffic flows and then treat them according to their individual requirements, rather than simply using the default mechanism.

The general workflow for quality of service is as follows:

- 1 Create a QoS policy is created that identifies traffic flows and specifies how each flow is to be treated.
- 2 Apply the policy to an interface.

QoS Mechanisms

In addition to the default queuing mechanism described above, the Vyatta system provides a variety of QoS mechanisms for identifying and treating the various traffic flows that pass through an interface. Some of these apply only to inbound traffic and some apply only to outbound traffic.

Drop Tail

The **drop tail** mechanism applies only to outbound traffic. It provides pure FIFO (First In First Out) queuing. In other words, data packets are transmitted in the same order that they arrive. If the queue fills up, then the “tail” (i.e. packets that are just arriving in the queue) is dropped. With drop-tail queuing, there is a single queue and all traffic is treated equally. In other words, there is no prioritization of traffic as is true in the default case.

Fair Queue

The **fair queue** mechanism applies only to outbound traffic. It provides queuing based on the Stochastic Fairness Queuing algorithm. In this algorithm traffic flows (identified by IP protocol, source address, and/or destination address) receive fair access to network resources. In other words, no one flow can use the majority of the bandwidth.

Rate Limiting

The **rate limit** mechanism applies only to outbound traffic. It provides queuing based on the Token Bucket Filter algorithm. This algorithm only passes packets arriving at a rate which does not exceed an administratively set rate. It is possible, however, for short bursts of traffic to occur in excess of this rate.

Traffic Shaping

The **traffic shaper** mechanism applies only to outbound traffic. It provides queuing based on the Token Bucket shaping algorithm. This algorithm allows for bursting if a “bucket” has tokens to “spend”.

Traffic Limiting

The **traffic limiter** mechanism applies only to inbound traffic. Each flow is assigned a bandwidth limit. All traffic within a flow that arrives in excess of the bandwidth limit is dropped. This mechanism can be used to throttle incoming traffic.

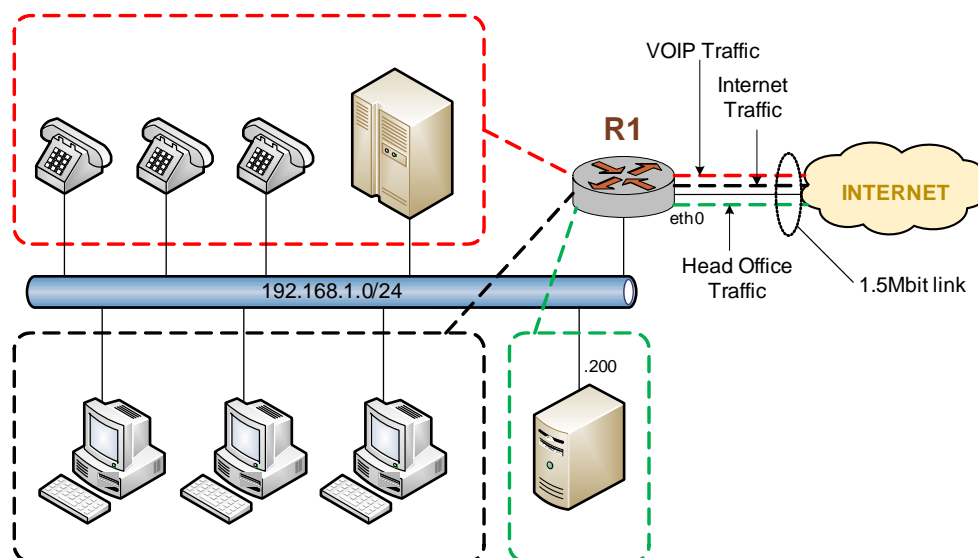
QoS Configuration Example

Figure 2-1 shows a simple site using QoS on the Vyatta system (R1) to treat three distinct traffic flows in different ways. This scenario represents a single branch office with a Voice over IP (VoIP) phone system, users that connect to the Internet, and a server that requires a relatively high-speed connection to head office. In this example:

- All traffic flows through a 1.5 Mbit link to the Internet Service Provider (ISP).

- A minimum 50% of this bandwidth is to be set aside for the VoIP traffic, 35% for the head office traffic, and 15% for all other traffic.
 - In addition, the VoIP traffic is to be categorized into two distinct flows:
 - 5% of bandwidth is to be used for control (that is, SIP traffic for setting up calls).
 - 45% of bandwidth is to be used for data (that is, RTP media).
- The different flows are identified by their Differentiated Services Code Point (DSCP) values: SIP traffic is assigned a DSCP value of 26 and RTP traffic is assigned a DSCP value of 46.)
- The head office traffic arrives from a single server at IP address 192.168.1.200.

Figure 2-1 Example site using QoS



To configure this scenario, perform the following steps in configuration mode.

Example 2-1 QoS example

Step	Command
Create the configuration node for the QoS policy.	<pre>vyatta@R1# set qos-policy traffic-shaper OFFICE [edit]</pre>
Add a description.	<pre>vyatta@R1# set qos-policy traffic-shaper OFFICE description "QoS policy for office WAN" [edit]</pre>
Set the overall link bandwidth.	<pre>vyatta@R1# set qos-policy traffic-shaper OFFICE bandwidth 1500kbit [edit]</pre>

Example 2-1 QoS example

Add a description for the first traffic class - VOIP data traffic.	vyatta@R1# set qos-policy traffic-shaper OFFICE class 10 description "VOIP - RTP traffic" [edit]
Assign bandwidth to the VOIP data traffic.	vyatta@R1# set qos-policy traffic-shaper OFFICE class 10 bandwidth 45% [edit]
Identify the VOIP data traffic (DSCP=46).	vyatta@R1# set qos-policy traffic-shaper OFFICE class 10 match VOIP-RTP ip dscp 46 [edit]
Add a description for the second traffic class - VOIP control traffic.	vyatta@R1# set qos-policy traffic-shaper OFFICE class 20 description "VOIP -SIP traffic" [edit]
Assign bandwidth to the VOIP control traffic.	vyatta@R1# set qos-policy traffic-shaper OFFICE class 20 bandwidth 5% [edit]
Identify the VOIP control traffic (DSCP=26).	vyatta@R1# set qos-policy traffic-shaper OFFICE class 20 match VOIP-SIP ip dscp 26 [edit]
Add a description for the third traffic class - head office traffic.	vyatta@R1# set qos-policy traffic-shaper OFFICE class 30 description "Head office traffic" [edit]
Assign bandwidth to the head office traffic.	vyatta@R1# set qos-policy traffic-shaper OFFICE class 30 bandwidth 35% [edit]
Identify the head office traffic (IP address=192.168.1.200/24).	vyatta@R1# set qos-policy traffic-shaper OFFICE class 30 match HO-TRAFFIC ip source address 192.168.1.200/24 [edit]
Assign bandwidth to the remainder of the traffic.	vyatta@R1# set qos-policy traffic-shaper OFFICE default bandwidth 15% [edit]
Commit the change.	vyatta@R1# commit [edit]

Example 2-1 QoS example

Show the qos-policy configuration.

```
vyatta@R1# show qos-policy
traffic-shaper OFFICE {
    bandwidth 1500kbit
    class 10 {
        bandwidth 45%
        description "VOIP - RTP traffic"
        match VOIP-RTP {
            ip {
                dscp 46
            }
        }
    }
    class 20 {
        bandwidth 5%
        description "VOIP - SIP traffic"
        match VOIP-SIP {
            ip {
                dscp 26
            }
        }
    }
    class 30 {
        bandwidth 35%
        description "Head office traffic"
        match HO-TRAFFIC {
            ip {
                source {
                    address 192.168.1.200/24
                }
            }
        }
    }
    default {
        bandwidth 15%
    }
    description "QoS policy for office WAN"
}
[edit]
```

Assign the QoS policy to the WAN interface.

```
vyatta@R1# set interfaces ethernet eth0 qos-policy out
OFFICE
[edit]
```

QoS Commands

This chapter contains the following commands.

Configuration Commands	
Applying QoS Policies to Interfaces	
interfaces adsl <adslx> pvc <pvc-id> bridged-ethernet qos-policy out <policy-name>	Applies an outbound QoS policy to a PVC with RFC 1483 Bridged Ethernet encapsulation on an ADSL interface.
interfaces adsl <adslx> pvc <pvc-id> classical-ipoa qos-policy out <policy-name>	Applies an outbound QoS policy to a PVC with RFC 1577 Classical IPOA encapsulation on an ADSL interface.
interfaces adsl <adslx> pvc <pvc-id> pppoa <num> qos-policy out <policy-name>	Applies an outbound QoS policy to a PVC with PPPoA encapsulation on an ADSL interface.
interfaces adsl <adslx> pvc <pvc-id> pppoe <num> qos-policy out <policy-name>	Applies an outbound QoS policy to a PVC with PPPoE encapsulation on an ADSL interface.
interfaces bonding <bondx> qos-policy out <policy-name>	Applies an outbound QoS policy to an Ethernet link bonding interface.
interfaces ethernet <ethx> pppoe <num> qos-policy out <policy-name>	Applies an outbound QoS policy to a PVC with PPPoE encapsulation on an Ethernet interface.
interfaces ethernet <ethx> qos-policy	Applies QoS policy to the specified Ethernet interface.
interfaces ethernet <ethx> vif <vlan-id> qos-policy out <policy-name>	Applies an outbound QoS policy to the specified virtual interface.
interfaces serial <wanx> qos-policy	Applies QoS policy to the specified Serial interface.
Drop Tail Policies	
qos-policy drop-tail <policy-name>	Defines a drop tail (pure FIFO) QoS policy.
qos-policy drop-tail <policy-name> queue-limit <limit>	Sets an upper bound for the number of packets allowed in the queue for a drop queue policy.
Fair Queue Policies	
qos-policy fair-queue <policy-name>	Defines a fair queue QoS policy.
qos-policy fair-queue <policy-name> description <desc>	Sets a description for a fair queue policy.
qos-policy fair-queue <policy-name> hash-interval <seconds>	Specifies the interval between flow hash function updates for a fair queue policy.

