JUNIPER NETWORKS

JunosE™ Software for E Series™ Broadband Services Routers

Classifier Control Lists and Policy Lists Management

Release
14.1.x

Published: 2012-12-20

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

JunosE™ Software for E Series™ Broadband Services Routers Classifier Control Lists and Policy Lists Management
Release 14.1.x

Revision History
December 2012—FRS JunosE 14.1.x

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

YEAR 2000 NOTICE

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

SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

END USER LICENSE AGREEMENT

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

Table of Contents

List of Figures

List of Tables

About the Documentation

E Series and JunosE Documentation and Release Notes

For a list of related JunosE documentation, see http://www.juniper.net/techpubs/software/index.html.

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

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

Audience

This guide is intended for experienced system and network specialists working with Juniper Networks E Series Broadband Services Routers in an Internet access environment.

E Series and JunosE Text and Syntax Conventions

Table 1 on page x defines notice icons used in this documentation.

Table 1: Notice Icons

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

Table 2 on page x defines text and syntax conventions that we use throughout the E Series and JunosE documentation.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents commands and keywords in text.	• Issue the **clock source** command. • Specify the keyword **exp-msg**.
Bold text like this	Represents text that the user must type.	**host1(config)#traffic class low-loss1**

`Fixed-width text like this`	Represents information as displayed on your terminal's screen.	**host1#show ip ospf 2**
		`Routing Process OSPF 2 with Router ID 5.5.0.250`
		`Router is an Area Border Router (ABR)`

Italic text like this	• Emphasizes words. • Identifies variables. • Identifies chapter, appendix, and book names.	• There are two levels of access: *user* and *privileged*. • *clusterId, ipAddress.* • *Appendix A, System Specifications*
Plus sign (+) linking key names	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
Syntax Conventions in the Command Reference Guide		
Plain text like this	Represents keywords.	terminal length
Italic text like this	Represents variables.	*mask*, *accessListName*

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

Convention	Description	Examples
| (pipe symbol)	Represents a choice to select one keyword or variable to the left or to the right of this symbol. (The keyword or variable can be either optional or required.)	diagnostic | line
[ ] (brackets)	Represent optional keywords or variables.	[internal | external]
[ ]* (brackets and asterisk)	Represent optional keywords or variables that can be entered more than once.	[level1 | level2 | l1]*
{ } (braces)	Represent required keywords or variables.	{ permit | deny } { in | out } { *clusterId* | *ipAddress* }

Obtaining Documentation

To obtain the most current version of all Juniper Networks technical documentation, see the Technical Documentation page on the Juniper Networks Web site at http://www.juniper.net/.

To download complete sets of technical documentation to create your own documentation CD-ROMs or DVD-ROMs, see the Portable Libraries page at

http://www.juniper.net/techpubs/resources/index.html

Copies of the Management Information Bases (MIBs) for a particular software release are available for download in the software image bundle from the Juniper Networks Web site athttp://www.juniper.net/.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation to better meet your needs. Send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

CHAPTER 1

Classifier Control Lists for Policies

Classifier Control Lists Overview

Classifier control lists (CLACLs) specify the criteria by which the router defines a packet flow. Table 3 on page 3 lists the criteria that you can use to create CLACLs for different types of traffic flows.

Table 3: CLACL Criteria

Type of CLACL	Criteria
ATM	• CLP • Color • Traffic class • User packet class
Frame Relay	• Color • Mark discard eligibility (DE) bit • Traffic class • User packet class
GRE	• Color • Traffic class • Type-of-service (ToS) byte • User packet class

Table 3: CLACL Criteria *(continued)*

Type of CLACL	Criteria
IP	• Color • Destination IP address • Destination port • Destination route class • Internet Control Message Protocol (ICMP) • Internet Gateway Management Protocol (IGMP) • IP flags • IP fragmentation offset • Locally destined traffic • Protocol • Source IP address • Source port • Source route class • Transmission Control Protocol (TCP) • Traffic class • Type-of-service (ToS) byte • User Datagram Protocol (UDP) • User packet class
IPv6	• Color • Destination IPv6 address • Destination port • Destination route class • Internet Control Message Protocol version 6 (ICMPv6) • IPv6 traffic class • Locally destined traffic • Multicast Listener Discovery (MLD) • Next header • Source IPv6 address • Source port • Source route class • Traffic class • Transmission Control Protocol (TCP) • User Datagram Protocol (UDP) • User packet class
L2TP	• Color • Traffic class • User packet class
MPLS	• Color • Mark experimental (EXP) bit • Traffic class • User packet class

Table 3: CLACL Criteria *(continued)*

Type of CLACL	Criteria
VLAN	• Color • Traffic class • User packet class • User priority

You configure CLACLs with a name and then values to match in the IP datagram header. A CLACL does not include an action: actions take place when a match is included in a policy list.

