BROCADE

CONFIGURATION GUIDE

Brocade Vyatta Network OS Policy-based Routing Configuration Guide, 5.2R1

Supporting Brocade 5600 vRouter, VNF Platform, and Distributed Services Platform

53-1004733-01
24 October 2016

Contents

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE

A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION

An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used to highlight specific words or phrases.

Format	Description
bold text	Identifies command names.
	Identifies keywords and operands.
	Identifies the names of GUI elements.
	Identifies text to enter in the GUI.
italic text	Identifies emphasis.
	Identifies variables.
	Identifies document titles.
`Courier font`	Identifies CLI output.
	Identifies command syntax examples.

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
value	In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, **--show** WWN.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options. In Fibre Channel products, square brackets may be used instead for this purpose.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Brocade resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

White papers, data sheets, and the most recent versions of Brocade software and hardware manuals are available at www.brocade.com. Product documentation for all supported releases is available to registered users at MyBrocade.
Click the **Support** tab and select **Document Library** to access documentation on MyBrocade or www.brocade.com You can locate documentation by product or by operating system.

Release notes are bundled with software downloads on MyBrocade. Links to software downloads are available on the MyBrocade landing page and in the Document Library.

Document feedback

Quality is our first concern at Brocade, and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can provide feedback in two ways:

- Through the online feedback form in the HTML documents posted on www.brocade.com
- By sending your feedback to documentation@brocade.com

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers should contact their OEM/solution provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to www.brocade.com and select **Support**.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone	E-mail
Preferred method of contact for non-urgent issues: • Case management through the MyBrocade portal. • Quick Access links to Knowledge Base, Community, Document Library, Software Downloads and Licensing tools	Required for Sev 1-Critical and Sev 2-High issues: • Continental US: 1-800-752-8061 • Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33) • Toll-free numbers are available in many countries. • For areas unable to access a toll-free number: +1-408-333-6061	support@brocade.com Please include: • Problem summary • Serial number • Installation details • Environment description

Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/solution provider, contact your OEM/solution provider for all of your product support needs.

- OEM/solution providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/solution provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/solution provider.

About This Guide

This guide describes how to define and configure routing policies on Brocade products that run on the Brocade Vyatta Network OS (referred to as a virtual router, vRouter, or router in the guide).

Policy-based Routing

Introduction

Policy-based routing (PBR) enables you to use IP traffic rules to classify traffic based on its attributes and apply processing differentially according to the classification, and to selectively route IP packets, for example, to an alternate next hop. PBR on the Brocade vRouter is supported just on incoming Layer 3 and Layer 4 traffic.

All packets received on an interface are considered for policy-based routing provided that interface is assigned a routing policy.

When no routing policies are applied, routing decisions are made by using the default (main) routing table (Table 254) of the system.

PBR policies can be applied to data plane interfaces for inbound traffic, but not to loopback, tunnel, bridge, OpenVPN, VTI, and IP unnumbered interfaces.

On the Brocade vRouter, you cannot apply policy based routing to locally generated packets.

Defining a routing policy

The routing policy classifies traffic and specifies the handling that should take place for different classes. This classification and handling are accomplished by using a set of policy rules.

Rules are configured with match criteria that include an extensive set of attributes—including protocol, source and destination addresses and ports, fragmentation, ICMP or ICMPv6 type, and TCP flags. You can also preconfigure groups of addresses, ports, and networks and refer to these groups in policy rules.

The routing policy must be applied to an interface for the policy to be effective.

To implement policy-based routing, perform the following steps:

1. Define the policy rules.
2. Attach the policy to an ingress interface.
3. Create a route in a PBR table other than Table 254.

NOTE
Table 254 is also known as the main table or default table.

Routing policy rules

Packets that match the PBR rule criteria do one of the following:

- They are dropped (if the **drop** action is set).
- They are routed by using a specific PBR routing table.

Packets that match the rule parameters are considered for policy-based routing. As many as 9,999 rules in a policy are supported. If no match criteria are specified, all packets are routed according to the default Table 254.

The packets that do not match any policy rule are routed according to the routes in the main table.

NOTE
You can configure rules to match IPv4 ICMP, IPv6 ICMP, IPv6 routing header, or TCP without specifying the respective protocol, provided that a protocol specific match option is present. For example TCP flags, ICMP type.

Routing policy rules are executed in numeric sequence, from lowest to highest. You can renumber rules by using the **rename** command in configuration mode (refer to *Brocade Vyatta Network OS Basic System Configuration Guide*).

NOTE
To avoid having to renumber routing policy rules, a good practice is to number rules in increments of 10. This increment allows room for the insertion of new rules within the policy.

PBR behavior

Routes remain persistent in the controller. If the data plane goes down, and up, the routes are automatically re-established without the need for reconfiguration.

PBR rules can be changed dynamically and does not require the rebinding of the PBR policy to an interface.

Configuration for VLAN-based classification, virtual interface (vif), MAC address, packet mangling, and so on, are not supported.

The controller automatically continuously resyncs the route information to the data plane.

Multiple PBR policies can be applied to an interface. For best results, we recommend that these policies are unique.

Packet forwarding path

When enabled, PBR processes incoming packets after packet validation and firewall action. Packets received by the data plane ingress interfaces for transmission to the egress interface follow the forwarding path listed below. There is only a single Virtual Routing and Forwarding (VRF) instance for PBR.

1. Packet validation and reassembly
2. Firewall
3. DNAT
4. PBR classification, route table ID determination
5. SNAT
6. Firewall
7. QoS
8. Transmit out of an egress interface

Configuration Examples

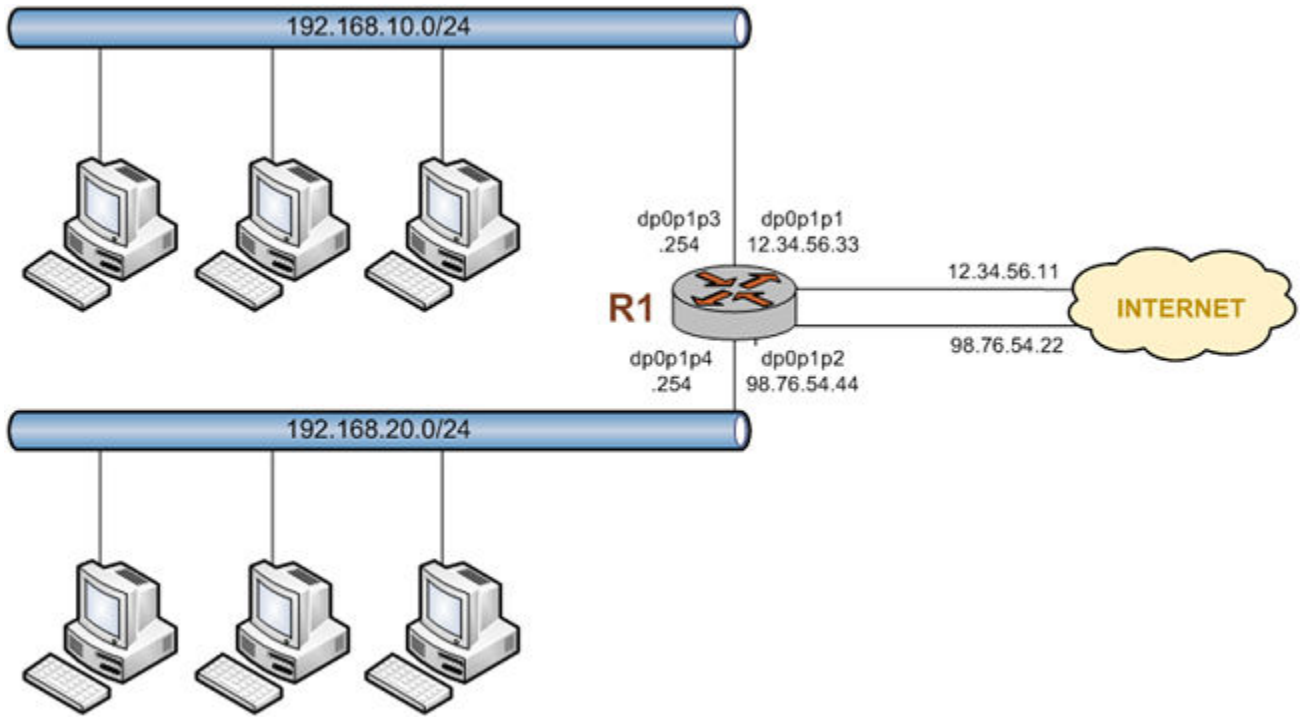
PBR routing example

The following figure shows a simple site that uses PBR on the Brocade vRouter (R1) to route traffic from two different internal subnets to two Internet links.

The following conditions apply to this scenario:

- All Internet-bound traffic from subnet 192.168.10.0/24 is routed out interface dp0p1p1.
- All Internet-bound traffic from subnet 192.168.20.0/24 is routed out interface dp0p1p2.