qos-policy fair-queue <policy-name> queue-limit <limit>	Sets an upper bound for the number of packets allowed in the queue for a fair queue policy.
Rate Limit Policies	
qos-policy rate-limit <policy-name>	Defines a rate limiting QoS policy.
qos-policy rate-limit <policy-name> bandwidth	Specifies the bandwidth limit for all combined traffic constrained by this policy.
qos-policy rate-limit <policy-name> burst	Sets the burst size for a rate limiting QoS policy.
qos-policy rate-limit <policy-name> description <desc>	Sets a description for a rate limiting policy.
qos-policy rate-limit <policy-name> latency	Sets the limit on queue size based on latency for a rate limiting QoS policy.
Traffic Limiter Policies	
qos-policy traffic-limiter <policy-name>	Defines a traffic limiting QoS policy.
qos-policy traffic-limiter <policy-name> description <desc>	Specifies a description for a traffic limiter QoS policy.
Traffic Limiter Policy Classes	
qos-policy traffic-limiter <policy-name> class <class>	Defines a traffic class for a traffic limiter QoS policy.
qos-policy traffic-limiter <policy-name> class <class> bandwidth	Specifies the bandwidth rate cap for a traffic class.
qos-policy traffic-limiter <policy-name> class <class> description <desc>	Sets a description for a traffic class.
qos-policy traffic-limiter <policy-name> class <class> match <match-name>	Defines a traffic class matching rule.
qos-policy traffic-limiter <policy-name> class <class> match <match-name> description <desc>	Sets a description for a match rule.
qos-policy traffic-limiter <policy-name> class <class> match <match-name> ip destination	Specifies a match criterion based on IP destination information.
qos-policy traffic-limiter <policy-name> class <class> match <match-name> ip dscp <value>	Specifies a match criterion based on the value of the DSCP field.
qos-policy traffic-limiter <policy-name> class <class> match <match-name> ip protocol <proto>	Specifies a match criterion based on the IP protocol.
qos-policy traffic-limiter <policy-name> class <class> match <match-name> ip source	Specifies a match criterion based on source IP information.
qos-policy traffic-limiter <policy-name> class <class> match <match-name> vif <vlan-id>	Specifies a match criterion based on VLAN ID.

qos-policy traffic-limiter <policy-name> class <class> priority <priority>	Specifies the priority of a traffic class for allocation of extra bandwidth.
Traffic Shaper Policies	
qos-policy traffic-shaper <policy-name>	Defines a traffic shaping QoS policy.
qos-policy traffic-shaper <policy-name> bandwidth	Specifies the bandwidth available for all combined traffic constrained by this policy.
qos-policy traffic-shaper <policy-name> description <desc>	Specifies a description for a traffic shaper QoS policy.
Traffic Shaper Policy Classes	
qos-policy traffic-shaper <policy-name> class <class>	Defines a traffic class for a traffic shaper QoS policy.
qos-policy traffic-shaper <policy-name> class <class> bandwidth	Specifies the base guaranteed bandwidth rate for a traffic class.
qos-policy traffic-shaper <policy-name> class <class> burst	Sets the burst size for a traffic class.
qos-policy traffic-shaper <policy-name> class <class> ceiling	Sets a bandwidth ceiling for a traffic class.
qos-policy traffic-shaper <policy-name> class <class> description <desc>	Sets a description for a traffic class.
qos-policy traffic-shaper <policy-name> class <class> match <match-name>	Defines a traffic class matching rule.
qos-policy traffic-shaper <policy-name> class <class> match <match-name> description <desc>	Sets a description for a match rule.
qos-policy traffic-shaper <policy-name> class <class> match <match-name> interface <interface>	Specifies a match criterion based on incoming interface.
qos-policy traffic-shaper <policy-name> class <class> match <match-name> ip destination	Specifies a match criterion based on IP destination information.
qos-policy traffic-shaper <policy-name> class <class> match <match-name> ip dscp <value>	Specifies a match criterion based on the value of the DSCP field.
qos-policy traffic-shaper <policy-name> class <class> match <match-name> ip protocol <proto>	Specifies a match criterion based on the IP protocol.
qos-policy traffic-shaper <policy-name> class <class> match <match-name> ip source	Specifies a match criterion based on source IP information.
qos-policy traffic-shaper <policy-name> class <class> match <match-name> vif <vlan-id>	Specifies a match criterion based on VLAN ID.
qos-policy traffic-shaper <policy-name> class <class> priority <priority>	Specifies the priority of a traffic class for allocation of extra bandwidth.

qos-policy traffic-shaper <policy-name> class <class> queue-limit <limit>	Specifies the maximum queue size for a traffic class.
qos-policy traffic-shaper <policy-name> class <class> queue-type <type>	Specifies the type of queuing to use for a traffic class.
qos-policy traffic-shaper <policy-name> class <class> set-dscp <value>	Rewrites the DSCP field in packets in this traffic class to the specified value.
Traffic Shaper Policy Default Class	
qos-policy traffic-shaper <policy-name> default	Defines a default traffic shaper QoS policy.
qos-policy traffic-shaper <policy-name> default bandwidth	Specifies the base guaranteed bandwidth rate for the default traffic class.
qos-policy traffic-shaper <policy-name> default burst	Sets the burst size for the default traffic class.
qos-policy traffic-shaper <policy-name> default ceiling	Sets a bandwidth ceiling for the default traffic class.
qos-policy traffic-shaper <policy-name> default priority <priority>	Specifies the priority of the default traffic class for allocation of extra bandwidth.
qos-policy traffic-shaper <policy-name> default queue-limit <limit>	Specifies the maximum queue size for the default traffic class.
qos-policy traffic-shaper <policy-name> default queue-type <type>	Specifies the type of queuing to use for the default traffic class.
qos-policy traffic-shaper <policy-name> default set-dscp <value>	Rewrites the DSCP field in packets in the default traffic class to the specified value.
Operational Commands	
show queueing	Displays current QoS policies.

interfaces adsl <adslx> pvc <pvc-id> bridged-ethernet qos-policy out <policy-name>

Applies an outbound QoS policy to a PVC with RFC 1483 Bridged Ethernet encapsulation on an ADSL interface.

Syntax

set interfaces adsl *adslx* **pvc** *pvc-id* **bridged-ethernet qos-policy out** *policy-name*

delete interfaces adsl *adslx* **pvc** *pvc-id* **bridged-ethernet qos-policy out**

show interfaces adsl *adslx* **pvc** *pvc-id* **bridged-ethernet qos-policy out**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
  adsl adslx {
    pvc [0-255/0-65535|auto] {
      bridged-ethernet {
        out text
      }
    }
  }
}
```

Parameters

<i>adslx</i>	Mandatory. Multi-node. The identifier for the ADSL interface you are defining. This may be adsl0 to adslx , depending on what physical ADSL ports are actually available on the system.
<i>pvc-id</i>	Mandatory. The identifier for the PVC. It can either be the <i>vpi/vci</i> pair or the keyword auto , where <i>vpi</i> is a Virtual Path Index from 0 to 255, <i>vci</i> is a Virtual Circuit Index from 0 to 65535, and auto directs the system to detect the Virtual Path Index and Virtual Circuit Index automatically.
<i>policy-name</i>	The name of the outbound QoS policy to apply to this interface.

Default

None.

Usage Guidelines

Use this command to apply an outbound Quality of Service (QoS) policy to an ADSL interface encapsulated with RFC 1483 Bridged Ethernet.

Use the **set** form of this command to apply a QoS policy to the interface.

Use the **delete** form of this command to remove a QoS policy from the interface.

Use the **show** form of this command to display QoS policy configuration for an interface.

interfaces adsl <adslx> pvc <pvc-id> classical-ipoa qos-policy out <policy-name>

Applies an outbound QoS policy to a PVC with RFC 1577 Classical IPOA encapsulation on an ADSL interface.

Syntax

set interfaces adsl *adslx* **pvc** *pvc-id* **classical-ipoa qos-policy out** *policy-name*

delete interfaces adsl *adslx* **pvc** *pvc-id* **classical-ipoa qos-policy out**

show interfaces adsl *adslx* **pvc** *pvc-id* **classical-ipoa qos-policy out**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
  adsl adslx {
    pvc [0-255/0-65535|auto] {
      classical-ipoa {
        out text
      }
    }
  }
}
```

Parameters

<i>adslx</i>	Mandatory. Multi-node. The identifier for the ADSL interface you are defining. This may be adsl0 to adslx , depending on what physical ADSL ports are actually available on the system.
<i>pvc-id</i>	Mandatory. The identifier for the PVC. It can either be the <i>vpi/vci</i> pair or the keyword auto , where <i>vpi</i> is a Virtual Path Index from 0 to 255, <i>vci</i> is a Virtual Circuit Index from 0 to 65535, and auto directs the system to detect the Virtual Path Index and Virtual Circuit Index automatically.
<i>policy-name</i>	The name of the outbound QoS policy to apply to this interface.

Default

None.

Usage Guidelines

Use this command to apply an outbound Quality of Service (QoS) policy to an ADSL interface encapsulated with RFC 1577 Classical IP over Asynchronous Transfer Mode (IPOA).

Use the **set** form of this command to apply a QoS policy to the interface.

Use the **delete** form of this command to remove a QoS policy from the interface.

Use the **show** form of this command to display QoS policy configuration for an interface.

interfaces adsl <adslx> pvc <pvc-id> pppoa <num> qos-policy out <policy-name>

Applies an outbound QoS policy to a PVC with PPPoA encapsulation on an ADSL interface.

Syntax

set interfaces adsl *adslx* **pvc** *pvc-id* **pppoa** *num* **qos-policy out** *policy-name*

delete interfaces adsl *adslx* **pvc** *pvc-id* **pppoa** *num* **qos-policy out**

show interfaces adsl *adslx* **pvc** *pvc-id* **pppoa** *num* **qos-policy out**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
  adsl adslx {
    pvc [0-255/0-65535|auto] {
      pppoa 0-15 {
        out text
      }
    }
  }
}
```

Parameters

<i>adslx</i>	Mandatory. Multi-node. The identifier for the ADSL interface you are defining. This may be adsl0 to adslx , depending on what physical ADSL ports are actually available on the system.
<i>pvc-id</i>	Mandatory. The identifier for the PVC. It can either be the <i>vpi/vci</i> pair or the keyword auto , where <i>vpi</i> is a Virtual Path Index from 0 to 255, <i>vci</i> is a Virtual Circuit Index from 0 to 65535, and auto directs the system to detect the Virtual Path Index and Virtual Circuit Index automatically.
<i>num</i>	Mandatory. The PPPoA unit number. This number must be unique across all PPPoA interfaces. In addition, only one PPPoA instance can be configured on a PVC. PPPoA units range from 0 to 15 and the resulting interfaces are named pppoa0 to pppoa15 .
<i>policy-name</i>	The name of the outbound QoS policy to apply to this interface.

Default

None.

Usage Guidelines

Use this command to apply an outbound QoS policy to an ADSL interface with Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA) encapsulation.

Use the **set** form of this command to apply a QoS policy to the interface.

Use the **delete** form of this command to remove a QoS policy from the interface.

Use the **show** form of this command to display QoS policy configuration for an interface.

interfaces adsl <adslx> pvc <pvc-id> pppoe <num> qos-policy out <policy-name>

Applies an outbound QoS policy to a PVC with PPPoE encapsulation on an ADSL interface.

Syntax

set interfaces adsl *adslx* **pvc** *pvc-id* **pppoe** *num* **qos-policy out** *policy-name*

delete interfaces adsl *adslx* **pvc** *pvc-id* **pppoe** *num* **qos-policy out**

show interfaces adsl *adslx* **pvc** *pvc-id* **pppoe** *num* **qos-policy out**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
  adsl adslx {
    pvc [0-255/0-65535|auto] {
      pppoe 0-15 {
        out text
      }
    }
  }
}
```

Parameters

<i>adslx</i>	Mandatory. The name of the interface. This can be the name of a PPPoA-, PPPoE-, or Classical IPOA- encapsulated DSL interface; that is, the interface name can be pppoax , pppoex , or adslx .
<i>pvc-id</i>	Mandatory. The identifier for the PVC. It can either be the <i>vpi/vci</i> pair or the keyword auto , where <i>vpi</i> is a Virtual Path Index from 0 to 255, <i>vci</i> is a Virtual Circuit Index from 0 to 65535, and auto directs the system to detect the Virtual Path Index and Virtual Circuit Index automatically.
<i>num</i>	Mandatory. The PPPoE unit number. The range of values is 0 to 15.
<i>policy-name</i>	The name of the outbound QoS policy to apply to this interface.