NOTE: Do not use the asterisk (*) for the name of a classifier list. The asterisk is used as a wildcard for the **classifier-group** command.

If you do not specify one of the **frame-relay**, **gre-tunnel**, **ip**, **ipv6**, **l2tp**, **mpls**, or **vlan** keywords, the router creates an IP classifier list. This version of the command has been deprecated and may be removed in a future release.

Related Documentation

- Policy Resources Overview
- Monitoring Policy Management Overview

CHAPTER 2

Policy Lists

Policy Lists Overview

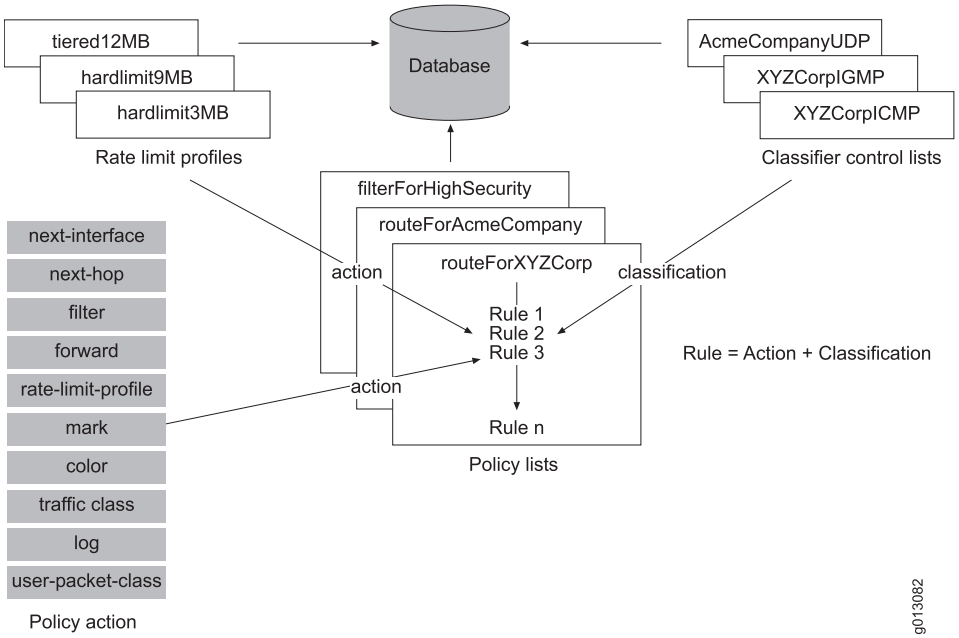
You create a policy rule by specifying a policy action within a classifier group that references a CLACL. These rules become part of a policy list that you can attach to an interface as either an input policy, secondary-input policy, or output policy. The router applies the rules in the attached policy list to the packets traversing that interface.

You can apply policy lists to packets:

- Arriving at an interface (input policy); on IP and IPv6 interfaces the packets arrive before route lookup
- Arriving at the interface, but after route lookup (secondary input policy); secondary input policies are supported only on IP and IPv6 interfaces
- Leaving an interface (output policy)

Figure 1 on page 8 shows how a sample IP policy list is constructed.

Figure 1: Constructing an IP Policy List



You can create a policy list with an unlimited number of classifier groups, each containing an unlimited number of rules. These rules can reference up to 512 classifier entries.

If you enter a **policy-list** command and then enter **exit**, the router creates a policy list with no rules. If the router does not find any rules in a policy, it inserts a default filter rule. Attaching this policy list to an interface filters all packets on that interface.

NOTE: If you do not specify one of the **frame-relay**, **gre-tunnel**, **ip**, **ipv6**, **l2tp**, **mpls**, or **vlan** keywords, the router creates an IP policy list. This version of the command has been deprecated and may be removed in a future release.

You can create policy lists for ATM, Frame Relay, IP, IPv6, GRE tunnels, L2TP, MPLS, and VLANs.

NOTE: Commands that you issue in Policy Configuration mode do not take effect until you exit from that mode.

Related Documentation

- Classifier Control Lists Overview on page 3
- Monitoring Policy Management Overview

Statistics Collection for Output Policies on Tunnel Interfaces Overview

You can configure the policy manager application to collect and store statistical counters for output policies attached to tunnel interfaces as a measure of the number of fragments.