FIGURE 1 Routing using PBR



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

TABLE 1 Routing using PBR

Step	Command

Create Rule 10 and specify the destination address to match. In this case, any destination address is a match.	`vyatta@R1# set policy route pbr myroute rule 10 address-family ipv4`
	`vyatta@R1# set policy route pbr myroute rule 10 action accept`
	
	`vyatta@R1# set policy route pbr myroute rule 10 destination address 0.0.0.0/0`

TABLE 1 Routing using PBR (continued)

Step	Command
Specify the source address to match. In this case, any address on subnet 192.168.10.0/24 is a match.	`vyatta@R1# set policy route pbr myroute rule 10 source address 192.168.10.0/24`
Specify that all matching packets use alternate routing table 1.	`vyatta@R1# set policy route pbr myroute rule 10 table 1`

Create rule 20 and specify the destination address to match. In this case, any destination address is a match.	`vyatta@R1# set policy route pbr myroute rule 20 address-family ipv4`
	`vyatta@R1# set policy route pbr myroute rule 20 action accept`
	`vyatta@R1# set policy route pbr myroute rule 20 destination address 0.0.0.0/0`

Specify the source address to match. In this case, any address on subnet 192.168.20.0/24 is a match.	`vyatta@R1# set policy route pbr myroute rule 20 source address 192.168.20.0/24`
Specify that all matching packets use alternate routing table 2.	`vyatta@R1# set policy route pbr myroute rule 20 table 2`
Commit the changes.	`vyatta@R1# commit`

Show the policy-based routing configuration.	`vyatta@R1# show policy route`
	`policy {`
	`  route {`
	`  pbr myroute {`
	`  rule 10 {`
	`  action accept`
	`  address-family ipv4`
	`  destination {`
	`  address 0.0.0.0/0`
	`  }`
	`  source {`
	`  address 192.168.10.0/24`
	`  }`
	`  table 1`
	`  }`
	`  rule 20 {`
	`  action accept`
	`  address-family ipv4`
	`  destination {`
	`  address 0.0.0.0/0`
	`  }`
	`  source {`
	`  address 192.168.20.0/24`
	`  }`
	`  table 2`
	`  }`
	`  }`
	`  }`
	`}`

TABLE 1 Routing using PBR (continued)

Step	Command
Create the alternative routing table 1.	`vyatta@R1# set protocols static table 1 route 0.0.0.0/0 next-hop 12.34.56.11`
Create the alternative routing table 2.	`vyatta@R1# set protocols static table 2 route 98.76.54.0/24 next-hop 98.76.54.22`
Commit the change.	`vyatta@R1# commit`

Show the alternate routing table configuration.	`vyatta@R1# show protocols static`
	
	`static {`
	`  table 1 {`
	`  route 12.34.56.0/24 {`
	`  next-hop 12.34.56.11`
	`  }`
	`  }`
	`  table 2 {`
	`  route 98.76.54.0/24 {`
	`  next-hop 98.76.54.22`
	`  }`
	`  }`
	`  }`

Apply the IP addresses to the corresponding data plane interfaces.	`vyatta@R1# set interfaces dataplane dp0p1p1 address 12.34.56.33/24`
	`vyatta@R1# set interfaces dataplane dp0p1p2 address 98.76.54.44/24`
	`vyatta@R1# set interfaces dataplane dp0p1p3 address 192.168.10.254/24`
	`vyatta@R1# set interfaces dataplane dp0p1p4 address 192.168.20.254/24`

Apply the policy route with dp0p1p3, and dp0p1p4 interfaces	`vyatta@R1# set interfaces dataplane dp0p1p3 policy route pbr myroute` `vyatta@R1# set interfaces dataplane dp0p1p4 policy route pbr myroute`

Show the data plane interface configuration.	`vyatta@R1# show interfaces dataplane`
	
	`dataplane dp0p1p1 {`
	`  address 0.0.0.0/0`
	`}`
	`dataplane dp0p1p2 {`
	`  address 98.76.54.44/24`
	`}`
	`dataplane dp0p1p3 {`
	`  address 192.168.10.254/24`
	`  policy {`
	`  route {`
	`  pbr myroute`
	`  }`
	`  }`
	`}`
	`dataplane dp0p1p4 {`
	`  address 192.168.20.254/24`
	`  policy {`
	`  route {`
	`  pbr myroute`
	`  }`
	`  }`
	`}`

Binding interfaces to PBR tables

To configure an interface-based static route in a policy route table, perform the following steps:

TABLE 2 Applying a policy route to an interface

Step	Command
Configure the interface route for the interface.	`vyatta@R1# set protocols static table 10 interface-route 192.168.20.254/24 nexthop-interface dp0p256p1 distance 25`

View the configuration.	`vyatta@vyatta:~$ show protocols`
	
	`protocols {`
	`  static {`
	`  table 10 {`
	`  interface-route 192.168.20.254/24 {`
	`  nexthop-interface dp0p256p1 {`
	`  distance 25`
	`  }`
	`  }`
	`  }`
	`  }`
	`}`

Commit the change.	`vyatta@R1# commit`

Policy-based Routing Commands

clear policy

Clears the statistics for route policies.

Syntax

clear policy

Modes

Operational mode

Usage Guidelines

Use this command to clear the statistics for policy-based routing.

interfaces dataplane <interface> policy route pbr <name>

Applies an IP routing policy to inbound traffic on an interface.

Syntax

set interfaces dataplane *interface* **policy route pbr** *name*

delete interfaces dataplane *interface* **policy route pbr** [*name*]

show interfaces *interface* **policy route pbr** [*name*]

Parameters

interface

The type of interface. For detailed keywords and arguments that can be specified as interface types, refer to Supported Interface Types on page 57.

policy route pbr *name*

An IP routing policy.

Modes

Configuration mode

Configuration Statement

```
interfaces dataplane interface {
    policy {
        route {
            pbr name
        }
    }
}
```

Usage Guidelines

A routing policy has no effect on traffic traversing the system until it has been applied to an interface.

You must specify the address-family, action, and table leaf nodes to configure a routing policy. It is recommended to use the **delete policy route pbr** *name* **rule** *number* command to delete a routing policy.

NOTE

Policy-based routing policies can be applied to data plane interfaces, but not on loopback, tunnel, bridge, OpenVPN, or VTI interfaces.

To use the policy-based routing feature, you must define a routing policy by using the **set policy route pbr** *name* **rule** *number* command, and then apply the routing policy to interfaces by using a statement like this one. Once applied, the rule set acts as a packet filter.

Use the **set** form of this command to apply an IP routing policy to an interface.

Use the **delete** form of this command to remove an IP routing policy from an interface.

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

policy route pbr <name> rule <rule-number>

Defines an IP routing policy rule.

Syntax

set policy route pbr *name* **rule** *rule-number*

delete policy route pbr *name* **rule** [*rule-number*]

show policy route pbr *name* **rule**

Parameters

name

The name of an IP routing policy.

rule-number

The numeric identifier of the rule. Rule numbers determine the order in which rules are executed. Each rule must have a unique rule number. The numbers range from 1 through 9999.
You can define multiple rules by creating more than one **rule** configuration node.

Modes

Configuration mode

Configuration Statement

```
policy {
    route {
        pbr name {
                rule rule-number
            }
        }
    }
```

Usage Guidelines

A policy identifies traffic that matches parameters and specifies which routing table to use. The table defines the route for a packet to take. A routing policy is a named collection of as many as 9,999 packet-classification rules. When applied to an interface, the policy rule classifies incoming traffic.

You must specify the address-family, action, and table leaf nodes to configure a routing policy. It is recommended to use the **delete policy route pbr** *name* **rule** *number* command to delete a routing policy.

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

Use the **delete** form of this command to delete an existing IP routing policy.

Use the **show** form of this command to display a rule.

policy route pbr <name> rule <rule-number> action <action>

Defines the action for an IP routing policy rule.

Syntax

set policy route pbr *name* **rule** *rule-number* **action** { **drop** | **accept** }

delete policy route pbr *name* **rule** *rule-number* **action** [**drop** | **accept**]

show policy route pbr *name* **rule** *rule-number* **action**

Parameters

name

The name of an IP routing policy.

rule-number

The numeric identifier of the rule. Rule numbers determine the order in which rules are executed. Each rule must have a unique rule number. The numbers range from 1 through 9999.
You can define multiple rules by creating more than one **rule** configuration node.

action

The action for an IP routing policy. The actions for an IP routing policy are **accept** and **drop**.

accept

Accepts the packet.

drop

Drops the packet silently.

Modes

Configuration mode

Configuration Statement

```
policy {
    route {
        pbr name {
               rule rule-number {
                    action accept
                    action drop
                }
            }
        }
    }
```

Usage Guidelines

You must specify the address-family, action, and table leaf nodes to configure a routing policy. It is recommended to use the **delete policy route pbr** *name* **rule** *number* command to delete a routing policy.

If a rule does not explicitly drop a packet in the action, the PBR action is to accept the packet, which causes it to be sent to the specified alternate routing table for lookup and forwarding.