Default

None.

Usage Guidelines

Use this command to apply an outbound QoS policy to an ADSL interface with Point-to-Point Protocol over Ethernet (PPPoE) encapsulation.

Use the **set** form of this command to apply a QoS policy to the interface.

Use the **delete** form of this command to remove a QoS policy from the interface.

Use the **show** form of this command to display QoS policy configuration for an interface.

interfaces bonding <bondx> qos-policy out <policy-name>

Applies an outbound QoS policy to an Ethernet link bonding interface.

Syntax

```
set interfaces bonding bondx qos-policy out policy-name
delete interfaces bonding bondx qos-policy out
show interfaces bonding bondx qos-policy out
```

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    bonding bondx {
        out text
    }
}
```

Parameters

<i>bondx</i>	Multi-node. The identifier for the bonding interface. Supported values are bond0 through bond99 .
<i>policy-name</i>	The name of the outbound QoS policy to apply to this interface.

Default

None.

Usage Guidelines

Use this command to apply an outbound QoS policy to an Ethernet link bonding interface..

Use the **set** form of this command to apply a QoS policy to the interface.

Use the **delete** form of this command to remove a QoS policy from the interface.

Use the **show** form of this command to display QoS policy configuration for an interface.

interfaces ethernet <ethx> pppoe <num> qos-policy out <policy-name>

Applies an outbound QoS policy to a PVC with PPPoE encapsulation on an Ethernet interface.

Syntax

set interfaces ethernet *ethx* **pppoe** *num* **qos-policy out** *policy-name*

delete interfaces ethernet *ethx* **pppoe** *num* **qos-policy out**

show interfaces ethernet *ethx* **pppoe** *num* **qos-policy out**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {  
    ethernet [eth0..eth23] {  
        pppoe 0-15 {  
            out text  
        }  
    }  
}
```

Parameters

<i>ethx</i>	Mandatory. The name of a defined Ethernet interface. The range is eth0 to eth23 .
<i>num</i>	Mandatory. The PPPoE unit number. The range of values is 0 to 15.
<i>policy-name</i>	The name of the outbound QoS policy to apply to this interface.

Default

None.

Usage Guidelines

Use this command to apply an outbound QoS policy to an Ethernet interface with Point-to-Point Protocol over Ethernet (PPPoE) encapsulation.

For information about defining QoS policies, see the *Vyatta Policy and QoS Reference Guide*.

Use the **set** form of this command to apply a QoS policy to the interface.

Use the **delete** form of this command to remove a QoS policy from the interface.

Use the **show** form of this command to display QoS policy configuration for an interface.

interfaces ethernet <ethx> qos-policy

Applies QoS policy to the specified Ethernet interface.

Syntax

```
set interfaces ethernet ethx qos-policy {in in-policy-name | out out-policy-name}
delete interfaces ethernet ethx qos-policy {in | out}
show interfaces ethernet ethx qos-policy {in | out}
```

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
  ethernet eth0..eth23 {
    qos-policy {
      in text
      out text
    }
  }
}
```

Parameters

<i>ethx</i>	Mandatory. The name of an Ethernet interface.
<i>in-policy-name</i>	The name of the inbound QoS policy to apply to this interface.
<i>out-policy-name</i>	The name of the outbound QoS policy to apply to this interface.

Default

None.

Usage Guidelines

Use this command to apply a QoS policy to an interface.

Use the **set** form of this command to apply the QoS policy to the interface.

Use the **delete** form of this command to remove the QoS policy from the interface.

Use the **show** form of this command to display QoS policy configuration for an interface.

interfaces ethernet <ethx> vif <vlan-id> qos-policy out <policy-name>

Applies an outbound QoS policy to the specified virtual interface.

Syntax

```
set interfaces ethernet ethx vif vlan-id qos-policy out policy-name
delete interfaces ethernet ethx vif vlan-id qos-policy out
show interfaces ethernet ethx vif vlan-id qos-policy out
```

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
  ethernet eth0..eth23 {
    vif 0-4095 {
      qos-policy {
        out text
      }
    }
  }
}
```

Parameters

<i>ethx</i>	Mandatory. The name of an Ethernet interface.
<i>vlan-id</i>	Mandatory. The VLAN ID for the vif. The range is 0 to 4095.
<i>policy-name</i>	The name of the outbound QoS policy to apply to this interface.

Default

None.

Usage Guidelines

Use this command to apply an outbound QoS policy to an interface.

Use the **set** form of this command to apply the QoS policy to the interface.

Use the **delete** form of this command to remove the QoS policy from the interface.

Use the **show** form of this command to display QoS policy configuration for an interface.

interfaces serial <wanx> qos-policy

Applies QoS policy to the specified Serial interface.

Syntax

```
set interfaces serial wanx qos-policy {in in-policy-name | out out-policy-name}  
delete interfaces serial wanx qos-policy {in | out}  
show interfaces serial wanx qos-policy {in | out}
```

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {  
    serial wan0..wan23 {  
        qos-policy {  
            in text  
            out text  
        }  
    }  
}
```

Parameters

<i>wanx</i>	Mandatory. The name of an Serial interface.
<i>in-policy-name</i>	The name of the inbound QoS policy to apply to this interface.
<i>out-policy-name</i>	The name of the outbound QoS policy to apply to this interface.

Default

None.

Usage Guidelines

Use this command to apply a QoS policy to an interface.

Use the **set** form of this command to apply the QoS policy to the interface.

Use the **delete** form of this command to remove the QoS policy from the interface.

Use the **show** form of this command to display QoS policy configuration for an interface.

qos-policy drop-tail <policy-name>

Defines a drop tail (pure FIFO) QoS policy.

Syntax

```
set qos-policy drop-tail policy-name
delete qos-policy drop-tail policy-name
show qos-policy drop-tail policy-name
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
    drop-tail text {
    }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the drop tail policy.
--------------------	--

Default

None.

Usage Guidelines

Use this command to define a drop tail QoS policy. The drop tail policy acts on outbound traffic only. The policy name must be unique and not used with other QoS policy commands.

The drop tail policy provides a pure First In First Out (FIFO) queueing mechanism.

Use the **set** form of this command to create a drop tail policy.

Use the **delete** form of this command to remove a drop tail policy.

Use the **show** form of this command to display drop tail policy configuration.

qos-policy drop-tail <policy-name> queue-limit <limit>

Sets an upper bound for the number of packets allowed in the queue for a drop queue policy.

Syntax

```
set qos-policy drop-tail policy-name queue-limit limit
delete qos-policy drop-tail policy-name queue-limit
show qos-policy drop-tail policy-name queue-limit
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
    drop-tail text {
        queue-limit u32
    }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the drop tail policy.
<i>limit</i>	Optional. The maximum queue size, in packets. The range is 0 to 4294967295. The default is the same as the underlying hardware transmit queue length. For Ethernet this is typically 1000 packets.

Default

For Ethernet the queue limit is typically 1000 packets.

Usage Guidelines

Use this command to set the maximum number of packets that can wait in a queue for this queuing policy. If maximum queue size is reached, the system begins dropping packets.

Use the **set** form of this command to set the queue limit.

Use the **delete** form of this command to restore the default queue limit.

Use the **show** form of this command to display queue limit configuration.

qos-policy fair-queue <policy-name>

Defines a fair queue QoS policy.

Syntax

```
set qos-policy fair-queue policy-name
delete qos-policy fair-queue policy-name
show qos-policy fair-queue policy-name
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
    fair-queue text {
    }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the fair queue policy.
--------------------	---

Default

None.

Usage Guidelines

Use this command to define a fair queue (FQ) QoS policy. The FQ policy acts on outbound traffic only. The policy name must be unique and not used with other QoS policy commands.

The Vyatta system uses Stochastic Fair Queuing, which is one of a number of FQ algorithms aiming to provide per-flow-based fairness. The FQ algorithm attempts to provide fair access to network resources and prevent any one flow from consuming an inordinate amount of output port bandwidth.

In Stochastic Fair Queuing, bandwidth is divided into separate hash buckets based on the combination of IP protocol, source, and destination address such that no single flow receives an unfair portion of bandwidth.

Use the **set** form of this command to create an FQ policy.

Use the **delete** form of this command to remove an FQ policy.

Use the **show** form of this command to display FQ policy configuration.

qos-policy fair-queue <policy-name> description <desc>

Sets a description for a fair queue policy.

Syntax

```
set qos-policy fair-queue policy-name description desc  
delete qos-policy fair-queue policy-name description  
show qos-policy fair-queue policy-name description
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    fair-queue text {  
        description text  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the fair queue policy.
<i>desc</i>	Mandatory. The description for this fair queue policy.

Default

None.

Usage Guidelines

Use this command to record a description for a fair queue policy.

Use the **set** form of this command to specify a description.

Use the **delete** form of this command to remove a description.

Use the **show** form of this command to display description configuration.

qos-policy fair-queue <policy-name> hash-interval <seconds>

Specifies the interval between flow hash function updates for a fair queue policy.

Syntax

```
set qos-policy fair-queue policy-name hash-interval seconds
delete qos-policy fair-queue policy-name hash-interval
show qos-policy fair-queue policy-name hash-interval
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
    fair-queue text {
        hash-interval u32
    }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the fair queue policy.
<i>seconds</i>	Mandatory. The rehash interval, in seconds. The range is 0 to 4294967295, where 0 means the hash function is never updated.

Default

The hash function is never updated.

Usage Guidelines

Use this command to set the interval at which the flow hash function is updated.

Updating the hash function at intervals increases security and prevents attacks based on an attacker determining the hash bucket for traffic flows and sending spoofed packets based on that information.

Use the **set** form of this command to specify a flow hash update interval.

Use the **delete** form of this command to restore the default hash interval.

Use the **show** form of this command to display hash interval configuration.

qos-policy fair-queue <policy-name> queue-limit <limit>

Sets an upper bound for the number of packets allowed in the queue for a fair queue policy.