In certain network environments, it might be useful to monitor and track the outgoing traffic from a tunnel interface to which policies are applied in terms of number of fragments, instead of monitoring the outgoing policed traffic in terms of number of packets. Based on the topology needs and management of services for subscribers, you can configure statistics for traffic on tunnel interfaces with output policies to be counted as either numbers of fragments or numbers of packets.

Related Documentation

- Configuring Statistics Collection for Output Policies on Tunnel Interfaces on page 30
- Verifying Statistics Collection for Output Policies on Tunnel Interfaces on page 66
- enable-frag-stats
- show enable-frag-stats

PART 2

Configuration

CHAPTER 3

Configuration Tasks for Managing Classifier Control Lists

Creating or Modifying Classifier Control Lists for ATM Policy Lists

You can create or modify a classifier control list that can be used only in ATM policy lists.

- Issue the **atm classifier-list** command:

```
host1(config)#atm classifier-list atmclassifier color red user-packet-class 10
  clp 1
```

Related Documentation

- Classifier Control Lists Overview on page 3
- Policy Lists Overview on page 7
- atm classifier-list

Creating or Modifying Classifier Control Lists for Frame-Relay Policy Lists

You can create or modify a classifier control list that can be used only in Frame Relay policy lists.

- Issue the **frame-relay classifier-list** command.;

```
host1(config)#frame-relay classifier-list frclassifier color red user-packet-class 10
  de-bit 1
```

Related Documentation

- Classifier Control Lists Overview on page 3
- Policy Lists Overview on page 7
- frame-relay classifier-list

Creating or Modifying Classifier Control Lists for GRE Tunnel Policy Lists

You can create or modify a classifier control list that can be used only in GRE tunnel policy lists.

- Issue the **gre-tunnel classifier-list** command:

```
host1(config)#gre-tunnel classifier-list greClassifier50 color yellow  user-packet-class
  7 dsfield 40
```

Related Documentation

- Classifier Control Lists Overview on page 3
- Policy Lists Overview on page 7
- gre-tunnel classifier-list

Creating or Modifying Classifier Control Lists for IP Policy Lists

Tasks to create or modify classifier control lists for IP policy lists:

- Creating Classifier Control List for Only IP Policy Lists on page 14
- Setting Up an IP Classifier Control List to Accept Traffic from All Sources on page 15
- Classifying IP Traffic Based on Source and Destination Addresses on page 15
- Using IP Classifier Control Lists to Match Route Class Values on page 15
- Creating IP Classifier Control Lists for TCP and UDP Ports on page 15
- Creating an IP Classifier Control List That Matches the ToS Byte on page 16
- Creating an IP Classifier Control List That Filters ICMP Echo Requests on page 16
- Creating IP Classifier Control Lists That Use TCP or IP Flags on page 16
- Creating IP Classifier Control Lists That Match the IP Fragmentation Offset on page 16

Creating Classifier Control List for Only IP Policy Lists

You can create or modify a classifier control list that can be used only in IP policy lists. The behavior of multiple-element classifier-list classification is the logical OR of the elements in the CLACL.

- Issue the **ip classifier-list** command to match all packets that have a source IP address of 192.168.30.100 or have a destination IP address of 192.168.30.200:

```
host1(config)#ip classifier-list boston5 ip host 192.168.30.100 any
host1(config)#ip classifier-list boston5 ip any host 192.168.30.200
```

Setting Up an IP Classifier Control List to Accept Traffic from All Sources

You can set up a CLACL to accept IP traffic from all source addresses on the subnet.

- Issue the **ip classifier-list** command:

```
host1(config)#ip classifier-list XYZCorpPermit ip 192.168.0.0 0.0.255.255 any
```

Classifying IP Traffic Based on Source and Destination Addresses

You can classify traffic based on source and destination addresses, You can specify the address as a host address, or a subnet with a wildcard. If you specify the address as a subnet, the mask, in binary notation, must be a series of contiguous zeros, followed by a series of contiguous ones. The **any** keyword is the address wildcard, matching traffic for any address.

- Issue the **ip classifier-list** command to classify traffic on any source or destination address:

```
host1(config)#ip classifier-list YourListName ip any any
host1(config)#ip classifier-list YourListName ip host 10.10.10.10 any
host1(config)#ip classifier-list YourListName ip 10.10.0.0 0.0.255.255 host  10.10.10.2
```

Using IP Classifier Control Lists to Match Route Class Values

You can set up classifier control lists to match route-class values. In this example, svale20 matches the source address lookup route-class value of 1, svale30 matches the destination address lookup route-class value of 1 and a ToS byte value of 10, svale40 matches the source address lookup route-class value of 1 and the packets destined to a local interface, and west20 matches the source address lookup route-class value of 1 and packets that are not destined for a local interface (packets destined for remote interfaces).