An applied policy can only be deleted after first removing it from an assigned interface.

Use the **set** form of this command to set the action for a rule.

Use the **delete** form of this command to remove the action for a rule.

Use the **show** form of this command to display a rule within an IP routing policy.

policy route pbr <name> rule <rule-number> address-family <address-family>

Defines the address family for an IP routing policy rule.

Syntax

set policy route pbr *name* **rule** *rule-number* **address-family** [**ipv4** | **ipv6**]

delete policy route pbr *name* **rule** *rule-number* **address-family** [**ipv4** | **ipv6**]

show policy route pbr *name* **rule** *rule-number* **address-family**

Parameters

name

The name of an IP routing policy. The policy name must be unique and must not be used with other PBR policy commands.

rule-number

The numeric identifier of the rule. Rule numbers determine the order in which rules are executed. Each rule must have a unique rule number. The numbers range from 1 through 9999.
You can define multiple rules by creating more than one **rule** configuration node.

address-family

The address-family for an IP routing policy rule. The address-family for an IP routing policy are **ipv4** and **ipv6**.

Modes

Configuration mode

Configuration Statement

```
policy {
    route {
        pbr name {
                rule rule-number {
                    address-family ipv4
                    address-family ipv6
                }
            }
        }
    }
```

Usage Guidelines

You must specify the address-family, action, and table leaf nodes to configure a routing policy. It is recommended to use the **delete policy route pbr** *name* **rule** *number* command to delete a routing policy.

Use the **set** form of this command to define the address family and routing protocol for an IP routing policy rule.

Use the **delete** form of this command to remove the address family and routing protocol for an IP routing policy rule.

Use the **show** form of this command to view the address family and routing protocol for an IP routing policy rule.

policy route pbr <name> rule <rule-number> description <description>

Provides a brief description for an IP routing policy rule.

Syntax

set policy route pbr *name* **rule** *rule-number* **description** *description*

delete policy route pbr *name* **rule** *rule-number* **description**

show policy route pbr *name* **rule** *rule-number* **description**

Parameters

name

The name of an IP routing policy.

rule-number

The numeric identifier of the rule. Rule numbers determine the order in which rules are executed. Each rule must have a unique rule number. The numbers range from 1 through 9999.

You can define multiple rules by creating more than one **rule** configuration node.

description

A brief description for the rule. If the description contains spaces, it must be enclosed in double quotation marks (").

Modes

Configuration mode

Configuration Statement

```
policy {
    route {
        pbr name {
                rule rule-number {
                    description description
                }
            }
        }
    }
```

Usage Guidelines

You must specify the address-family, action, and table leaf nodes to configure a routing policy. It is recommended to use the **delete policy route pbr** *name* **rule** *number* command to delete a routing policy.

Use the **set** form of this command to provide a description for an IP routing policy rule.

Use the **delete** form of this command to remove a description for an IP routing policy rule.

Use the **show** form of this command to display a description for an IP routing policy rule.

policy route pbr <name> rule <rule-number> destination <destination>

Defines the destination address for an IP routing policy rule.

Syntax

set policy route pbr *name* **rule** *rule-number* **destination** { **address** *address* | **mac-address** *mac-address* | **port** *port* }

delete policy route pbr *name* **rule** *rule-number* **destination** [**address** | **mac-address** | **port**]

show policy route pbr *name* **rule** *rule-number* **destination**

Parameters

name

The name of an IP routing policy.

rule-number

The numeric identifier of a policy rule. Rule numbers determine the order in which rules are processed. Each rule must have a unique rule number. The number ranges from 1 through 9999.
You can define multiple rules by creating more than one **rule** configuration node.

destination

The destination address for an IP routing policy rule. The destination address can be any of the following parameters.

address

Specifies an address to match. Address formats are as follows:
address-group name: An address group that is configured with a list of addresses.
ip-address: An IPv4 address.
ip-address/prefix: An IPv4 network address, where 0.0.0.0/0 matches any network.
!*ip-address*: All IP addresses except the specified IPv4 address.
!*ip-address/prefix*: All IP addresses except the specified IPv4 network address.
ipv6-address: An IPv6 address; for example, fe80::20c:29fe:fe47:f89.
ip-address/prefix: An IPv6 network address, where ::/0 matches any network; for example, fe80::20c:29fe:fe47:f88/64.
!*ipv6-address*: All IP addresses except the specified IPv6 address.
!*ip-address/prefix*: All IP addresses except the specified IPv6 network address.

mac-address

Specifies a media access control (MAC) address to match. The address format is six 8-bit numbers, separated by colons, in hexadecimal; for example, 00:0a:59:9a:f2:ba.

NOTE
For policy based routing, the usefulness of this parameter is limited because the MAC address is on a local interface.

port

Specifies a port to match. Port formats are as follows:

- *port-group name*: A port group that is configured with a list of ports.
- *port name*: A port name as shown in `/etc/services`, for example, http.
- *1-65535*: A port number in the range from 1 through 65535.
- *start-end*: A range of port numbers, for example, 1001-1005.

A packet is considered a match if it matches any port name or number specified in the group. Only one port group may be specified. The port group must already be defined.

destination

Specifies a media access control (MAC) address to match. The address format is six 8-bit numbers, separated by colons, in hexadecimal; for example, 00:0a:59:9a:f2:ba.

NOTE

For policy-based routing, the usefulness of this parameter is limited because the MAC address is on a local interface.

Modes

Configuration mode

Configuration Statement

```
policy {
    route {
        pbr name {
                rule rule-number {
                    destination {
                        address address
                        mac-address address
                        port port
                    }
                }
            }
        }
    }
```

Usage Guidelines

This match criterion specifies a group of addresses, ports, or networks for packet destination address.

A packet is considered a match for an address, a network, or a port group if it matches any host IP address, network address, or port name or number, respectively, in the group. However, if more than one group is specified, the packet must be a match for both groups to be considered a match. For example, if both an address group and a port group are specified, the destination of the packet must match at least one item in the address group and at least one item in the port group.

An address group may be specified with a port group.

If both an address and a port are specified, the packet is considered a match only if both the address and the port match.

Use the **set** form of this command to create or modify a rule within an IP routing policy.

Use the **delete** form of this command to remove a rule from an IP routing policy.

Use the **show** form of this command to display a rule within an IP routing policy.

policy route pbr <name> rule <rule-number> disable

Disables a routing policy rule.

Syntax

set policy route pbr *name* **rule** *rule-number* **disable**

delete policy route pbr *name* **rule** *rule-number* **disable**

show policy route pbr *name* **rule** *rule-number*

Command Default

The rule is enabled.

Parameters

name

The name of an IP routing policy.

rule-number

The numeric identifier of the rule. Rule numbers determine the order in which rules are executed. Each rule must have a unique rule number. The numbers range from 1 through 9999.
You can define multiple rules by creating more than one **rule** configuration node.

Modes

Configuration mode

Configuration Statement

```
policy {
    route {
        pbr name {
                rule rule-number {
                    disable
                }
            }
        }
    }
```

Usage Guidelines

You must specify the address-family, action, and table leaf nodes to configure a routing policy. It is recommended to use the **delete policy route pbr** *name* **rule** *number* command to delete a routing policy.

Use the **set** form of this command to disable a routing policy rule.

Use the **delete** form of this command to re-enable a rule.

Use the **show** form of this command to display a routing policy rule.

policy route pbr <name> rule <rule-number> icmp <icmp>

Creates a routing policy rule to match Internet Control Message Protocol (ICMP) packets.

Syntax

set policy route pbr *name* **rule** *rule-number* **icmp** { **type** *type-number* [**code** *code-number*] | **name** *name* }

delete policy route pbr *name* **rule** *rule-number* **icmp** [**type** [*number* **code**] | **name**]

show policy route pbr *name* **rule** *rule-number* **icmp** [**type** [*number* **code**] | **name**]

Command Default

The rule is enabled.

Parameters

name

Name of a PBR group. The PBR group must be unique and must not be used with other PBR policy commands.

rule-number

The numeric identifier of the rule. Rule numbers determine the order in which rules are executed. Each rule must have a unique rule number. The numbers range from 1 through 9999.
You can define multiple rules by creating more than one **rule** configuration node.

icmp

The ICMP packet that matches the routing policy rule. The ICMP packet identifiers are **type**, **code**, and **name**.

type-number

An IPv4 ICMP type number. Values range from 0 through 255.

code-number

An IPv4 ICMP code number. Values range from 0 through 255.

name

Specifies matching for ICMP type names. The default name is **any**.

Modes

Configuration mode

Configuration Statement

```
policy {
    route {
        pbr name {
            rule rule-number {
                icmp {
                    type type-number {
                        code code-number
                    }
                    name name
                }
            }
        }
```

```
    }
}
```

Usage Guidelines

You must specify the address-family, action, and table leaf nodes to configure a routing policy. It is recommended to use the **delete policy route pbr** *name* **rule** *number* command to delete a routing policy.