Syntax

```
set qos-policy fair-queue policy-name queue-limit limit
delete qos-policy fair-queue policy-name queue-limit
show qos-policy fair-queue policy-name queue-limit
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
    fair-queue text {
        queue-limit u32
    }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the fair queue policy.
<i>limit</i>	Mandatory. The maximum queue size, in packets. The range is 0 to 4294967295. The default is 127.

Default

A queue is not permitted to exceed 127 packets.

Usage Guidelines

Use this command to set the maximum number of packets that can wait in a queue for this queuing policy. If maximum queue size is reached, the system begins dropping packets.

Use the **set** form of this command to set the queue limit.

Use the **delete** form of this command to restore the default queue limit.

Use the **show** form of this command to display queue limit configuration.

qos-policy rate-limit <policy-name>

Defines a rate limiting QoS policy.

Syntax

```
set qos-policy rate-limit policy-name
delete qos-policy rate-limit policy-name
show qos-policy rate-limit policy-name
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
    rate-limit text {
    }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the rate limiting policy.
--------------------	--

Default

None.

Usage Guidelines

Use this command to define a rate limiting QoS policy. Rate limit policy acts on outbound traffic only. The policy name must be unique and not used with other QoS policy commands.

The Vyatta system uses a version of the Token Bucket Filter (TBF) algorithm. TBF is a classless queuing discipline that only passes packets arriving at a rate which is not exceeding some administratively set rate, but with the possibility to allow short bursts in excess of this rate.

Use the **set** form of this command to create a rate limiting QoS policy.

Use the **delete** form of this command to remove a rate limiting QoS policy.

Use the **show** form of this command to display rate limiting QoS policy configuration.

qos-policy rate-limit <policy-name> bandwidth

Specifies the bandwidth limit for all combined traffic constrained by this policy.

Syntax

```
set qos-policy rate-limit policy-name bandwidth [rate | rate-suffix]  
delete qos-policy rate-limit policy-name bandwidth  
show qos-policy rate-limit policy-name bandwidth
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    rate-limit text {  
        bandwidth text  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the rate limiting policy.
<i>rate</i>	The bandwidth, specified in kilobits per second.
<i>rate-suffix</i>	The bandwidth, specified as a number and a scaling suffix (for example, 10mbit). The following suffixes are supported: kbit : Kilobits per second. mbit : Megabits per second. gbit : Gigabits per second. kbps : Kilobytes per second. mbps : Megabytes per second. gbps : Gigabytes per second.

Default

None.

Usage Guidelines

Use this command to set bandwidth constraints for a rate limiting QoS policy. This is the maximum bandwidth available for all classes and must be set.

Use the **set** form of this command to specify bandwidth constraints for the policy.

Use the **delete** form of this command to restore default bandwidth constraints for the policy.

Use the **show** form of this command to display policy bandwidth configuration.

qos-policy rate-limit <policy-name> burst

Sets the burst size for a rate limiting QoS policy.

Syntax

set qos-policy rate-limit *policy-name* **burst** [*num* | *num-suffix*]

delete qos-policy rate-limit *policy-name* **burst**

show qos-policy rate-limit *policy-name* **burst**

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    rate-limit text {  
        burst text  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the rate limiting policy.
<i>num</i>	The burst size, specified in bytes.
<i>num-suffix</i>	The burst size, specified as a number and a scaling suffix (for example, 10mb). The following suffixes are supported: kb : Kilobytes. mb : Megabytes. gb : Gigabytes.

Default

The default burst size is 15 kilobytes.

Usage Guidelines

Use this command to set the burst size for a rate limiting QoS policy. This is the maximum amount of traffic that may be sent at a given time.

Use the **set** form of this command to specify the burst size for a rate limiting QoS policy.

Use the **delete** form of this command to restore the default burst size for a rate limiting QoS policy.

Use the **show** form of this command to display rate limit burst size configuration.

qos-policy rate-limit <policy-name> description <desc>

Sets a description for a rate limiting policy.

Syntax

```
set qos-policy rate-limit policy-name description desc  
delete qos-policy rate-limit policy-name description  
show qos-policy rate-limit policy-name description
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    rate-limit text {  
        description text  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the rate limit policy.
<i>desc</i>	Mandatory. The description for this rate limit policy.

Default

None.

Usage Guidelines

Use this command to record a description for a rate limit policy.

Use the **set** form of this command to specify a description.

Use the **delete** form of this command to remove a description.

Use the **show** form of this command to display description configuration.

qos-policy rate-limit <policy-name> latency

Sets the limit on queue size based on latency for a rate limiting QoS policy.

Syntax

set qos-policy rate-limit *policy-name* **latency** [*num* | *num-suffix*]

delete qos-policy rate-limit *policy-name* **latency**

show qos-policy rate-limit *policy-name* **latency**

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    rate-limit text {  
        latency text  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the rate limiting policy.
<i>num</i>	The latency, specified in milliseconds.
<i>num-suffix</i>	The latency, specified as a time and a scaling suffix (for example, 10ms). The following suffixes are supported: secs : Seconds. ms : Milliseconds. us : Microseconds.

Default

The default latency is 50 milliseconds.

Usage Guidelines

Use this command to set the latency for a rate limiting QoS policy. This is the maximum amount of time a packet can sit in the Token Bucket Filter.

Use the **set** form of this command to specify the latency for a rate limiting QoS policy.

Use the **delete** form of this command to restore the default latency for a rate limiting QoS policy.

Use the **show** form of this command to display rate limit latency configuration.

qos-policy traffic-limiter <policy-name>

Defines a traffic limiting QoS policy.

Syntax

```
set qos-policy traffic-limiter policy-name
delete qos-policy traffic-limiter policy-name
show qos-policy traffic-limiter policy-name
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
    traffic-limiter text {
    }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic limiting policy.
--------------------	---

Default

None.

Usage Guidelines

Use this command to define a traffic limiter QoS policy. Traffic limiter policy acts on inbound traffic only. The policy name must be unique and not used with other QoS policy commands.

Traffic is evaluated against the matching rules which are similar to outbound traffic shaper. Any traffic that matches no rules is let through unrestricted. Any traffic that exceeds the bandwidth limits is dropped.

Use the **set** form of this command to create a traffic limiter QoS policy.

Use the **delete** form of this command to remove a traffic limiter QoS policy.

Use the **show** form of this command to display traffic limiter QoS policy configuration.

qos-policy traffic-limiter <policy-name> class <class>

Defines a traffic class for a traffic limiter QoS policy.

Syntax

```
set qos-policy traffic-limiter policy-name class class  
delete qos-policy traffic-limiter policy-name class class  
show qos-policy traffic-limiter policy-name class class
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-limiter text {  
        class 1-4095 {  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic limiting policy.
<i>class</i>	Mandatory. The class ID. The range is 1 to 4095.

Default

None.

Usage Guidelines

Use this command to define a traffic class for a traffic limiter QoS policy. This allows packets to be grouped into various traffic classes, which can be treated with different levels of service.

Use the **set** form of this command to create a traffic class in a traffic limiter QoS policy.

Use the **delete** form of this command to remove a traffic class from a traffic limiter QoS policy.

Use the **show** form of this command to display traffic class configuration within a traffic limiter QoS policy.

qos-policy traffic-limiter <policy-name> class <class> bandwidth

Specifies the bandwidth rate cap for a traffic class.

Syntax

```
set qos-policy traffic-limiter policy-name class class bandwidth [rate | rate-suffix]  
delete qos-policy traffic-limiter policy-name class class bandwidth  
show qos-policy traffic-limiter policy-name class class bandwidth
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-limiter text {  
        class 1-4095 {  
            bandwidth text  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic limiting policy.
<i>class</i>	Mandatory. The class ID. The range is 1 to 4095.
<i>rate</i>	The bandwidth, specified in kilobits per second.
<i>rate-suffix</i>	The bandwidth, specified as a number and a scaling suffix (for example, 10mbit). The following suffixes are supported: kbit : Kilobits per second. mbit : Megabits per second. gbit : Gigabits per second. kbps : Kilobytes per second. mbps : Megabytes per second. gbps : Gigabytes per second.

Default

None. This value must be set.

Usage Guidelines

Use this command to set a bandwidth cap for a traffic class.

Use the **set** form of this command to set the available bandwidth for the traffic class.

Use the **delete** form of this command to restore the default available bandwidth for the traffic class.

Use the **show** form of this command to display class bandwidth configuration.

qos-policy traffic-limiter <policy-name> class <class> description <desc>

Sets a description for a traffic class.

Syntax

```
set qos-policy traffic-limiter policy-name class class description desc  
delete qos-policy traffic-limiter policy-name class class description  
show qos-policy traffic-limiter policy-name class class description
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-limiter text {  
        class 1-4095 {  
            description text  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic limiting policy.
<i>class</i>	Mandatory. The class ID. The range is 1 to 4095.
<i>desc</i>	Mandatory. The description for this traffic class.

Default

None.

Usage Guidelines

Use **this** command to record a description for a traffic class.

Use the **set** form of this command to specify a description.

Use the **delete** form of this command to remove a description.

Use the **show** form of this command to display description configuration.

qos-policy traffic-limiter <policy-name> class <class> match <match-name>

Defines a traffic class matching rule.

Syntax

```
set qos-policy traffic-limiter policy-name class class match match-name  
delete qos-policy traffic-limiter policy-name class class match match-name  
show qos-policy traffic-limiter policy-name class class match match-name
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-limiter text {  
        class 1-4095 {  
            match text {  
            }  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic limiting policy.
<i>class</i>	Mandatory. The class ID. The range is 1 to 4095.
<i>match-name</i>	Mandatory. Class matching rule name.

Default

None.

Usage Guidelines

Use this command to define a rule setting out the match conditions for membership in a traffic class.

Use the **set** form of this command to create the traffic class matching rule. Note that you cannot use **set** to change the name of an existing traffic class matching rule. To change the rule, delete it and re-create it.

Use the **delete** form of this command to remove the traffic class matching rule configuration node.

Use the **show** form of this command to display traffic class matching rule configuration.

qos-policy traffic-limiter <policy-name> class <class> match <match-name> description <desc>

Sets a description for a match rule.

Syntax

```
set qos-policy traffic-limiter policy-name class class match match-name description  
desc
```

```
delete qos-policy traffic-limiter policy-name class class match match-name description
```

```
show qos-policy traffic-limiter policy-name class class match match-name description
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-limiter text {  
        class 1-4095 {  
            match text {  
                description text  
            }  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic limiting policy.
--------------------	---

<i>class</i>	Mandatory. The class ID. The range is 1 to 4095.
--------------	--

<i>match-name</i>	Mandatory. Class matching rule name.
-------------------	--------------------------------------

<i>desc</i>	Mandatory. The description for this match.
-------------	--

Default

None.

Usage Guidelines

Use this command to record a description for a traffic class matching rule.

Use the **set** form of this command to set the description.

Use the **delete** form of this command to remove the description.

Use the **show** form of this command to display description configuration.

qos-policy traffic-limiter <policy-name> class <class> match <match-name> ip destination

Specifies a match criterion based on IP destination information.