- Issue the **ip classifier-list** command:

```
host1(config)#ip classifier-list svale20 source-route-class 1 ip any any
host1(config)#ip classifier-list svale30 destination-route-class 1 ip any any
   tos 10
host1(config)#ip classifier-list svale40 source-route-class 1 local true ip any any
host1(config)#ip classifier-list west20 source-route-class 1 local false ip any any
```

Creating IP Classifier Control Lists for TCP and UDP Ports

You can specify a single TCP or UDP port or a range of ports, where packets are matched with source address 198.168.30.100 and UDP source port numbers in the range 1–10.

- Issue the **ip classifier-list** command to create a CLACL on a UDP host:

```
host1(config)#ip classifier-list YourListName udp host 192.168.30.100 range 1  10 any
```

To create a CLACL that matches all traffic on UDP source ports greater than 100:

```
host1(config)#ip classifier-list XYZCorpUdp udp any gt 100 172.17.2.1  0.0.255.255
```

To match a non-TCP packet originating from IP address 172.28.100.52:

```
host1(config)#ip classifier-list YourListName not tcp host 172.28.100.52 any
```

To specify a single TCP or UDP port or range of ports, an ICMP code and optional type, or an IGMP type, which matches packets with source address 198.168.30.100 and ICMP type 2 and code 10:

```
host1(config)#ip classifier-list YourListName icmp host 192.168.30.100 any 2  10
```

Creating an IP Classifier Control List That Matches the ToS Byte

You can create an IP CLACL that matches the ToS byte in the IP header.

- Issue the **ip classifier-list** command using the **tos** keyword.

```
host1(config)#ip classifier-list tos128 ip any any tos 128
host1(config)#ip classifier-list low-drop-prec ip any any dsfield 10
host1(config)#ip classifier-list priority ip any any precedence 1
```

Creating an IP Classifier Control List That Filters ICMP Echo Requests

You can create a CLACL that filters all ICMP echo requests headed toward an access link under a denial-of-service attack.

- Issue the **ip classifier-list** command:

```
host1(config)#ip classifier-list XYZCorpIcmpEchoReqs icmp any any 8 0
host1(config)#ip classifier-list XYZCorpIgmpType1 icmp any any
```

Creating IP Classifier Control Lists That Use TCP or IP Flags

You can create CLACLs that use TCP or IP flags. For both IP flags and TCP flags, if you specify only a single flag, the logical equation does not require quotation marks.

- Issue the **ip classifier-list** command with the **tcp-flags** keyword and a logical equation (a quotation-enclosed string using ! for NOT, & for AND) to match one or more of the **ack, fin, psh, rst, syn, or urg TCP flags**:

```
host1(config)#ip classifier-list telnetConnects tcp 192.168.10.0 0.0.0.255 host
  10.10.10.10 eq 23 tcp-flags "syn & !ack"
```

- Issue the **ip classifier-list** command with the **ip-flags** keyword and a logical equation (a quotation-enclosed string using ! for NOT, & for AND) to match one or more of the **dont-fragment**, **more-fragments**,, or **reserved** IP flags:

```
host1(config)#ip classifier-list dontFragment ip any any ip-flags "dont-fragment"
```

Creating IP Classifier Control Lists That Match the IP Fragmentation Offset

You can create CLACLs that match the IP fragmentation offset.

- Issue the **ip classifier-list** command with the **ip-frag-offset** keyword and the **eq** or **gt** operator to match an IP fragmentation offset equal to 0, 1, or greater than 1:

```
host1(config)#ip classifier-list fragOffsetAttack ip any host 10.10.10.10  ip-frag-offset
  eq 1
host1(config)#ip policy-list dosProtect
```

```
host1(config-policy-list)#filter classifier-group fragOffsetAttack
host1(config-policy-list)#forward
```

Related Documentation

- Classifier Control Lists Overview on page 3
- ip classifier-list

Creating or Modifying Classifier Control Lists for IPv6 Policy Lists

You can create or modify a classifier control list that can be used only in IPv6 policy lists.