> NOTE
> As ICMP is an IPv4 protocol and ICMPv6 is an IPv6 protocol, configuring a routing policy rule to match ICMPv6 packets when address-family ipv4 is configured or vice versa are unlikely to be useful and probably will not behave as you are expecting it to behave.

You can specify an ICMP type code by type; for example, 128 (echo-request), or by a type and code pair; for example, type 1 and code 4 (port-unreachable). Alternatively, you can specify the ICMP type code explicitly by using the **name** *name* parameter ; for example, `name echo-request`.

For a list of ICMP codes and types, refer to ICMP Types on page 53.

Use the **set** form of this command to create a rule to match ICMP packets.

Use the **delete** form of this command to delete a rule that matches ICMP packets.

Use the **show** form of this command to display a rule that matches ICMP packets.

policy route pbr <name> rule <rule-number> icmpv6 <icmpv6>

Creates a routing policy rule to match Internet Control Message Protocol (ICMP) IPv6 packets.

Syntax

set policy route pbr *name* **rule** *rule-number* **icmpv6** { **type** *type-number* [**code** *code-number*] | **name** *name* }

delete policy route pbr *name* **rule** *rule-number* **icmpv6** [**type** [*number* **code**] | **name**]

show policy route pbr *name* **rule** *rule-number* **icmpv6** [**type** [*number* **code**] | **name**]

Command Default

The rule is enabled.

Parameters

name

Name of a PBR group. The PBR group must be unique and must not be used with other PBR policy commands.

rule-number

The numeric identifier of the rule. Rule numbers determine the order in which rules are executed. Each rule must have a unique rule number. The numbers range from 1 through 9999.
You can define multiple rules by creating more than one **rule** configuration node.

icmpv6

The ICMPv6 packet that matches the routing policy rule. The ICMPv6 packet identifiers are **type**, **code**, and **name**.

type-number

An IPv6 ICMP type number. Values range from 0 through 255.

code-number

An IPv6 ICMP code number. Values range from 0 through 255.

name

Specifies matching for ICMPv6 type names. The default name is **any**.

Modes

Configuration mode

Configuration Statement

```
policy {
    route {
        pbr name {
            rule rule-number {
                icmpv6 {
                    type type-number {
                        code code-number
                    }
                    name name
                }
            }
        }
```

```
    }
}
```

Usage Guidelines

You must specify the address-family, action, and table leaf nodes to configure a routing policy. It is recommended to use the **delete policy route pbr** *name* **rule** *number* command to delete a routing policy.

> NOTE
> As ICMP is an IPv4 protocol and ICMPv6 is an IPv6 protocol, configuring a routing policy rule to match ICMPv6 packets when address-family ipv4 is configured or vice versa are unlikely to be useful and probably will not behave as you are expecting it to behave.

You can specify an ICMPv6 type code by type; for example, 128 (echo-request), or by a type and code pair; for example, type 1 and code 4 (port-unreachable). Alternatively, you can specify the ICMPv6 type code explicitly by using the **name** *name* parameter; for example, `name echo-request`.

For a list of ICMPv6 codes and types, refer to ICMPv6 Types on page 55.

Use the **set** form of this command to create a rule to match ICMPv6 packets.

Use the **delete** form of this command to delete a rule that matches ICMPv6 packets.

Use the **show** form of this command to view a rule that matches ICMPv6 packets.

policy route pbr <name> rule <rule-number> ipv6-route type <type-number>

Defines the IPv6 route type to match for a routing policy rule.

Syntax

set policy route pbr *name* **rule** *rule-number* **ipv6-route type** *type-number*

delete policy route pbr *name* **rule** *rule-number* **ipv6-route type**

show policy route pbr *name* **rule** *rule-number* **ipv6-route type**

Parameters

name

Name of a PBR group. The PBR group must be unique and must not be used with other PBR policy commands.

rule-number

The numeric identifier of the rule. Rule numbers determine the order in which rules are executed. Each rule must have a unique rule number. The numbers range from 1 through 9999.
You can define multiple rules by creating more than one **rule** configuration node.

ipv6-route

Specifies matching based on an IPv6 route.

type-number

IPv6 route-type. Values range from 0 through 255.

Modes

Configuration mode

Configuration Statement

```
policy {
    route {
        pbr name {
            rule rule-number {
                ipv6-route {
                    type type-number
                }
            }
        }
    }
}
```

Usage Guidelines

NOTE
This command can be used to block Type 0 routing headers in IPv6. RFC 5095 deprecates the use of Type 0 routing headers in IPv6 because they are a security risk.

You must specify the address-family, action, and table leaf nodes to configure a routing policy. It is recommended to use the**delete policy route pbr** *name* **rule** *number* command to delete a routing policy.

Use the **set** form of this command to define the IPv6 route type for a routing-policy rule set.

Use the **delete** form of this command to delete the IPv6 route type for the routing-policy rule set.

Use the **show** form of this command to display the IPv6 route type for the routing-policy rule set.

policy route pbr <name> rule <rule-number> log

Enables logging for a routing policy rule.

Syntax

set policy route pbr *name* **rule** *rule-number* **log**

delete policy route pbr *name* **rule** *number* **log**

show policy route pbr *name* **rule** *number*

Command Default

Logging is disabled.

Parameters

name

The name of an IP routing policy.

rule-number

The numeric identifier of the rule. Rule numbers determine the order in which rules are executed. Each rule must have a unique rule number. The numbers range from 1 through 9999.
You can define multiple rules by creating more than one **rule** configuration node.

Modes

Configuration mode

Configuration Statement

```
policy {
    route {
        pbr name {
                rule rule-number {
                    log
                }
            }
        }
    }
```

Usage Guidelines

You must specify the address-family, action, and table leaf nodes to configure a routing policy. It is recommended to use the **delete policy route pbr** *name* **rule** *number* command to delete a routing policy.

When logging is enabled, any action taken is logged.

Use the **set** form of this command to enable logging for a routing policy rule.

Use the **delete** form of this command to restore the default behavior for logging, that is, actions are not logged.

Use the **show** form of this command to display whether logging is enabled or disabled.

policy route pbr <name> rule <rule-number> port <port>

Defines the source port name, number, range, or port group for a routing policy rule.

Syntax

set policy route pbr *name* **rule** *rule-number* { **port** [*port* | *1-65535* | *start-end* | *port-group-name*] }

delete policy route pbr *name* **rule** *rule-number* [**port** [*port* | *1-65535* | *start-end* | *port-group-name*]]

show policy route pbr *name* **rule** *number* [**port**]

Parameters

name

The name of an IP routing policy.

rule-number

The numeric identifier of a policy rule. Rule numbers determine the order in which rules are processed. Each rule must have a unique rule number. The number ranges from 1 through 9999.
You can define multiple rules by creating more than one **rule** configuration node.

port [*port* | *1-65535* | *start-end* | *port-group-name*]

Applicable only when the protocol is TCP or UDP. A source port to match. The format of the port is any of the following:
port-name: The name of an IP service; for example, http. You can specify any service name in the `/etc/services` file.
1-65535: A port number. The numbers range from 1 through 65535.
start-end: A specified range of ports; for example, 1001-1005.
port-group-name: A port group. A packet is considered a match if it matches any port name or number specified in the group. Only one port group may be specified. The port group must already be defined.
This criterion specifies a group of addresses, ports, or networks for packet source address.
A packet is considered a match for an address, a network, or a port group if it matches any host IP address, network address, or port name or number, respectively, in the group. However, if more than one group is specified, the packet must be a match for both groups to be considered a match. For example, if both an address group and a port group are specified, the source of the packet must match at least one item in the address group and at least one item in the port group.
An address group may be specified with a port group.
If both an address and a port are specified, the packet is considered a match only if both the address and the port match.

Modes

Configuration mode

Configuration Statement

```
policy {
    route {
        pbr name {
                rule rule-number {
                    port name
                    port 1-65535
```

```
                port start-end
                port port-group-name
            }
        }
    }
}
```

Usage Guidelines

You must specify the address-family, action, and table leaf nodes to configure a routing policy. It is recommended to use the **delete policy route pbr** *name* **rule** *number* command to delete a routing policy.

This criterion specifies a port or a group of ports for packet source address for a routing policy rule.

A packet is considered a match for an address, a network, or a port group if it matches any host IP address, network address, or port name or number, respectively, in the group. However, if more than one group is specified, the packet must be a match for both groups in order to be considered a match. For example, if an address group and a port group are both specified, the packet's source must match at least one item in the address group and at least one item in the port group.

An address group can be specified together with a port group, and a network group can be specified together with a port group. You cannot specify both an address and a network group.

The address family must match the specified family by using the **set policy route pbr** *name* **rule** *number* **address-family ipv4** command.

Use the **set** form of this command to define the source for a routing policy rule.

Use the **delete** form of this command to remove the source for a routing policy rule.

Use the **show** form of this command to view the source for a routing policy rule.

policy route pbr <name> rule <rule-number> pcp <pcp-number>

Defines the 801.1 priority-code point number to match for a routing policy rule.