Syntax

```
set qos-policy traffic-limiter policy-name class class match match-name ip destination
{address ipv4 / port port}

delete qos-policy traffic-limiter policy-name class class match match-name ip
destination [address / port]

show qos-policy traffic-limiter policy-name class class match match-name ip
destination
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
  traffic-limiter text {
    class 1-4095 {
      match text {
        ip {
          destination {
            address ipv4
            port text
          }
        }
      }
    }
  }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic limiting policy.
<i>class</i>	Mandatory. The class ID. The range is 1 to 4095.
<i>match-name</i>	Mandatory. Class matching rule name.

<i>ipv4</i>	Performs a match based on the destination IP address and prefix.
<i>port</i>	Performs a match based on destination port. The port may be specified as a lower-case name (for example ssh) or as a number. The range for port numbers is 0 to 65535.

Default

If not set, packets are not matched against destination information.

Usage Guidelines

Use this command to define a match condition based on destination address and/or port for a traffic class.

You can match packets based on a destination represented by either or both of IP address and destination port(s).

Note that you are not able to match on both “ip” and “vif” (or “interface”) inside the same traffic limiter configuration.

Use the **set** form of this command to specify a destination to be matched.

Use the **delete** form of this command to remove destination as a match condition.

Use the **show** form of this command to display destination match condition configuration.

qos-policy traffic-limiter <policy-name> class <class> match <match-name> ip dscp <value>

Specifies a match criterion based on the value of the DSCP field.

Syntax

```
set qos-policy traffic-limiter policy-name class class match match-name ip dscp value
delete qos-policy traffic-limiter policy-name class class match match-name ip dscp
show qos-policy traffic-limiter policy-name class class match match-name ip dscp
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
  traffic-limiter text {
    class 1-4095 {
      match text {
        ip {
          dscp text
        }
      }
    }
  }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic limiting policy.
<i>class</i>	Mandatory. The class ID. The range is 1 to 4095.
<i>match-name</i>	Mandatory. Class matching rule name.
<i>value</i>	Performs a match based on the specified value. This value is compared with the value in the DSCP field of the ToS byte in the IP header. The DSCP value can be specified as a decimal number (for example, 12), as a hexadecimal number (for example 0x1D), or as a standard name from <i>/etc/iproute2/rt_dsfield</i> (for example, lowdelay).

Default

If not set, packets are not matched against DSCP value.

Usage Guidelines

Use this command to define a match condition based on the Differentiated Services Code Point (DSCP) field.

The DSCP field is a 6-bit field in the Type of Service (ToS) byte of the IP header. It provides a way of marking packets in order to allow classification of traffic into service classes, and traffic conditioning such as metering, policing, and shaping.

Note that you are not able to match on both “ip” and “vif” (or “interface”) inside the same traffic limiter configuration.

Use the **set** form of this command to set a match condition based on DSCP value.

Use the **delete** form of this command to remove DSCP as a match condition.

Use the **show** form of this command to display DSCP value configuration.

qos-policy traffic-limiter <policy-name> class <class> match <match-name> ip protocol <proto>

Specifies a match criterion based on the IP protocol.

Syntax

```
set qos-policy traffic-limiter policy-name class class match match-name ip protocol
proto
delete qos-policy traffic-limiter policy-name class class match match-name ip protocol
show qos-policy traffic-limiter policy-name class class match match-name ip protocol
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
  traffic-limiter text {
    class 1-4095 {
      match text {
        ip {
          protocol text
        }
      }
    }
  }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic limiting policy.
<i>class</i>	Mandatory. The class ID. The range is 1 to 4095.
<i>match-name</i>	Mandatory. Class matching rule name.
<i>proto</i>	Performs a match based on the protocol name (for example, icmp) or number, as assigned by the IANA.

Default

If not set, packets are not matched against IP protocol.

Usage Guidelines

Use this command to define a match condition for a traffic class based on protocol.

Note that you are not able to match on both “ip” and “vif” (or “interface”) inside the same traffic limiter configuration.

Use the **set** form of this command to set a match condition based on protocol.

Use the **delete** form of this command to remove protocol value as a match condition.

Use the **show** form of this command to match condition protocol configuration.

qos-policy traffic-limiter <policy-name> class <class> match <match-name> ip source

Specifies a match criterion based on source IP information.

Syntax

```
set qos-policy traffic-limiter policy-name class class match match-name ip source  
{address ipv4 | port port}
```

```
delete qos-policy traffic-limiter policy-name class class match match-name ip source  
{address | port}
```

```
show qos-policy traffic-limiter policy-name class class match match-name ip source
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-limiter text {  
        class 1-4095 {  
            match text {  
                ip {  
                    source {  
                    }  
                }  
            }  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic limiting policy.
<i>class</i>	Mandatory. The class ID. The range is 1 to 4095.
<i>match-name</i>	Mandatory. Class matching rule name.
<i>ipv4</i>	The source IP address and prefix to match for this rule.

<i>port</i>	The source port to match for this rule. The port may be specified as a lower-case name (for example ssh) or as a number. The range for port numbers is 0 to 65535.
-------------	--

Default

If not set, packets are not matched against IP source information.

Usage Guidelines

Use this command to define a match condition based on source address and/or port for a traffic class.

You can match packets based on a source represented by either or both of IP address and destination port(s).

Note that you are not able to match on both “ip” and “vif” (or “interface”) inside the same traffic limiter configuration.

Use the **set** form of this command to specify a source to be matched.

Use the **delete** form of this command to remove source as a match condition.

Use the **show** form of this command to display source match condition configuration.

qos-policy traffic-limiter <policy-name> class <class> match <match-name> vif <vlan-id>

Specifies a match criterion based on VLAN ID.

Syntax

```
set qos-policy traffic-limiter policy-name class class match match-name vif vlan-id  
delete qos-policy traffic-limiter policy-name class class match match-name vif  
show qos-policy traffic-limiter policy-name class class match match-name vif
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-limiter text {  
        class 1-4095 {  
            match text {  
                vif 1-4096  
            }  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic limiting policy.
<i>class</i>	Mandatory. The class ID. The range is 1 to 4095.
<i>match-name</i>	Mandatory. Class matching rule name.
<i>vlan-id</i>	Performs a match based on VLAN ID. The range is 1 to 4096.

Default

If not set, packets are not matched against VLAN ID.

Usage Guidelines

Use this command to define a match condition based on VLAN ID for a traffic class.

Note that you are not able to match on both “ip” and “vif” (or “interface”) inside the same traffic limiter configuration.

Use the **set** form of this command to specify a VLAN ID to be matched.

Use the **delete** form of this command to remove VLAN ID as a match condition.

Use the **show** form of this command to display VLAN ID match condition configuration.

qos-policy traffic-limiter <policy-name> class <class> priority <priority>

Specifies the priority of a traffic class for allocation of extra bandwidth.

Syntax

```
set qos-policy traffic-limiter policy-name class class priority priority
delete qos-policy traffic-limiter policy-name class class priority
show qos-policy traffic-limiter policy-name class class priority
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
  traffic-limiter text {
    class 1-4095 {
      priority u32
    }
  }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic limiting policy.
<i>class</i>	Mandatory. The class ID. The range is 1 to 4095.
<i>priority</i>	The priority with which this traffic class should be allocated extra bandwidth. The range is 1 to 1000, where the higher the number the lower the priority. The default is 20.

Default

Traffic classes are assigned a priority of 20.

Usage Guidelines

Use this command to set the priority with which a traffic class is to be awarded extra bandwidth when excess is available.

Use the **set** form of this command to specify priority for a traffic class.

Use the **delete** form of this command to restore the default priority for a traffic class.

Use the **show** form of this command to display traffic class priority configuration.

qos-policy traffic-limiter <policy-name> description <desc>

Specifies a description for a traffic limiter QoS policy.

Syntax

```
set qos-policy traffic-limiter policy-name description desc  
delete qos-policy traffic-limiter policy-name description  
show qos-policy traffic-limiter policy-name description
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-limiter text {  
        description text  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic limiting policy.
<i>desc</i>	The description for this traffic limiter policy.

Default

None.

Usage Guidelines

Use this command to record a description for a traffic limiter policy.

Use the **set** form of this command to specify a description for a traffic limiter policy.

Use the **delete** form of this command to remove a description from a traffic limiter policy.

Use the **show** form of this command to display description configuration for a traffic limiter policy.

qos-policy traffic-shaper <policy-name>

Defines a traffic shaping QoS policy.

Syntax

```
set qos-policy traffic-shaper policy-name
delete qos-policy traffic-shaper policy-name
show qos-policy traffic-shaper policy-name
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
    traffic-shaper text {
    }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
--------------------	--

Default

None.

Usage Guidelines

Use this command to define a traffic shaper QoS policy. Traffic shaper policy acts on outbound traffic only. The policy name must be unique and not used with other QoS policy commands.

The Vyatta system uses a version of the Token Bucket traffic shaping algorithm. The Token Bucket algorithm places a limit on the average traffic transmission rate, but allows controlled bursting on the network. The Token Bucket algorithm provides the ability to control bandwidth for VoIP, or limit bandwidth consumption for peer-to-peer applications.

In the Token Bucket algorithm, each flow has a certain number of tokens in its “bucket,” and transmitting traffic “spends” these tokens. If the token bucket is empty, the flow is not permitted to send packets.

This method allows a network administrator to control the amount of bandwidth allocated to different types of traffic. This method also allows a flow to burst traffic, provided it has enough tokens in its bucket.

Use the **set** form of this command to create a traffic shaper QoS policy.

Use the **delete** form of this command to remove a traffic shaper QoS policy.

Use the **show** form of this command to display traffic shaper QoS policy configuration.

qos-policy traffic-shaper <policy-name> bandwidth

Specifies the bandwidth available for all combined traffic constrained by this policy.

Syntax

```
set qos-policy traffic-shaper policy-name bandwidth [auto | rate | rate-suffix]  
delete qos-policy traffic-shaper policy-name bandwidth  
show qos-policy traffic-shaper policy-name bandwidth
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-shaper text {  
        bandwidth text  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
auto	Automatically bases the bandwidth on the interface speed.
<i>rate</i>	The bandwidth, specified in kilobits per second.
<i>rate-suffix</i>	The bandwidth, specified as a number and a scaling suffix (for example, 10mbit). The following suffixes are supported: kbit : Kilobits per second. mbit : Megabits per second. gbit : Gigabits per second. kbps : Kilobytes per second. mbps : Megabytes per second. gbps : Gigabytes per second.

Default

The default is **auto**.

Usage Guidelines

Use this command to set bandwidth constraints for a traffic shaper QoS policy. This is the maximum bandwidth available for all classes.

Use the **set** form of this command to specify bandwidth constraints for the policy.

Use the **delete** form of this command to restore default bandwidth constraints for the policy.

Use the **show** form of this command to display policy bandwidth configuration.

qos-policy traffic-shaper <policy-name> class <class>

Defines a traffic class for a traffic shaper QoS policy.

Syntax

```
set qos-policy traffic-shaper policy-name class class  
delete qos-policy traffic-shaper policy-name class class  
show qos-policy traffic-shaper policy-name class class
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-shaper text {  
        class 3-4095 {  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>class</i>	Mandatory. The class ID. The range is 3 to 4095.