- Issue the **ipv6 classifier-list** command:

```
host1(config)#ipv6 classifier-list ipv6classifier color red user-packet-class 5  tcfield 10
host1(config)#ipv6 classifier-list YourListName udp destination-port eq 75
host1(config)#ipv6 classifier-list telnetConnects tcp destination-port eq 23  tcp-flags
   "syn & !ack"
host1(config)#ipv6 classifier-list listname icmpv6 icmp-type 3 icmp-code 6
host1(config)#ipv6 classifier-list listname icmpv6 icmp-type 3
host1(config)#ipv6 classifier-list svale20 source-route-class 1
host1(config)#ipv6 classifier-list svale30 destination-route-class 1 tcfield 10
host1(config)#ipv6 classifier-list svale40 source-route-class 1 local true
host1(config)#ipv6 classifier-list west25 source-route-class 1 local false
host1(config)#ipv6 classifier-list YourClaclList source-host 2001:db8:1::8001
   destination-address 2001:db8:3::/48
```

Related Documentation

- Classifier Control Lists Overview on page 3
- Policy Lists Overview on page 7
- ipv6 classifier-list

Creating or Modifying Classifier Control Lists for L2TP Policy Lists

You can create or modify a classifier control list that can be used only in L2TP policy lists.

- Issue the **l2tp classifier-list** command:

```
host1(config)#l2tp classifier-list l2tpclassifier color red user-packet-class 7
```

Related Documentation

- Classifier Control Lists Overview on page 3
- Policy Lists Overview on page 7
- l2tp classifier-list

Creating or Modifying Classifier Control Lists for MPLS Policy Lists

You can create or modify a classifier control list that can be used only in MPLS policy lists.

- Issue the **mpls classifier-list** command:

```
host1(config)#mpls classifier-list mplsClass user-packet-class 10 exp-bits 3 exp-mask
  5
```

Related Documentation

- Classifier Control Lists Overview on page 3
- Policy Lists Overview on page 7
- mpls classifier-list

Creating or Modifying Classifier Control Lists for VLAN Policy Lists

You can create or modify a classifier control list that can be used only in VLAN policy lists.

- Issue the **vlan classifier-list** command:

```
host1(config)#vlan classifier-list lowLatencyLowDrop user-priority 7
host1(config)#vlan classifier-list lowLatencyLowDrop user-priority 6
host1(config)#vlan classifier-list lowLatency user-priority 5
host1(config)#vlan classifier-list excellentEffort user-priority 4
host1(config)#vlan classifier-list bestEffort user-priority 3
host1(config)#vlan classifier-list bestEffort user-priority 2
host1(config)#vlan classifier-list bestEffort user-priority 1
host1(config)#vlan classifier-list bestEffort user-priority 0
```

NOTE: You cannot configure classifier control lists (CLACLs) for policy lists to be attached to VLAN interfaces, without specifying the criteria by which the router defines a packet flow. Although the carriage return, **<cr>**, option is displayed when you type a question mark (**?**) after entering the **vlan classifier list** *classifierName* command without defining any other keyword or CLACL criterion, an error message is displayed when you press **Enter** to configure the VLAN CLACL with only the name. You must specify at least one criterion for the VLAN CLACL to be successfully configured.

Related Documentation

- Classifier Control Lists Overview on page 3
- Policy Lists Overview on page 7
- vlan classifier-list

CHAPTER 4

Configuration Tasks for Creating Policy Lists

Creating Policy Lists for ATM

In the following example, you create two policies: one for CBR traffic and one for UBR traffic. One policy is attached to an interface that contains CBR traffic and the other to an interface that contains UBR traffic.

1. Create a CBR policy list.

   ```
   host1(config)#atm policy-list polCbr
   host1(config-policy-list)#
   ```

2. Create the classification group and assign a strict priority traffic class and color green.

   ```
   host1(config-policy-list)#classifier-group *
   host1(config-policy-list-classifier-group)#traffic-class strict-priority
   host1(config-policy-list-classifier-group)#color green
   ```

3. Exit Policy List Configuration mode to save the configuration.

   ```
   host1(config-policy-list-classifier-group)#exit
   host1(config-policy-list)#exit
   host1(config)#
   ```

4. Create a UBR policy that maps to the strict best-effort traffic class and color red.

   ```
   host1(config)#atm policy-list polUbr
   host1(config-policy-list)#classifier-group *
   ```

```
host1(config-policy-list-classifier-group)#traffic-class best-effort
host1(config-policy-list-classifier-group)#color red
```

5. Exit Policy List Configuration mode to save the configuration.

```
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#exit
host1(config)#
```

6. Attach the policies to ATM subinterfaces.

```
host1(config)#interface atm 0/0.100
host1(config-if)#atm policy input polUbr statistics enabled
host1(config-if)#exit
host1(config)#interface atm 0/0.101
host1(config-if)#atm policy input polCbr statistics enabled
host1(config-if)#exit
```