Syntax

set policy route pbr *name* **rule** *rule-number* **pcp** *pcp-number*

delete policy route pbr *name* **rule** *rule-number* **pcp**

show policy route pbr *name* **rule** *rule-number* **pcp**

Parameters

name

Name of a PBR group. The PBR group must be unique and must not be used with other PBR policy commands.

rule-number

The numeric identifier of the rule. Rule numbers determine the order in which rules are executed. Each rule must have a unique rule number. The numbers range from 1 through 9999.
You can define multiple rules by creating more than one **rule** configuration node.

pcp-number

802.1 priority-code point number. Values range from 0 through 7.

Modes

Configuration mode

Configuration Statement

```
policy {
    route {
        pbr name {
            rule rule-number {
                pcp pcp-number
            }
        }
    }
}
```

Usage Guidelines

You must specify the address-family, action, and table leaf nodes to configure a routing policy. It is recommended to use the **delete policy route pbr** *name* **rule** *number* command to delete a routing policy.

Use the **set** form of this command to define an 802.1 priority-code point for a routing-policy rule set.

Use the **delete** form of this command to delete the 802.1 priority-code point for the routing-policy rule set.

Use the **show** form of this command to display the 802.1 priority-code point for the routing-policy rule set.

policy route pbr <name> rule <rule-number> protocol <protocol>

Defines the protocol of an IP routing policy rule.

Syntax

set policy route pbr *name* **rule** *rule-number* **protocol** { *text* | *0-255* | **all** | *name* }

delete policy route pbr *name* **rule** *rule-number* **protocol** [*text* | *0-255* | **all** | *name*]

show policy route pbr *name* **rule** *rule-number* **protocol**

Parameters

name

The name of an IP routing policy.

rule-number

The numeric identifier of the rule. Rule numbers determine the order in which rules are executed. Each rule must have a unique rule number. The numbers range from 1 through 9999.
You can define multiple rules by creating more than one **rule** configuration node.

protocol

The *protocol* is any of the following:
text: Matches packets by protocol type. Any protocol literals or numbers listed in the file `/etc/protocols` can be specified. The keywords **icmpv6** and **all** (for all protocols) are also supported.
0-255: An IP protocol number that ranges from 0 through 255.
all: All IP protocols.
! *protocol*: All IP protocols except for the specified name or number. Prefixing the protocol name with the negation operator (the exclamation mark) matches every protocol except the specified protocol. For example, !tcp matches all protocols except TCP.
This parameter matches the last, next-header field in the IP header chain. This match means that if the packet has no extension headers, it matches the next-header field in the main header. If the packet does have extension headers, the parameter matches the next-header field of the last extension header in the chain. In other words, the parameter always matches the ID of the transport-layer packet that is being carried.
Exercise care when employing more than one rule that uses the negation. Routing policy rules are evaluated sequentially, and a sequence of negated rules could result in unexpected behavior.

Modes

Configuration mode

Configuration Statement

```
policy {
    route {
        pbr name {
                rule rule-number {
                    protocol
                        text
                        0-255
                        all
                        name
                }
            }
```

```
        }
    }
```

Usage Guidelines

You must specify the address-family, action, and table leaf nodes to configure a routing policy. It is recommended to use the **delete policy route pbr** *name* **rule** *number* command to delete a routing policy.

> NOTE
> The routing policy does not validate the protocol against the configured address-family. "protocol icmp" type is used with "address-family ipv4" while "protocol icmpv6" type is used with "address-family ipv6".

Use the **set** form of this command to define the protocol of an IP routing policy rule.

Use the **delete** form of this command to remove a protocol from a routing policy rule.

Use the **show** form of this command to view the protocol of a routing policy rule.

policy route pbr <name> rule <rule-number> source address <address>

Defines the source address for a routing policy rule.

Syntax

set policy route pbr *name* **rule** *rule-number* **source address** *address*

delete policy route pbr *name* **rule** *rule-number* **source address** [*addresss*]

show policy route pbr *name* **rule** *rule-number* **source**

Parameters

name

The name of an IP routing policy.

rule-number

The numeric identifier of a policy rule. Rule numbers determine the order in which rules are processed. Each rule must have a unique rule number. The number ranges from 1 through 9999.
You can define multiple rules by creating more than one **rule** configuration node.

source

Specifies matching based on a source address.

address

Specifies an address to match. Address formats are as follows:
address-group name: An address group that is configured with a list of addresses.
ip-address: An IPv4 address.
ip-address/prefix: An IPv4 network address, where 0.0.0.0/0 matches any network.
!*ip-address*: All IP addresses except the specified IPv4 address.
!*ip-address/prefix*: All IP addresses except the specified IPv4 network address.
ipv6-address: An IPv6 address; for example, fe80::20c:29fe:fe47:f89.
ip-address/prefix: An IPv6 network address, where ::/0 matches any network; for example, fe80::20c:29fe:fe47:f88/64.
!*ipv6-address*: All IP addresses except the specified IPv6 address.
!*ip-address/prefix*: All IP addresses except the specified IPv6 network address.

Modes

Configuration mode

Configuration Statement

```
policy {
    route {
        pbr name {
                rule rule-number {
                    source {
                        address address

                    }
                }
            }
        }
    }
```

Usage Guidelines

This match criterion specifies a port or a group of ports for packet source address for a routing policy rule.

A packet is considered a match for an address, a network, or a port group if it matches any host IP address, network address, or port name or number, respectively, in the group. However, if more than one group is specified, the packet must be a match for both groups to be considered a match. For example, if both an address group and a port group are specified, the source of the packet must match at least one item in the address group and at least one item in the port group.

An address group may be specified with a port group.

If both an address and a port are specified, the packet is considered a match only if both the address and the port match.

Use the **set** form of this command to define the source for a routing policy rule.

Use the **delete** form of this command to remove the source for a routing policy rule.

Use the **show** form of this command to view the source for a routing policy rule.

policy route pbr <name> rule <rule-number> source mac-address <address>

Defines the source MAC address to match for a routing policy rule.

Syntax

set policy route pbr *name* **rule** *number* **source mac-address** *address*

delete policy route pbr *name* **rule** *number* **source mac-address** [*address*]

show policy route pbr *name* **rule** *number* **source mac-address** [*address*]

Parameters

name

Name of a PBR group. The PBR group must be unique and must not be used with other PBR policy commands.

rule-number

The numeric identifier of the rule. Rule numbers determine the order in which rules are executed. Each rule must have a unique rule number. The numbers range from 1 through 9999.
You can define multiple rules by creating more than one **rule** configuration node.

source

Specifies matching based on a source address.

address

Media access control (MAC) address. The address format is six 8-bit numbers, separated by colons, in hexadecimal; for example, 00:0a:59:9a:f2:ba.

Modes

Configuration mode

Configuration Statement

```
policy {
    route {
        pbr name {
            rule rule-number {
                source {
                    mac-address address
                }
            }
        }
    }
}
```

Usage Guidelines

NOTE

For policy based routing, the usefulness of this command is limited because the MAC address is on a local interface.

You must specify the address-family, action, and table leaf nodes to configure a routing policy. It is recommended to use the **delete policy route pbr** *name* **rule** *number* command to delete a routing policy.

Use the **set** form of this command to define a source MAC address for a routing-policy rule set.

Use the **delete** form of this command to delete the source MAC address for the routing-policy rule set.

Use the **show** form of this command to display the source MAC address for the routing-policy rule set.

policy route pbr <name> rule <rule-number> source port <port>

Defines the source port name, number, range, or port group for a routing policy rule.

Syntax

set policy route pbr *name* **rule** *rule-number* **source port** [*name* | *1-65535* | *start-end* | *port-group-name*]

delete policy route pbr *name* **rule** *rule-number* **source port** [*name* | *1-65535* | *start-end* | *port-group-name*]

show policy route pbr *name* **rule** *rule-number* **source port**

Parameters

name

The name of an IP routing policy.

rule-number

The numeric identifier of a policy rule. Rule numbers determine the order in which rules are processed. Each rule must have a unique rule number. The number ranges from 1 through 9999.
You can define multiple rules by creating more than one **rule** configuration node.

source

Specifies matching based on a source address.

port [*name* | *1-65535* | *start-end* | *port-group-name*]

Applicable only when the protocol is TCP or UDP. A source port to match. The format of the port is any of the following:
name: The name of an IP service; for example, http. You can specify any service name in the `/etc/services` file.
1-65535: A port number. The numbers range from 1 through 65535.
start-end: A specified range of ports; for example, 1001-1005.
port-group-name: A port group. A packet is considered a match if it matches any port name or number specified in the group. Only one port group may be specified. The port group must already be defined.
This criterion specifies a group of addresses, ports, or networks for packet source address.
A packet is considered a match for an address, a network, or a port group if it matches any host IP address, network address, or port name or number, respectively, in the group. However, if more than one group is specified, the packet must be a match for both groups to be considered a match. For example, if both an address group and a port group are specified, the source of the packet must match at least one item in the address group and at least one item in the port group.
An address group may be specified with a port group.
If both an address and a port are specified, the packet is considered a match only if both the address and the port match.