Default

None.

Usage Guidelines

Use this command to define a traffic class for a traffic shaper QoS policy. This allows packets to be grouped into various traffic classes, which can be treated with different levels of service.

Use the **set** form of this command to create a traffic class in a traffic shaper QoS policy.

Use the **delete** form of this command to remove a traffic class from a traffic shaper QoS policy.

Use the **show** form of this command to display traffic class configuration within a traffic shaper QoS policy.

qos-policy traffic-shaper <policy-name> class <class> bandwidth

Specifies the base guaranteed bandwidth rate for a traffic class.

Syntax

```
set qos-policy traffic-shaper policy-name class class bandwidth [rate | rate-pct |  
rate-suffix]
```

```
delete qos-policy traffic-shaper policy-name class class bandwidth
```

```
show qos-policy traffic-shaper policy-name class class bandwidth
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-shaper text {  
        class 3-4095 {  
            bandwidth text  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>class</i>	Mandatory. The class ID. The range is 3 to 4095.
<i>rate</i>	The bandwidth, specified in kilobits per second.
<i>rate-pct</i>	The bandwidth, specified as a percentage of the overall bandwidth rate. The format is <i>num</i> % (for example, 85%).

<i>rate-suffix</i>	The bandwidth, specified as a number and a scaling suffix (for example, 10mbit). The following suffixes are supported: kbit : Kilobits per second. mbit : Megabits per second. gbit : Gigabits per second. kbps : Kilobytes per second. mbps : Megabytes per second. gbps : Gigabytes per second.
--------------------	---

Default

100% bandwidth usage is available.

Usage Guidelines

Use this command to set a base level of guaranteed bandwidth for a traffic class.

Use the **set** form of this command to set the available bandwidth for the traffic class.

Use the **delete** form of this command to restore the default available bandwidth for the traffic class.

Use the **show** form of this command to display class bandwidth configuration.

qos-policy traffic-shaper <policy-name> class <class> burst

Sets the burst size for a traffic class.

Syntax

```
set qos-policy traffic-shaper policy-name class class burst [num | num-suffix]  
delete qos-policy traffic-shaper policy-name class class burst  
show qos-policy traffic-shaper policy-name class class burst
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-shaper text {  
        class 3-4095 {  
            burst text  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>class</i>	Mandatory. The class ID. The range is 3 to 4095.
<i>num</i>	The burst size, specified in bytes.
<i>num-suffix</i>	The burst size, specified as a number and a scaling suffix (for example, 10mb). The following suffixes are supported: kb : Kilobytes. mb : Megabytes. gb : Gigabytes.

Default

The burst size is 15 kilobytes.

Usage Guidelines

Use this command to set the burst size for the traffic class. This is the maximum amount of traffic that may be sent at a given time.

Use the **set** form of this command to specify the burst size for a traffic class.

Use the **delete** form of this command to restore the default burst size for a traffic class.

Use the **show** form of this command to display traffic class burst size configuration.

qos-policy traffic-shaper <policy-name> class <class> ceiling

Sets a bandwidth ceiling for a traffic class.

Syntax

```
set qos-policy traffic-shaper policy-name class class ceiling [rate | rate-pct | rate-suffix]  
delete qos-policy traffic-shaper policy-name class class ceiling  
show qos-policy traffic-shaper policy-name class class ceiling
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-shaper text {  
        class 3-4095 {  
            ceiling text  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>class</i>	Mandatory. The class ID. The range is 3 to 4095.
<i>rate</i>	The maximum bandwidth, specified in kilobits per second.
<i>rate-pct</i>	The maximum bandwidth, specified as a percentage of the interface speed. The format is <i>num%</i> (for example, 85%).
<i>rate-suffix</i>	The bandwidth, specified as a number and a scaling suffix (for example, 10mbit). The following suffixes are supported: kbit : Kilobits per second. mbit : Megabits per second. gbit : Gigabits per second.

Default

The default is 100%.

Usage Guidelines

Use **this** command to set the maximum amount of bandwidth a traffic class may consume when excess bandwidth is available.

Use the **set** form of this command to set the bandwidth ceiling for a traffic class.

Use the **delete** form of this command to restore the default bandwidth ceiling for a traffic class.

Use the **show** form of this command to display traffic class bandwidth ceiling configuration.

qos-policy traffic-shaper <policy-name> class <class> description <desc>

Sets a description for a traffic class.

Syntax

```
set qos-policy traffic-shaper policy-name class class description desc  
delete qos-policy traffic-shaper policy-name class class description  
show qos-policy traffic-shaper policy-name class class description
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-shaper text {  
        class 3-4095 {  
            description text  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>class</i>	Mandatory. The class ID. The range is 3 to 4095.
<i>desc</i>	Mandatory. The description for this traffic class.

Default

None.

Usage Guidelines

Use **this** command to record a description for a traffic class.

Use the **set** form of this command to specify a description.

Use the **delete** form of this command to remove a description.

Use the **show** form of this command to display description configuration.

qos-policy traffic-shaper <policy-name> class <class> match <match-name>

Defines a traffic class matching rule.

Syntax

```
set qos-policy traffic-shaper policy-name class class match match-name  
delete qos-policy traffic-shaper policy-name class class match match-name  
show qos-policy traffic-shaper policy-name class class match match-name
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-shaper text {  
        class 3-4095 {  
            match text {  
            }  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>class</i>	Mandatory. The class ID. The range is 3 to 4095.
<i>match-name</i>	Mandatory. Class matching rule name.

Default

None.

Usage Guidelines

Use this command to define a rule setting out the match conditions for membership in a traffic class.

Use the **set** form of this command to create the traffic class matching rule. Note that you cannot use **set** to change the name of an existing traffic class matching rule. To change the rule, delete it and re-create it.

Use the **delete** form of this command to remove the traffic class matching rule configuration node.

Use the **show** form of this command to display traffic class matching rule configuration.

qos-policy traffic-shaper <policy-name> class <class> match <match-name> description <desc>

Sets a description for a match rule.

Syntax

```
set qos-policy traffic-shaper policy-name class class match match-name description  
desc
```

```
delete qos-policy traffic-shaper policy-name class class match match-name description
```

```
show qos-policy traffic-shaper policy-name class class match match-name description
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-shaper text {  
        class 3-4095 {  
            match text {  
                description text  
            }  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>class</i>	Mandatory. The class ID. The range is 3 to 4095.
<i>match-name</i>	Mandatory. Class matching rule name.
<i>desc</i>	Mandatory. The description for this match.

Default

None.

Usage Guidelines

Use this command to record a description for a traffic class matching rule.

Use the **set** form of this command to set the description.

Use the **delete** form of this command to remove the description.

Use the **show** form of this command to display description configuration.

qos-policy traffic-shaper <policy-name> class <class> match <match-name> interface <interface>

Specifies a match criterion based on incoming interface.

Syntax

set qos-policy traffic-shaper *policy-name* **class** *class* **match** *match-name* **interface** *interface*

delete qos-policy traffic-shaper *policy-name* **class** *class* **match** *match-name* **interface** *interface*

show qos-policy traffic-shaper *policy-name* **class** *class* **match** *match-name* **interface** *interface*

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-shaper text {  
        class 3-4095 {  
            match text {  
                interface text  
            }  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>class</i>	Mandatory. The class ID. The range is 3 to 4095.
<i>match-name</i>	Mandatory. Class matching rule name.
<i>interface</i>	Performs a match based on the specified Ethernet interface name. The ingress interface for incoming traffic will be compared with this value.

Default

None.

Usage Guidelines

Use this command to set a match condition for a traffic class based on incoming interface.

If incoming packets ingress through the interface specified by this command, the traffic is a member of this traffic class (provided other match conditions are satisfied).

Note that you are not able to match on both “ip” and “vif” (or “interface”) inside the same traffic shaper configuration.

Use the **set** form of this command to specify an interface to be matched by incoming packets.

Use the **delete** form of this command to remove the match interface.

Use the **show** form of this command to display interface match configuration.

qos-policy traffic-shaper <policy-name> class <class> match <match-name> ip destination

Specifies a match criterion based on IP destination information.

Syntax

```
set qos-policy traffic-shaper policy-name class class match match-name ip destination
{address ipv4 / port port}

delete qos-policy traffic-shaper policy-name class class match match-name ip
destination [address / port]

show qos-policy traffic-shaper policy-name class class match match-name ip
destination
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
  traffic-shaper text {
    class 3-4095 {
      match text {
        ip {
          destination {
            address ipv4
            port text
          }
        }
      }
    }
  }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>class</i>	Mandatory. The class ID. The range is 3 to 4095.
<i>match-name</i>	Mandatory. Class matching rule name.

<i>ipv4</i>	Performs a match based on the destination IP address and prefix.
<i>port</i>	Performs a match based on destination port. The port may be specified as a lower-case name (for example ssh) or as a number. The range for port numbers is 0 to 65535.

Default

If not set, packets are not matched against destination information.

Usage Guidelines

Use this command to define a match condition based on destination address and/or port for a traffic class.

You can match packets based on a destination represented by either or both of IP address and destination port(s).

Note that you are not able to match on both “ip” and “vif” (or “interface”) inside the same traffic shaper configuration.

Use the **set** form of this command to specify a destination to be matched.

Use the **delete** form of this command to remove destination as a match condition.

Use the **show** form of this command to display destination match condition configuration.

qos-policy traffic-shaper <policy-name> class <class> match <match-name> ip dscp <value>

Specifies a match criterion based on the value of the DSCP field.

Syntax

```
set qos-policy traffic-shaper policy-name class class match match-name ip dscp value
delete qos-policy traffic-shaper policy-name class class match match-name ip dscp
show qos-policy traffic-shaper policy-name class class match match-name ip dscp
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
  traffic-shaper text {
    class 3-4095 {
      match text {
        ip {
          dscp text
        }
      }
    }
  }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>class</i>	Mandatory. The class ID. The range is 3 to 4095.
<i>match-name</i>	Mandatory. Class matching rule name.
<i>value</i>	Performs a match based on the specified value. This value is compared with the value in the DSCP field of the ToS byte in the IP header. The DSCP value can be specified as a decimal number (for example, 12), as a hexadecimal number (for example 0x1D), or as a standard name from <i>/etc/iproute2/rt_dsfield</i> (for example, lowdelay).

Default

If not set, packets are not matched against DSCP value.

Usage Guidelines

Use this command to define a match condition based on the Differentiated Services Code Point (DSCP) field.

The DSCP field is a 6-bit field in the Type of Service (ToS) byte of the IP header. It provides a way of marking packets in order to allow classification of traffic into service classes, and traffic conditioning such as metering, policing, and shaping.

Note that you are not able to match on both “ip” and “vif” (or “interface”) inside the same traffic shaper configuration.

Use the **set** form of this command to set a match condition based on DSCP value.

Use the **delete** form of this command to remove DSCP as a match condition.

Use the **show** form of this command to display DSCP value configuration.

qos-policy traffic-shaper <policy-name> class <class> match <match-name> ip protocol <proto>

Specifies a match criterion based on the IP protocol.