7. Display the policy lists.

```
host1#show atm subinterface atm 0/0.100
Circuit                   Interface
 Interface  ATM-Prot VCD VPI VCI  Type   Encap MTU  Status   Type
----------- -------- --- --- --- ------- ----- ---- ------ ---------
ATM 0/0.100 RFC-1483 100   0 100 PVC     SNAP  9180 up     Static

Auto configure status         : static
Auto configure interface(s)   : none
Detected 1483 encapsulation   : none
Detected dynamic interface    : none
Interface types in lockout    : none

Assigned profile (IP)         : none assigned
Assigned profile (BridgedEnet): none assigned
Assigned profile (PPP)        : none assigned
Assigned profile (PPPoE)      : none assigned
Assigned profile (any)        : none assigned

SNMP trap link-status: disabled

InPackets:                0
InBytes:                  0
OutPackets:               0
OutBytes:                 0
InErrors:                 0
OutErrors:                0
InPacketDiscards:         0
InPacketsUnknownProtocol: 0
OutDiscards:              0
ATM policy input polUbr
  Statistics are disabled
1 interface(s) found

host1#show atm subinterface atm 0/0.101
                                  Circuit                   Interface
 Interface  ATM-Prot VCD VPI VCI  Type   Encap MTU  Status   Type
----------- -------- --- --- --- ------- ----- ---- ------ ---------
ATM 0/0.101 RFC-1483 101   0 101 PVC     SNAP  9180 up     Static

Auto configure status         : static
Auto configure interface(s)   : none
```



```
Detected 1483 encapsulation   : none
Detected dynamic interface    : none
Interface types in lockout    : none

Assigned profile (IP)         : none assigned
Assigned profile (BridgedEnet): none assigned
Assigned profile (PPP)        : none assigned
Assigned profile (PPPoE)      : none assigned
Assigned profile (any)        : none assigned

SNMP trap link-status: disabled

InPackets:                0
InBytes:                  0
OutPackets:               0
OutBytes:                 0
InErrors:                 0
OutErrors:                0
InPacketDiscards:         0
InPacketsUnknownProtocol: 0
OutDiscards:              0
ATM policy input polCbr
  classifier-group *
    3096 packets, 377678 bytes
    traffic-class best-effort
    color green
1 interface(s) found
```

Related Documentation

- Creating or Modifying Classifier Control Lists for ATM Policy Lists on page 13
- atm policy-list

Creating Policy Lists for Frame Relay

The following example creates a Frame Relay policy that on egress marks the DE bit to 1, and on ingress colors frames with a DE bit of 1 as red.

1. Create the policy list used to mark egress traffic, then create the classifier group for packets conforming to CLACL frMatchDeSet. Add a rule that marks the DE bit as 1.

   ```
   host1(config)#frame-relay policy-list frOutputPolicy
   host1(config-policy-list)#classifier-group frMatchDeSet
   host1(config-policy-list-classifier-group)#mark-de 1
   host1(config-policy-list-classifier-group)#exit
   host1(config-policy-list)#exit
   ```

2. Create the policy list used for the ingress traffic. and create the classifier group conforming to CLACL frMatchDeSet. Add a rule that colors the ingress traffic.

   ```
   host1(config)#frame-relay policy-list frInputPolicy
   host1(config-policy-list)#classifier-group frGroupA
   host1(config-policy-list-classifier-group)#color red
   host1(config-policy-list-classifier-group)#exit
   host1(config-policy-list)#exit
   ```

3. Apply the policy lists.

   ```
   host1(config)#interface serial 5/0:1/1.1
   host1(config-subif)#frame-relay policy output frOutputPolicy statistics enabled
   ```

```
host1(config-subif)#ip address 10.0.0.1 255.255.255.0
host1(config-subif)#exit
host1(config)#interface serial 5/1:1/1.1
host1(config-subif)#frame-relay policy input frInputPolicy statistics enabled
host1(config-subif)#exit
```

4. Display interface information to view the applied policies.

```
host1#show frame-relay subinterface

Frame relay sub-interface SERIAL5/0:1/1.1, status is up
Number of sub-interface down transitions is 0
Time since last status change 03:04:59
No baseline has been set
  In bytes: 660                    Out bytes: 660
  In frames: 5                     Out frames: 5
  In errors: 0                     Out errors: 0
  In discards: 0                   Out discards: 0
  In unknown protos: 0
Frame relay policy output frOutputPolicy
  classifier-group frGroupA entry 1
     5 packets, 640 bytes
     mark-de 1
Frame relay sub-interface SERIAL5/1:1/1.1, status is up
Number of sub-interface down transitions is 0
Time since last status change 03:05:09
No baseline has been set
  In bytes: 660                    Out bytes: 660
  In frames: 5                     Out frames: 5
  In errors: 0                     Out errors: 0
  In discards: 0                   Out discards: 0
  In unknown protos: 0
Frame relay policy input frInputPolicy
  classifier-group frMatchDeSet entry 1
     5 packets, 660 bytes
     color red
```