Modes

Configuration mode

Configuration Statement

```
policy {
    route {
        pbr name {
                rule rule-number {
```

```
                source {
                    port name
                    port 1-65535
                    port start-end
                    port port-group-name
                }
            }
        }
    }
}
```

Usage Guidelines

This criterion specifies a port or a group of ports for packet source address for a routing policy rule.

You must specify the address-family, action, and table leaf nodes to configure a routing policy. It is recommended to use the **delete policy route pbr** *name* **rule** *number* command to delete a routing policy.

A packet is considered a match for an address, a network, or a port group if it matches any host IP address, network address, or port name or number, respectively, in the group. However, if more than one group is specified, the packet must be a match for both groups in order to be considered a match. For example, if an address group and a port group are both specified, the packet's source must match at least one item in the address group and at least one item in the port group.

Use the **set** form of this command to define the source for a routing policy rule.

Use the **delete** form of this command to remove the source for a routing policy rule.

Use the **show** form of this command to view the source for a routing policy rule.

policy route pbr <name> rule <rule-number> table <table-number>

Defines the table number for an IP routing policy rule.

Syntax

set policy route pbr *name* **rule** *rule-number* **table** *table-number*

delete policy route pbr *name* **rule** *rule-number* **table** [*table-number*]

show policy route pbr *name* **rule** *rule-number*

Parameters

name

The name of an IP routing policy. The policy name must be unique and must not be used with other PBR policy commands.

rule-number

The numeric identifier of the rule. Rule numbers determine the order in which rules are executed. Each rule must have a unique rule number. The numbers range from 1 through 9999.
You can define multiple rules by creating more than one **rule** configuration node.

table-number

To match according to the PBR Table ID numbers 1 through 128. Performs alternate processing on packets satisfying the match criteria.

Modes

Configuration mode

Configuration Statement

```
policy {
    route {
        pbr name{
                rule rule-number {
                        table table-number
                }
            }
        }
    }
```

Usage Guidelines

You must specify the address-family, action, and table leaf nodes to configure a routing policy. It is recommended to use the **delete policy route pbr** *name* **rule** *number* command to delete a routing policy.

Use the **set** form of this command to define the address family or routing table ID for an IP routing policy rule.

Use the **delete** form of this command to remove the address family or routing table ID for a rule.

Use the **show** form of this command to view the address family or routing table ID for a rule.

The address family must match the specified family by using the **set policy route pbr** *name* **rule** *number* **address-family ipv4** command.

Use the **set** form of this command to define the source for a routing policy rule.

Use the **delete** form of this command to remove the source for a routing policy rule.

Use the **show** form of this command to view the source for a routing policy rule.

policy route pbr <name> rule <rule-number> tcp flags <tcp-flag>

Defines the types of TCP flags to be matched for a routing policy rule.

Syntax

set policy route pbr *name* **rule** *rule-number* **tcp flags** *flags*

delete policy route pbr *name* **rule** *rule-number* **tcp flags** [*flags*]

show policy route pbr *name* **rule** *rule-number* **tcp flags**

Parameters

name

The name of an IP routing policy.

rule-number

The numeric identifier of the rule. Rule numbers determine the order in which rules are executed. Each rule must have a unique rule number. The numbers range from 1 through 9999.
You can define multiple rules by creating more than one **rule** configuration node.

tcp-flags

The flags to be matched in a packet. The flags are any of SYN, ACK, FIN, RST, URG, and PSH. You can specify more than one flag in a list separated by commas.
Prefixing a flag name with the negation operator matches packets with that flag unset. You can also use **!** to match packets by not using a given TCP flag. For example, the list SYN, **!**ACK, **!**FIN, **!**RST matches only packets with the SYN flag set and the ACK, FIN, and RST flags unset.

Modes

Configuration mode

Configuration Statement

```
policy {
    route {
        pbr name {
              rule rule-number {
                    tcp {
                       flags tcp-flags
                    }
                }
            }
        }
    }
```

Usage Guidelines

You must specify the address-family, action, and table leaf nodes to configure a routing policy. It is recommended to use the **delete policy route pbr** *name* **rule** *number* command to delete a routing policy.

Use the **set** form of this command to define the types of TCP flags to be matched for a routing policy rule.

Use the **delete** form of this command to remove the types of TCP flags to be matched for a routing policy rule.

Use the **show** form of this command to view the types of TCP flags to be matched for a routing policy rule.

show policy route <interface>

Displays routing policy configuration or statistics.

Syntax

show policy route *interface*

Parameters

interface

The name of an interface.

Modes

Operational mode

Usage Guidelines

A policy identifies traffic that matches parameters and specifies which table to use. The table defines the routes for a packet to take. A routing policy is a named collection of as many as 9,999 packet-classification rules. When applied to an interface, the policy rule classifies incoming traffic.

NOTE

The PBR rule counters count all of the matched packets regardless of the availability of the route.

Use this command in operational mode to display packet statistics for all PBR rules in all groups.

For example:

show policy route

```
vyatta@vyatta:~$ show policy route
--------------------------------------
Rulesets Information: PBR
--------------------------------------
--------------------------------------------------------------------------------
PBR policy "myroute":
Active on (dp0p1p3, in)
rule    action  proto           packets         bytes
----    ------  -----           -------         -----
10      allow   any             0               0
  condition - from 192.168.10.0/24 ipv4 table 1

20      allow   any             0               0
  condition - from 192.168.20.0/24 ipv4 table 2

PBR policy "myroute":
Active on (dp0p1p4, in)
rule    action  proto           packets         bytes
----    ------  -----           -------         -----
10      allow   any             0               0
  condition - from 192.168.10.0/24 ipv4 table 1

20      allow   any             0               0
  condition - from 192.168.20.0/24 ipv4 table 2
```

show policy route table

Displays the configuration of the IP routing policy table.

Syntax

show policy route table

Modes

Operational mode

Usage Guidelines

Command Output

The **show policy route table** command displays the following information:

```
vyatta@vyatta# show policy route table
PBR Group                    Rule  Table
---------------------------  ----  -----
                     myroute    10     1
                     myroute    20     2
                     myroute    10     1
                     myroute    20     2
```

Output field	Description
PBR Group	Name of a PBR group.
Rule	Number of the IP policy rule that is configured for a PBR group.
Table	Number of the PBR table that is configured for a PBR group.

Related commands

The following table lists related commands that are documented elsewhere.

Related commands documented elsewhere	
protocols static table	The commands for creating alternate routing tables are described in *Brocade Vyatta Network OS Basic Routing Configuration Guide*
resources group address-group <group-name>	Defines a group of IP addresses that are referenced in firewall rules. (Refer to *Brocade Vyatta Network OS Basic Routing Configuration Guide*.)
resources group port-group <group-name>	Defines a group of ports that are referenced in firewall rules. (Refer to *Brocade Vyatta Network OS Basic Routing Configuration Guide*.)
show ip route table	The command for displaying the contents of an alternate routing table is described in *Brocade Vyatta Network OS Basic Routing Configuration Guide*.
firewall group	Routing policy match criteria support references to predefined groups of addresses, ports, and networks. Commands for defining such groups are described in *Brocade Vyatta Network OS Firewall Configuration Guide*.

ICMP Types

This appendix lists the Internet Control Messaging Protocol (ICMP) types defined by the Internet Assigned Numbers Authority (IANA).

The IANA has developed a standard that maps a set of integers onto ICMP types. The following table lists the ICMP types and codes defined by the IANA and maps them to the literal strings that are available in the Brocade vRouter.

TABLE 3 ICMP types

ICMP Type	Code	Literal	Description
0 - Echo reply	0	echo-reply	Echo reply (pong)
3 - Destination unreachable		destination- unreachable	Destination is unreachable
	0	network-unreachable	Destination network is unreachable
	1	host-unreachable	Destination host is unreachable
	2	protocol-unreachable	Destination protocol is unreachable
	3	port-unreachable	Destination port is unreachable
	4	fragmentation-needed	Fragmentation is required
	5	source-route-failed	Source route has failed
	6	network-unknown	Destination network is unknown
	7	host-unknown	Destination host is unknown
	9	network-prohibited	Network is administratively prohibited
	10	host-prohibited	Host is administratively is prohibited
	11	ToS-network-unreachable	Network is unreachable for ToS
	12	ToS-host-unreachable	Host is unreachable for ToS
	13	communication-prohibited	Communication is administratively prohibited
	14	host-precedence-violation	Requested precedence is not permitted.
	15	precedence-cutoff	Precedence is lower than the required minimum.
4 - Source quench	0	source-quench	Source is quenched (congestion control)
5 - Redirect message		redirect	Redirected message
	0	network-redirect	Datagram is redirected for the network
	1	host-redirect	Datagram is redirected for the host
	2	ToS-network-redirect	Datagram is redirected for the ToS and network
	3	ToS-host-redirect	Datagram is redirected for the ToS and host
8 - Echo request	0	echo-request	Echo request (ping)
9 - Router advertisement	0	router-advertisement	Router advertisement
10 - Router solicitation	0	router-solicitation	Router solicitation
11 - Time exceeded		time-exceeded	Time to live (TTL) has exceeded
	0	ttl-zero-during-transit	TTL has expired in transit

TABLE 3 ICMP types (continued)

ICMP Type	Code	Literal	Description
	1	ttl-zero-during-reassembly	Fragment reassembly time has exceeded
12 - Parameter problem: Bad IP header		parameter-problem	Bad IP header
	0	ip-header-bad	Pointer that indicates an error
	1	required-option-missing	Missing required option
13 - Timestamp	0	timestamp-request	Request for a timestamp
14 - Timestamp reply	0	timestamp-reply	Reply to a request for a timestamp
15 - Information request	0		Information request
16 - Information reply	0		Information reply
17 - Address mask request	0	address-mask-request	Address mask request
18 - Address mask reply	0	address-mask-reply	Address mask reply

ICMPv6 Types

This appendix lists the ICMPv6 types defined by the Internet Assigned Numbers Authority (IANA).