Syntax

```
set qos-policy traffic-shaper policy-name class class match match-name ip protocol
proto
delete qos-policy traffic-shaper policy-name class class match match-name ip protocol
show qos-policy traffic-shaper policy-name class class match match-name ip protocol
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
  traffic-shaper text {
    class 3-4095 {
      match text {
        ip {
          protocol text
        }
      }
    }
  }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>class</i>	Mandatory. The class ID. The range is 3 to 4095.
<i>match-name</i>	Mandatory. Class matching rule name.
<i>proto</i>	Performs a match based on the protocol name (for example, icmp) or number, as assigned by the IANA.

Default

If not set, packets are not matched against IP protocol.

Usage Guidelines

Use this command to define a match condition for a traffic class based on protocol.

Note that you are not able to match on both “ip” and “vif” (or “interface”) inside the same traffic shaper configuration.

Use the **set** form of this command to set a match condition based on protocol.

Use the **delete** form of this command to remove protocol value as a match condition.

Use the **show** form of this command to match condition protocol configuration.

qos-policy traffic-shaper <policy-name> class <class> match <match-name> ip source

Specifies a match criterion based on source IP information.

Syntax

```
set qos-policy traffic-shaper policy-name class class match match-name ip source  
{address ipv4 | port port}
```

```
delete qos-policy traffic-shaper policy-name class class match match-name ip source  
{address | port}
```

```
show qos-policy traffic-shaper policy-name class class match match-name ip source
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-shaper text {  
        class 3-4095 {  
            match text {  
                ip {  
                    source {  
                    }  
                }  
            }  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>class</i>	Mandatory. The class ID. The range is 3 to 4095.
<i>match-name</i>	Mandatory. Class matching rule name.
<i>ipv4</i>	The source IP address and prefix to match for this rule.

<i>port</i>	The source port to match for this rule. The port may be specified as a lower-case name (for example ssh) or as a number. The range for port numbers is 0 to 65535.
-------------	--

Default

If not set, packets are not matched against IP source information.

Usage Guidelines

Use this command to define a match condition based on source address and/or port for a traffic class.

You can match packets based on a source represented by either or both of IP address and destination port(s).

Note that you are not able to match on both “ip” and “vif” (or “interface”) inside the same traffic shaper configuration.

Use the **set** form of this command to specify a source to be matched.

Use the **delete** form of this command to remove source as a match condition.

Use the **show** form of this command to display source match condition configuration.

qos-policy traffic-shaper <policy-name> class <class> match <match-name> vif <vlan-id>

Specifies a match criterion based on VLAN ID.

Syntax

```
set qos-policy traffic-shaper policy-name class class match match-name vif vlan-id  
delete qos-policy traffic-shaper policy-name class class match match-name vif  
show qos-policy traffic-shaper policy-name class class match match-name vif
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-shaper text {  
        class 3-4095 {  
            match text {  
                vif 1-4096  
            }  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>class</i>	Mandatory. The class ID. The range is 3 to 4095.
<i>match-name</i>	Mandatory. Class matching rule name.
<i>vlan-id</i>	Performs a match based on VLAN ID. The range is 1 to 4096.

Default

If not set, packets are not matched against VLAN ID.

Usage Guidelines

Use this command to define a match condition based on VLAN ID for a traffic class.

Note that you are not able to match on both “ip” and “vif” (or “interface”) inside the same traffic shaper configuration.

Use the **set** form of this command to specify a VLAN ID to be matched.

Use the **delete** form of this command to remove VLAN ID as a match condition.

Use the **show** form of this command to display VLAN ID match condition configuration.

qos-policy traffic-shaper <policy-name> class <class> priority <priority>

Specifies the priority of a traffic class for allocation of extra bandwidth.

Syntax

```
set qos-policy traffic-shaper policy-name class class priority priority
delete qos-policy traffic-shaper policy-name class class priority
show qos-policy traffic-shaper policy-name class class priority
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
  traffic-shaper text {
    class 3-4095 {
      priority u32
    }
  }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>class</i>	Mandatory. The class ID. The range is 3 to 4095.
<i>priority</i>	The priority with which this traffic class should be allocated extra bandwidth. The range is 1 to 1000, where the higher the number the lower the priority. The default is 1000.

Default

Traffic classes are assigned a priority of 1000.

Usage Guidelines

Use this command to set the priority with which a traffic class is to be awarded extra bandwidth when excess is available.

Use the **set** form of this command to specify priority for a traffic class.

Use the **delete** form of this command to restore the default priority for a traffic class.

Use the **show** form of this command to display traffic class priority configuration.

qos-policy traffic-shaper <policy-name> class <class> queue-limit <limit>

Specifies the maximum queue size for a traffic class.

Syntax

```
set qos-policy traffic-shaper policy-name class class queue-limit limit  
delete qos-policy traffic-shaper policy-name class class queue-limit  
show qos-policy traffic-shaper policy-name class class queue-limit
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-shaper text {  
        class 3-4095 {  
            queue-limit u32  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>class</i>	Mandatory. The class ID. The range is 3 to 4095.
<i>limit</i>	The maximum queue size in packets.

Default

None.

Usage Guidelines

Use this command to set the maximum queue size (in packets) for a traffic class.

Use the **set** form of this command to specify the queue limit.

Use the **delete** form of this command to remove queue limit.

Use the **show** form of this command to display queue limit configuration.

qos-policy traffic-shaper <policy-name> class <class> queue-type <type>

Specifies the type of queuing to use for a traffic class.

Syntax

```
set qos-policy traffic-shaper policy-name class class queue-type type  
delete qos-policy traffic-shaper policy-name class class queue-type  
show qos-policy traffic-shaper policy-name class class queue-type
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-shaper text {  
        class 3-4095 {  
            queue-type [fair-queue|drop-tail|priority|random-detect]  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>class</i>	Mandatory. The class ID. The range is 3 to 4095.
<i>type</i>	The queuing method to use. Supported values are as follows: fair-queue: Uses a Stochastic Fair Queue (SFQ) queue. drop-tail: Uses a First In First Out (FIFO) queue. priority: Sets queue priority based on the Differentiated Services Code Point (DSCP) values in the Type of Service (ToS) byte of the IP header. random-detect: Uses a Random Early Detection (RED) queue.

Default

The default is **fair-queue**.

Usage Guidelines

Use this command to set the type of queuing mechanism to use for a traffic class.

Use the **set** form of this command to specify the queue type.

Use the **delete** form of this command to restore the default queue type.

Use the **show** form of this command to display queue type configuration.

qos-policy traffic-shaper <policy-name> class <class> set-dscp <value>

Rewrites the DSCP field in packets in this traffic class to the specified value.

Syntax

```
set qos-policy traffic-shaper policy-name class class set-dscp value  
delete qos-policy traffic-shaper policy-name class class set-dscp  
show qos-policy traffic-shaper policy-name class class set-dscp
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-shaper text {  
        class 3-4095 {  
            set-dscp text  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>class</i>	Mandatory. The class ID. The range is 3 to 4095.
<i>value</i>	The value to write into the DSCP field of packets in this traffic class. The DSCP value can be specified as a decimal number (for example, 12), as a hexadecimal number (for example 0x1D), or as a standard name from <i>/etc/iproute2/rt_dsfield</i> (for example, lowdelay). By default, the DSCP field is not rewritten.

Default

If not set, the DSCP byte is not rewritten.

Usage Guidelines

Use this command to direct the system to rewrite the Differentiated Services Code Point (DSCP) field of packets in a traffic class to a specific value.

Rewriting the DSCP field can be a way to specify forwarding behavior of a network for packets to allow classification of traffic into service classes, and traffic conditioning such as metering, policing, and shaping.

The following table shows the standard semantics for DSCP values, as specified by RFC 2474.

Table 2-1 RFC 2474 DSCP Values

Binary Value	Configured Value	Drop Rate	Meaning
101 110	46	N/A	Expedited forwarding (EF)
000 000	0	N/A	Default: Best-effort traffic
001 010	10	Low	Assured forwarding (AF) 11
001 100	12	Medium	Assured forwarding (AF) 12
001 110	14	High	Assured forwarding (AF) 13
010 010	18	Low	Assured forwarding (AF) 21
010 100	20	Medium	Assured forwarding (AF) 22
010 110	22	High	Assured forwarding (AF) 23
011 010	26	Low	Assured forwarding (AF) 31
011 100	28	Medium	Assured forwarding (AF) 32
011 110	30	High	Assured forwarding (AF) 33
100 010	34	Low	Assured forwarding (AF) 41
100 100	36	Medium	Assured forwarding (AF) 42
100 110	38	High	Assured forwarding (AF) 43

Use the **set** form of this command to rewrite DSCP values of packets in a traffic class.

Use the **delete** form of this command to stop DSCP values from being rewritten.

Use the **show** form of this command to display DSCP rewrite configuration.

qos-policy traffic-shaper <policy-name> default

Defines a default traffic shaper QoS policy.

Syntax

```
set qos-policy traffic-shaper policy-name default
delete qos-policy traffic-shaper policy-name default
show qos-policy traffic-shaper policy-name default
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
  traffic-shaper text {
    default {
    }
  }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
--------------------	--

Default

None.

Usage Guidelines

Use this command to define a default traffic shaping policy. This policy will be applied to all traffic that does not match any other defined class.

Use the **set** form of this command to create the default class configuration node.

Use the **delete** form of this command to remove the default class configuration node.

Use the **show** form of this command to display the default class configuration node.

qos-policy traffic-shaper <policy-name> default bandwidth

Specifies the base guaranteed bandwidth rate for the default traffic class.

Syntax

```
set qos-policy traffic-shaper policy-name default bandwidth [rate | rate-pct | rate-suffix]  
delete qos-policy traffic-shaper policy-name default bandwidth  
show qos-policy traffic-shaper policy-name default bandwidth
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-shaper text {  
        default {  
            bandwidth text  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>rate</i>	Bandwidth in kbps.
<i>rate-pct</i>	The bandwidth, specified as a percentage of the interface speed. The format is <i>num</i> % (for example, 85%).

<i>rate-suffix</i>	The bandwidth, specified as a number and a scaling suffix (for example, 10mbit). The following suffixes are supported: kbit : Kilobits per second. mbit : Megabits per second. gbit : Gigabits per second. kbps : Kilobytes per second. mbps : Megabytes per second. gbps : Gigabytes per second.
--------------------	---

Default

100% bandwidth usage is available.

Usage Guidelines

Use this command to set a base level of guaranteed bandwidth for the default traffic class.

Use the **set** form of this command to set the available bandwidth for the default traffic class.

Use the **delete** form of this command to restore the default available bandwidth for the default traffic class.

Use the **show** form of this command to display bandwidth configuration for the default traffic class.

qos-policy traffic-shaper <policy-name> default burst

Sets the burst size for the default traffic class.

Syntax

```
set qos-policy traffic-shaper policy-name default burst [num | num-suffix]  
delete qos-policy traffic-shaper policy-name default burst  
show qos-policy traffic-shaper policy-name default burst
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-shaper text {  
        default {  
            burst text  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>num</i>	Burst size in bytes.
<i>num-suffix</i>	The burst size, specified as a number and a scaling suffix (for example, 10mb). The following suffixes are supported: kb : Kilobytes. mb : Megabytes. gb : Gigabytes.