5. Display the classifier list.

```
host1#show classifier-list detailed

                        Classifier Control List Table
                        ---------- ------- ---- -----
Frame relay Classifier Control List frMatchDeSet
   Reference count:      1
   Entry count:          1

   Classifier-List frMatchDeSet Entry 1
      DE Bit:                    1
```

6. Display the policy lists.

```
host1#show policy-list

                                  Policy Table
                                  ------ -----

Frame relay Policy frOutputPolicy
   Administrative state: enable
   Reference count:      0
   Classifier control list: frMatchDeSet, precedence 100
      mark-de 1
```



```
Frame relay Policy frInputPolicy
   Administrative state: enable
   Reference count:      0
   Classifier control list: frGroupA, precedence 100
     color red
```

Related Documentation

- Creating or Modifying Classifier Control Lists for Frame-Relay Policy Lists on page 13
- frame-relay policy-list

Creating Policy Lists for GRE Tunnels

The following example creates a GRE tunnel policy list named routeGre50. For information about creating the CLACL used in this example, see the previous sections.

1. Create the policy list routeGre50.

   host1(config)#gre-tunnel policy-list routeGre50

2. Create the classification group for the CLACL named gre8 and assign a precedence of 150 to it.

   host1(config-policy-list)#classifier-group gre8 precedence 150
   host1(config-policy-list-classifier-group)#

3. Add two rules for traffic based on the CLACL named gre8: one rule to color packets as red, and a second rule that specifies the ToS DS field value to be assigned to the packets.

   host1(config-policy-list-classifier-group)#color red
   host1(config-policy-list-classifier-group)#mark dsfield 20
   host1(config-policy-list-classifier-group)#

4. Exit Policy List Configuration mode to save the configuration.

   host1(config-policy-list-classifier-group)#exit
   host1(config-policy-list)#exit
   host1(config)#

5. Display the policy list.

   host1#show policy-list routeGre50

```
                                  Policy Table
                                  ------ -----
GRE Tunnel Policy routeGre50
   Administrative state: enable
   Reference count:      0
   Classifier control list: gre8, precedence 150
      color red
      mark dsfield 20
```

Related Documentation

- Creating or Modifying Classifier Control Lists for GRE Tunnel Policy Lists on page 14
- gre-tunnel policy-list

Creating Policy Lists for IP

The following example creates an IP policy list named routeForABCCorp. For information about creating the CLACLs and rate-limit profile used in this example, see the previous sections.

1. Create the policy list routeForABCCorp.

   ```
   host1(config)#ip policy-list routeForABCCorp
   host1(config-policy-list)#
   ```

2. Create the classification group for the CLACL named ipCLACL10 and assign the precedence to the classification group.

   ```
   host1(config-policy-list)#classifier-group ipCLACL10 precedence 75
   host1(config-policy-list-classifier-group)#
   ```

3. Add a rule that specifies a group of forwarding solutions based on classifier list ipCLACL10.

   ```
   host1(config-policy-list-classifier-group)#forward next-hop 192.0.2.12 order 10
   host1(config-policy-list-classifier-group)#forward next-hop 192.0.100.109
     order 20
   host1(config-policy-list-classifier-group)#forward next-hop 192.120.17.5 order 30
   host1(config-policy-list-classifier-group)#forward interface ip 3/1 order 40
   ```

4. Add a rule that sets a ToS byte value of 125 for packets based on classifier list ipCLACL10.

   ```
   host1(config-policy-list-classifier-group)#mark tos 125
   ```

5. Add a rule that uses rate-limit profile ipRLP25.

   ```
   host1(config-policy-list-classifier-group)#rate-limit-profile ipRLP25
   ```

6. Exit Classifier Group Configuration mode for ipCLACL10, then create a new classification group for classifier list ipCLACL20. Add a rule that filters packets based on classifier list ipCLACL20.