The Internet Assigned Numbers Authority (IANA) has developed a standard that maps a set of integers onto ICMPv6 types. The following table lists the ICMPv6 types and codes defined by the IANA and maps them to the strings literal strings available in the Brocade vRouter.

TABLE 4 ICMPv6 types

ICMPv6 Type	Code	Literal	Description
1 - Destination unreachable		destination- unreachable	
	0	no-route	No route to destination
	1	communication-prohibited	Communication with destination administratively prohibited
	2		Beyond scope of source address
	3	address-unreachable	Address unreachable
	4	port-unreachable	Port unreachable
	5		Source address failed ingress/ egress policy
	6		Reject route to destination
2 - Packet too big	0	packet-too-big	
3 - Time exceeded		time-exceeded	
	0	ttl-zero-during-transit	Hop limit exceeded in transit
	1	ttl-zero-during-reassembly	Fragment reassembly time exceeded
4 - Parameter problem		parameter-problem	
	0	bad-header	Erroneous header field encountered
	1	unknown-header-type	Unrecognized Next Header type encountered
	2	unknown-option	Unrecognized IPv6 option encountered
128 - Echo request	0	echo-request	Echo request (ping)
129 - Echo reply	0	echo-reply	Echo reply (pong)
133 - Router solicitation	0	router-solicitation	Router solicitation
134 - Router advertisement	0	router-advertisement	Router advertisement
135 - Neighbor solicitation	0	neighbor-solicitation (neighbour-solicitation)	Neighbor solicitation
136 - Neighbor advertisement	0	neighbor-advertisement (neighbour-advertisement)	Neighbor advertisement

Supported Interface Types

The following table shows the syntax and parameters of supported interface types. Depending on the command, some of these types may not apply.

Interface Type	Syntax	Parameters
Bridge	**bridge** *brx*	*brx*: The name of a bridge group. The name ranges from br0 through br999.
Data plane	**dataplane** *interface-name*	*interface-name*: The name of a data plane interface. Following are the supported formats of the interface name: • **dp***x***p***y***p***z*—The name of a data plane interface, where — **dp***x* specifies the data plane identifier (ID). Currently, only dp0 is supported. — p*y* specifies a physical or virtual PCI slot index (for example, p129). — **p***z* specifies a port index (for example, p1). For example, dp0p1p2, dp0p160p1, and dp0p192p1. • **dp***x***em***y* —The name of a data plane interface on a LAN-on-motherboard (LOM) device that does not have a PCI slot, where **em***y* specifies an embedded network interface number (typically, a small number). For example, dp0em3. • **dp***x***s***y* —The name of a data plane interface on a device that is installed on a virtual PCI slot, where *x***s***y* specifies an embedded network interface number (typically, a small number). For example, dp0s2. • **dp***x***P***n***p***y***p***z* —The name of a data plane interface on a device that is installed on a secondary PCI bus, where **P***n* specifies the bus number. You can use this format to name data plane interfaces on large physical devices with multiple PCI buses. For these devices, it is possible to have network interface cards installed on different buses with these cards having the same slot ID. The value of *n* must be an integer greater than 0. For example, dp0P1p162p1 and dp0P2p162p1.
Data plane vif	**dataplane** *interface-name* **vif** *vif-id* [**vlan** *vlan-id*]	*interface-name*: Refer to the preceding description. *vif-id*: A virtual interface ID. The ID ranges from 1 through 4094. *vlan-id*: The VLAN ID of a virtual interface. The ID ranges from 1 through 4094.
Loopback	**loopback lo** or **loopback lo***n*	*n*: The name of a loopback interface, where *n* ranges from 1 through 99999.
OpenVPN	**openvpn** *vtunx*	*vtunx*: The identifier of an OpenVPN interface. The identifier ranges from vtun0 through vtun*x*, where *x* is a nonnegative integer.
Tunnel	**tunnel** *tunx* or **tunnel** *tunx* **parameters**	*tunx*: The identifier of a tunnel interface you are defining. The identifier ranges from tun0 through tun*x*, where *x* is a nonnegative integer.
Virtual tunnel	**vti** *vtix*	*vtix*: The identifier of a virtual tunnel interface you are defining. The identifier ranges from vti0 through vti*x*, where *x* is a nonnegative integer.

Interface Type	Syntax	Parameters
		Note: This interface does not support IPv6.
VRRP	*parent-interface* **vrrp vrrp-group** *group*	*parent-interface*: The type and identifier of a parent interface; for example, data plane dp0p1p2 or bridge br999. *group*: A VRRP group identifier. The name of a VRRP interface is not specified. The system internally constructs the interface name from the parent interface identifier plus the VRRP group number; for example, dp0p1p2v99. Note that VRRP interfaces support the same feature set as does the parent interface.

VRF support for PBR

The implementation of VRF on the Brocade 5600 vRouter supports policy-based routing (PBR).

Command support for VRF routing instances

VRF allows a Brocade 5600 vRouter to support multiple routing tables, one for each VRF routing instance. Some commands in this guide support VRF and can be applied to particular routing instances.

Use the guidelines in this section to determine correct syntax when adding VRF routing instances to commands. For more information about VRF, refer to *Brocade Vyatta Network OS Basic Routing Configuration Guide*. This guide includes an overview of VRF, VRF configuration examples, information about VRF-specific features, and a list of commands that support VRF routing instances.

Adding a VRF routing instance to a Configuration mode command

For most Configuration mode commands, specify the VRF routing instance at the beginning of a command. Add the appropriate VRF keywords and variable to follow the initial action (**set**, **show**, or **delete**) and before the other keywords and variables in the command.

Configuration mode example: syslog

The following command configures the syslog logging level for the specified syslog host. The command does not include a VRF routing instance, so the command applies to the default routing instance.

```
vyatta@R1# set system syslog host 10.10.10.1 facility all level debug
vyatta@R1# show system syslog
syslog {
    host 10.10.10.1 {
            facility all {
                    level debug
            }
    }
}
```

The following example shows the same command with the VRF routing instance (GREEN) added. Notice that **routing routing-instance GREEN** has been inserted between the basic action (**set** in the example) and the rest of the command. Most Configuration mode commands follow this convention.

```
vyatta@R1# set routing routing-instance GREEN system syslog host 10.10.10.1 facility all level debug
vyatta@R1# show routing
routing {
     routing-instance GREEN {
             system {
                     syslog {
                             host 11.12.13.2:514 {
                                     facility all {
                                             level debug
                                     }
                             }
                     }
             }
     }
}
```

Configuration mode example: SNMP

Some features, such as SNMP, are not available on a per-routing instance basis but can be bound to a specific routing instance. For these features, the command syntax is an exception to the convention of specifying the routing instance at the beginning of Configuration mode commands.

The following example shows how to configure the SNMPv1 or SNMPv2c community and context for the RED and BLUE routing instances. The first two commands specify the RED routing instance as the context for community A and BLUE routing instance as the context for community B. The subsequent commands complete the configuration.

For more information about configuring SNMP, refer to *Brocade Vyatta Network OS Remote Management Configuration Guide*.

```
vyatta@R1# set service snmp community commA context RED
vyatta@R1# set service snmp community commB context BLUE
vyatta@R1# set service snmp view all oid 1
vyatta@R1# set service snmp community commA view all
vyatta@R1# set service snmp community commB view all
vyatta@R1# show service snmp community
 community commA {
        context RED
        view all
 }
 community commB {
        context BLUE
        view all
 }
[edit]
vyatta@vyatta#
```

Adding a VRF routing instance to an Operational mode command

The syntax for adding a VRF routing instance to an Operational mode command varies according to the type of command parameters:

- If the command does not have optional parameters, specify the routing instance at the end of the command.
- If the command has optional parameters, specify the routing instance after the required parameters and before the optional parameters.