Default

The burst size is 15kb.

Usage Guidelines

Use this command to set the burst size for the default traffic class. This is the maximum amount of traffic that may be sent at a given time.

Use the **set** form of this command to specify the burst size for the default traffic class.

Use the **delete** form of this command to restore the default burst size for the default traffic class.

Use the **show** form of this command to display burst size configuration for the default traffic class.

qos-policy traffic-shaper <policy-name> default ceiling

Sets a bandwidth ceiling for the default traffic class.

Syntax

```
set qos-policy traffic-shaper policy-name default ceiling [rate | rate-pct | rate-suffix]  
delete qos-policy traffic-shaper policy-name default ceiling  
show qos-policy traffic-shaper policy-name default ceiling
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-shaper text {  
        default {  
            ceiling text  
        }  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>rate</i>	The limit in kbps.
<i>rate-pct</i>	The bandwidth, specified as a percentage of the overall bandwidth rate. The format is <i>num</i> % (for example, 85%).
<i>rate-suffix</i>	The bandwidth, specified as a number and a scaling suffix (for example, 10mbit). The following suffixes are supported: kbit : Kilobits per second. mbit : Megabits per second. gbit : Gigabits per second.

Default

The default is 100%.

Usage Guidelines

Use this command to set the maximum amount of bandwidth the default traffic class may consume when excess bandwidth is available.

Use the **set** form of this command to set the bandwidth ceiling for the default traffic class.

Use the **delete** form of this command to restore the default bandwidth ceiling for the default traffic class.

Use the **show** form of this command to display bandwidth ceiling configuration for the default traffic class.

qos-policy traffic-shaper <policy-name> default priority <priority>

Specifies the priority of the default traffic class for allocation of extra bandwidth.

Syntax

```
set qos-policy traffic-shaper policy-name default priority priority
delete qos-policy traffic-shaper policy-name default priority
show qos-policy traffic-shaper policy-name default priority
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
  traffic-shaper text {
    default {
      priority 0-7
    }
  }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>priority</i>	The priority with which this traffic class should be allocated extra bandwidth. The range is 0 to 7, where the higher the number the lower the priority. The default is 0.

Default

The default priority is assigned a value of 0.

Usage Guidelines

Use this command to set the priority with which the default traffic class is to be awarded extra bandwidth when excess is available.

Use the **set** form of this command to specify priority for the default traffic class.

Use the **delete** form of this command to restore the default priority for the default traffic class.

Use the **show** form of this command to display priority configuration for the default traffic class.

qos-policy traffic-shaper <policy-name> default queue-limit <limit>

Specifies the maximum queue size for the default traffic class.

Syntax

```
set qos-policy traffic-shaper policy-name default queue-limit limit
delete qos-policy traffic-shaper policy-name default queue-limit
show qos-policy traffic-shaper policy-name default queue-limit
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
  traffic-shaper text {
    default {
      queue-limit u32
    }
  }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>limit</i>	The maximum queue size in packets.

Default

None.

Usage Guidelines

Use this command to set the maximum queue size (in packets) for the default class.

Use the **set** form of this command to specify the queue limit.

Use the **delete** form of this command to remove queue limit.

Use the **show** form of this command to display queue limit configuration.

qos-policy traffic-shaper <policy-name> default queue-type <type>

Specifies the type of queuing to use for the default traffic class.

Syntax

```
set qos-policy traffic-shaper policy-name default queue-type type
delete qos-policy traffic-shaper policy-name default queue-type
show qos-policy traffic-shaper policy-name default queue-type
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
  traffic-shaper text {
    default {
      queue-type [fair-queue|drop-tail|priority|random-detect]
    }
  }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>type</i>	The queuing method to use. Supported values are as follows: fair-queue: Uses a Stochastic Fair Queue (SFQ) queue. drop-tail: Uses a First In First Out (FIFO) queue. priority: Sets queue priority based on the Differentiated Services Code Point (DSCP) values in the Type of Service (ToS) byte of the IP header. random-detect: Uses a Random Early Detection (RED) queue.

Default

The default is **fair-queue**.

Usage Guidelines

Use this command to set the type of queuing mechanism to use for the default traffic class.

Use the **set** form of this command to specify the queue type.

Use the **delete** form of this command to restore the default queue type.

Use the **show** form of this command to display queue type configuration.

qos-policy traffic-shaper <policy-name> default set-dscp <value>

Rewrites the DSCP field in packets in the default traffic class to the specified value.

Syntax

```
set qos-policy traffic-shaper policy-name default set-dscp value
delete qos-policy traffic-shaper policy-name default set-dscp
show qos-policy traffic-shaper policy-name default set-dscp
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {
  traffic-shaper text {
    default {
      set-dscp text
    }
  }
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>value</i>	The value to write into the DSCP field of packets in the default traffic class. The DSCP value can be specified as a decimal number (for example, 12), as a hexadecimal number (for example 0x1D), or as a standard name from <code>/etc/iproute2/rt_dsfield</code> (for example, lowdelay). By default, the DSCP field is not rewritten.

Default

If not set, the DSCP byte is not rewritten.

Usage Guidelines

Use this command to direct the system to rewrite the Differentiated Services Code Point (DSCP) field of packets in the default traffic class to a specific value.

Rewriting the DSCP field can be a way to specify forwarding behavior of a network for packets to allow classification of traffic into service classes, and traffic conditioning such as metering, policing, and shaping.

The following table shows the standard semantics for DSCP values, as specified by RFC 2474.

Table 2-2 RFC 2474 DSCP Values

Binary Value	Configured Value	Drop Rate	Meaning
101 110	46	N/A	Expedited forwarding (EF)
000 000	0	N/A	Default: Best-effort traffic
001 010	10	Low	Assured forwarding (AF) 11
001 100	12	Medium	Assured forwarding (AF) 12
001 110	14	High	Assured forwarding (AF) 13
010 010	18	Low	Assured forwarding (AF) 21
010 100	20	Medium	Assured forwarding (AF) 22
010 110	22	High	Assured forwarding (AF) 23
011 010	26	Low	Assured forwarding (AF) 31
011 100	28	Medium	Assured forwarding (AF) 32
011 110	30	High	Assured forwarding (AF) 33
100 010	34	Low	Assured forwarding (AF) 41
100 100	36	Medium	Assured forwarding (AF) 42
100 110	38	High	Assured forwarding (AF) 43

Use the **set** form of this command to rewrite DSCP values of packets in the default traffic class.

Use the **delete** form of this command to stop DSCP values in the default traffic class from being rewritten.

Use the **show** form of this command to display DSCP rewrite configuration for the default traffic class.

qos-policy traffic-shaper <policy-name> description <desc>

Specifies a description for a traffic shaper QoS policy.

Syntax

```
set qos-policy traffic-shaper policy-name description desc  
delete qos-policy traffic-shaper policy-name description  
show qos-policy traffic-shaper policy-name description
```

Command Mode

Configuration mode.

Configuration Statement

```
qos-policy {  
    traffic-shaper text {  
        description text  
    }  
}
```

Parameters

<i>policy-name</i>	Mandatory. The name of the traffic shaping policy.
<i>desc</i>	The description for this traffic shaper policy.

Default

None.

Usage Guidelines

Use this command to record a description for a traffic shaper policy.

Use the **set** form of this command to specify a description for a traffic shaper policy.

Use the **delete** form of this command to remove a description from a traffic shaper policy.

Use the **show** form of this command to display description configuration for a traffic shaper policy.

show queueing

Displays current QoS policies.

Syntax

```
show queueing [interface-type [interface]]
```

Command Mode

Operational mode.

Parameters

<i>interface-type</i>	Optional. The type of interface whose QoS policies you wish to see. Possible values include ethernet , adsl , and serial .
<i>interface</i>	Optional. The specific interface (e.g. eth0).

Default

None.

Usage Guidelines

Use this command to display current QoS policies.

Examples

Example 2-2 shows all QoS policies.

Example 2-2 “show queueing”: Displaying all QoS policies.

```
vyatta@vyatta:~$ show queueing
Output queues:
Interface  Qos-Policy          Sent    Dropped  Overlimit
eth0       traffic-shaper      99277   0         0

vyatta@vyatta:~$
```

Example 2-2 shows specific QoS policies.

Example 2-3 “show queueing ethernet eth0”: Displaying QoS policies on a specific interface.

```
vyatta@vyatta:~$ show queueing ethernet eth0
eth0 Output queue:
Class      Qos-Policy      Sent      Dropped      Overlimit
1          traffic-shaper   106384     0             0
  8001     fair-queue       48286     0             0
  8002     fair-queue       58098     0             0
  8003     drop-tail        0         0             0
vyatta@vyatta:~$
```

Glossary of Acronyms

ACL	access control list
ADSL	Asymmetric Digital Subscriber Line
AS	autonomous system
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
BIOS	Basic Input Output System
BPDU	Bridge Protocol Data Unit
CA	certificate authority
CHAP	Challenge Handshake Authentication Protocol
CLI	command-line interface
DDNS	dynamic DNS
DHCP	Dynamic Host Configuration Protocol
DLCI	data-link connection identifier
DMI	desktop management interface
DMZ	demilitarized zone
DNS	Domain Name System
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
eBGP	external BGP
EGP	Exterior Gateway Protocol

ECMP	equal-cost multipath
ESP	Encapsulating Security Payload
FIB	Forwarding Information Base
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HDLC	High-Level Data Link Control
I/O	Input/Output
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IGP	Interior Gateway Protocol
IPS	Intrusion Protection System
IKE	Internet Key Exchange
IP	Internet Protocol
IPOA	IP over ATM
IPsec	IP security
IPv4	IP Version 4
IPv6	IP Version 6
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAN	local area network
MAC	medium access control
MIB	Management Information Base
MLPPP	multilink PPP
MRRU	maximum received reconstructed unit
MTU	maximum transmission unit

NAT	Network Address Translation
ND	Neighbor Discovery
NIC	network interface card
NTP	Network Time Protocol
OSPF	Open Shortest Path First
OSPFv2	OSPF Version 2
OSPFv3	OSPF Version 3
PAM	Pluggable Authentication Module
PAP	Password Authentication Protocol
PCI	peripheral component interconnect
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PVC	permanent virtual circuit
QoS	quality of service
RADIUS	Remote Authentication Dial-In User Service
RIB	Routing Information Base
RIP	Routing Information Protocol
RIPng	RIP next generation
Rx	receive
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SSH	Secure Shell
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus

TCP	Transmission Control Protocol
ToS	Type of Service
Tx	transmit
UDP	User Datagram Protocol
vif	virtual interface
VLAN	virtual LAN
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	wide area network