Operational mode examples without optional parameters

The following command displays dynamic DNS information for the default routing instance.

```
vyatta@vyatta:~$ show dns dynamic status
```

The following command displays the same information for the specified routing instance (GREEN). The command does not have any optional parameters, so the routing instance is specified at the end of the command.

```
vyatta@vyatta:~$ show dns dynamic status routing-instance GREEN
```

Operational mode example with optional parameters

The following command obtains multicast path information for the specified host (10.33.2.5). A routing instance is not specified, so the command applies to the default routing instance.

```
vyatta@vyatta:~$ mtrace 10.33.2.5 detail
```

The following command obtains multicast path information for the specified host (10.33.2.5) and routing instance (GREEN). Notice that the routing instance is specified before the optional **detail** keyword.

```
vyatta@vyatta:~$ mtrace 10.33.2.5 routing-instance GREEN detail
```

Operational mode example output: SNMP

The following SNMP **show** commands display output for routing instances.

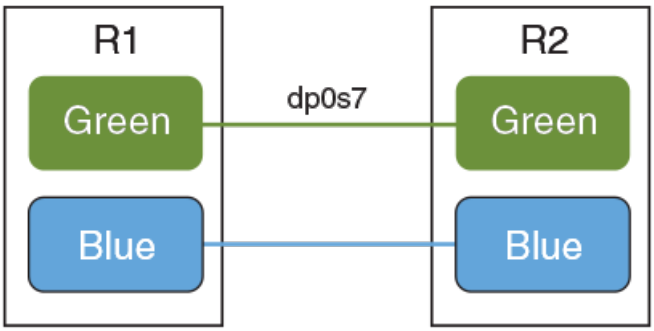
```
vyatta@vyatta:~$ show snmp routing-instance
Routing Instance SNMP Agent is Listening on for Incoming Requests:
Routing-Instance            RDID
------------------          ----
RED                         5

vyatta@vyatta:~$ show snmp community-mapping
SNMPv1/v2c Community/Context Mapping:
Community                   Context
---------                   -------
commA                       'RED'
commB                       'BLUE'
deva                        'default'


vyatta@vyatta:~$ show snmp trap-target
SNMPv1/v2c Trap-targets:
Trap-target                   Port   Routing-Instance Community
-----------                   ----   ---------------- ---------
1.1.1.1                              'RED'           'test'


vyatta@vyatta:~$ show snmp v3 trap-target
SNMPv3 Trap-targets:
Trap-target                   Port   Protocol Auth Priv Type   EngineID              Routing-Instance User
-----------                   ----   -------- ---- ---- ----   --------              ---------------- ----
2.2.2.2                       '162'  'udp'    'md5'      'infor                      'BLUE'           'test'
```

Configuring policy-based routing on a routing instance

In this example, the R1 vRouter is connected to the R2 vRouter through the dp0s7 interface that is bound to the GREEN routing instance.

The following steps show how to create an alternate routing table in the GREEN routing instance on dp0s7.

FIGURE 2 Configuring policy-based routing on a routing instance



To configure policy-based routing on a vRouter perform the following configuration and then reproduce the configuration as described in *Brocade Vyatta Network OS Basic Routing Configuration Guide*.

TABLE 5 Configuring policy-based static routes on a routing instance

Step	Command
Define the dp0s7 interface and bind it to the GREEN routing instance.	`vyatta@R1# set interfaces dataplane dp0s7` `vyatta@R1# set routing routing-instance GREEN interface dp0s7`
Define an interface based static route.	`vyatta@R1# set routing routing-instance GREEN protocols static table 10 interface-route 20.1.1.0/24 next-hop-interface dp0s7` `vyatta@R1# set routing routing-instance GREEN protocols static table 10 interface-route6 2010::/64 next-hop-interface dp0s7`

Create IPv4 and IPv6 PBR static routes under the GREEN routing instance.	`vyatta@R1# set routing routing-instance GREEN protocols static table 10 route 20.1.1.0/24 next-hop 10.1.1.2 interface dp0s7`
	
	`vyatta@R1# set routing routing-instance GREEN protocols static table 10 route6 2010::/64 next-hop 1010::2 interface dp0s7`

Create the IPv4 and IPv6 static routes with distance in the GREEN routing instance in the 10 PBR table.	`vyatta@R1# set routing routing-instance GREEN protocols static table 10 route 20.1.1.0/24 next-hop 10.1.1.2 distance 8` `vyatta@R1# set routing routing-instance GREEN protocols static table 10 route6 2010::/64 next-hop 1010::2 distance 8`
Create IPv4 and IPv6 black hole PBR static route configurations under the GREEN routing instance.	`vyatta@R1# set routing routing-instance GREEN protocols static table 10 route 20.1.1.0/24 blackhole` `vyatta@R1# set routing routing-instance GREEN protocols static table 10 route6 2010::/64 blackhole`
Create unreachable IPv4 and IPv6 PBR static routes under the GREEN routing instance.	`vyatta@R1# set routing routing-instance GREEN protocols static route table 10 route 20.1.1.0/24 unreachable` `vyatta@R1# set routing routing-instance GREEN protocols static route6 table 10 route6 2010::/64 unreachable`

View the configuration.	`vyatta@R1# show routing`
	`routing {`
	`routing-instance GREEN {`
	`interface dp0s7`
	`protocols {`
	`static {`
	`table 10 {`
	`interface-route 20.1.1.0/24 {`
	`next-hop-interface dp0s7`
	`}`
	`interface-route6 2010::/64 {`
	`next-hop-interface dp0s7`
	`}`
	`route 20.1.1.0/24 {`
	`blackhole`
	`next-hop 10.1.1.2 {`
	`distance 10`
	`interface dp0s7`
	`}`
	`unreachable`
	`}`
	`route6 2010::/64 {`
	`blackhole`
	`next-hop 1010::2 {`
	`distance 10`
	`interface dp0s5`
	`}`
	`unreachable`
	
	`}`

TABLE 5 Configuring policy-based static routes on a routing instance (continued)

Step	Command
	} } } }

List of Acronyms

Acronym	Description
ACL	access control list
ADSL	Asymmetric Digital Subscriber Line
AH	Authentication Header
AMI	Amazon Machine Image
API	Application Programming Interface
AS	autonomous system
ARP	Address Resolution Protocol
AWS	Amazon Web Services
BGP	Border Gateway Protocol
BIOS	Basic Input Output System
BPDU	Bridge Protocol Data Unit
CA	certificate authority
CCMP	AES in counter mode with CBC-MAC
CHAP	Challenge Handshake Authentication Protocol
CLI	command-line interface
DDNS	dynamic DNS
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DLCI	data-link connection identifier
DMI	desktop management interface
DMVPN	dynamic multipoint VPN
DMZ	demilitarized zone
DN	distinguished name
DNS	Domain Name System
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
eBGP	external BGP
EBS	Amazon Elastic Block Storage
EC2	Amazon Elastic Compute Cloud
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

Acronym	Description
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
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
ISAKMP	Internet Security Association and Key Management Protocol
ISM	Internet Standard Multicast
ISP	Internet Service Provider
KVM	Kernel-Based Virtual Machine
L2TP	Layer 2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAN	local area network
LDAP	Lightweight Directory Access Protocol
LLDP	Link Layer Discovery Protocol
MAC	medium access control
mGRE	multipoint GRE
MIB	Management Information Base
MLD	Multicast Listener Discovery
MLPPP	multilink PPP
MRRU	maximum received reconstructed unit
MTU	maximum transmission unit
NAT	Network Address Translation
NBMA	Non-Broadcast Multi-Access
ND	Neighbor Discovery
NHRP	Next Hop Resolution Protocol
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
PAT	Port Address Translation
PCI	peripheral component interconnect
PIM	Protocol Independent Multicast
PIM-DM	PIM Dense Mode

Acronym	Description
PIM-SM	PIM Sparse Mode
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PTMU	Path Maximum Transfer Unit
PVC	permanent virtual circuit
QoS	quality of service
RADIUS	Remote Authentication Dial-In User Service
RHEL	Red Hat Enterprise Linux
RIB	Routing Information Base
RIP	Routing Information Protocol
RIPng	RIP next generation
RP	Rendezvous Point
RPF	Reverse Path Forwarding
RSA	Rivest, Shamir, and Adleman
Rx	receive
S3	Amazon Simple Storage Service
SLAAC	Stateless Address Auto-Configuration
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SONET	Synchronous Optical Network
SPT	Shortest Path Tree
SSH	Secure Shell
SSID	Service Set Identifier
SSM	Source-Specific Multicast
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus
TBF	Token Bucket Filter
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
ToS	Type of Service
TSS	TCP Maximum Segment Size
Tx	transmit
UDP	User Datagram Protocol
VHD	virtual hard disk
vif	virtual interface
VLAN	virtual LAN
VPC	Amazon virtual private cloud
VPN	virtual private network
VRRP	Virtual Router Redundancy Protocol

Acronym	Description
WAN	wide area network
WAP	wireless access point
WPA	Wired Protected Access