   ```
   host1(config-policy-list-classifier-group)#exit
   host1(config-policy-list)#classifier-group ipCLACL20 precedence 125
   host1(config-policy-list-classifier-group)#filter
   ```

7. Exit Policy List Configuration mode to save the configuration.

   ```
   host1(config-policy-list-classifier-group)#exit
   host1(config-policy-list)#exit
   host1(config)#
   ```

8. Display the policy list.

   ```
   host1#show policy-list routeForABCCorp

                                    Policy Table
                                    ------ -----
   IP Policy routeForABCCorp
      Administrative state: enable
      Reference count:      0
      Classifier control list: ipCLACL10, precedence 75
         forward
   ```

```
      Virtual-router: default
      List:
        next-hop 192.0.2.12, order 10, rule 2 (active)
        next-hop 192.0.100.109, order 20, rule 3 (reachable)
        next-hop 192.120.17.5, order 30, rule 4 (reachable)
        interface ip3/1, order 40, rule 5
    mark tos 125
    rate-limit-profile ipRLP25
Classifier control list: ipCLACL20, precedence 125
    filter
```

Related Documentation

- Creating or Modifying Classifier Control Lists for IP Policy Lists on page 14
- Creating Multiple Forwarding Solutions with IP Policy Lists
- ip policy-list

Creating Policy Lists for IPv6

The following example creates an IPv6 policy list named routeForIPv6. For information about creating the CLACL used in this example, see the previous sections.

1. Create the policy list routeForIPv6.

   ```
   host1(config)#ipv6 policy-list routeForIPv6
   host1(config-policy-list)#
   ```

2. Create the classification group for the CLACL named ipv6tc67 and assign the precedence to the classification group.

   ```
   host1(config-policy-list)#classifier-group ipv6tc67 precedence 75
   host1(config-policy-list-classifier-group)#
   ```

3. Add a rule to color packets as red, and a second rule that sets the traffic class field of the packets to 7.

   ```
   host1(config-policy-list-classifier-group)#color red
   host1(config-policy-list-classifier-group)#mark tcfield 7
   ```

4. Add a rule that specifies a group of forwarding solutions based on classifier control list ipv6tc67.

   ```
   host1(config-policy-list-classifier-group)#forward next-hop 3001:82ab:1020:87ec::/64
     order 10
   host1(config-policy-list-classifier-group)#forward next-hop 2001:82ab:1020:87ec::/64
     virtual-router vr1 ignore-default-route order 20
   ```

5. Exit Policy List Configuration mode to save the configuration.

   ```
   host1(config-policy-list-classifier-group)#exit
   host1(config-policy-list)#exit
   host1(config)#
   ```

6. Display the policy list.

   ```
   host1#show policy-list routeForIPv6

                                      Policy Table
                                      ------ -----
   IPv6 Policy routeForIPv6
   ```

```
  Administrative state: enable
  Reference count:      0
  Classifier control list: C1, precedence 90
  Classifier control list: ipv6tc67, precedence 75
     forward
        Virtual-router: default
        List:
          next-hop 3001:82ab:1020:87ec::/64, order 10, rule 2 (active)
        Virtual-router: vr1
        List:
          next-hop 2001:82ab:1020:87ec::/64, ignore-default-route, order 20,
rule 3
     color red
     mark tc-precedence 7
```

You use the **exception http-redirect** command to create an exception rule within a policy classifier group to specify the client application for the destination of packets rather than forwarding them using the forwarding controller (FC).

In lower-numbered releases, the **exception http-redirect** command only supported the creation of exception rules within IPv4 policy lists. You can now configure the **exception http-redirect** command to create exception rules within IPv4 and IPv6 policy lists.

The following example creates an IPv6 policy list, **epIPv6** for the http-redirect exception:

1. Create the policy list epIPv6.

   ```
   host1(config)#ipv6 policy-list epIPv6
   host1(config-policy-list)#
   ```

2. Create the classification group to match all packets.

   ```
   host1(config-policy-list)#classifier-group *
   host1(config-policy-list-classifier-group)#
   ```

3. Create an exception policy for http-redirect.

   ```
   host1(config-policy-list-classifier-group)#exception http-redirect
   ```

4. Exit Policy List Configuration mode to save the configuration.

   ```
   host1(config-policy-list-classifier-group)#exit
   host1(config-policy-list)#exit
   host1(config)#
   ```

5. Display the policy list.

   ```
   host1#show policy-list epIPv6
                                    Policy Table
                                    ------ -----
   IPv6 Policy epIPv6
      Administrative state: enable
      Reference count:      0
      Classifier control list: *, precedence 100
         exception http-redirect
   ```

Related Documentation

- Creating or Modifying Classifier Control Lists for IPv6 Policy Lists on page 17
- ipv6 policy-list

- exception http-redirect

Creating Policy Lists for L2TP

The following example creates an L2TP policy list.

1. Create the policy list routeForl2tp.

   ```
   host1(config)#l2tp policy-list routeForl2tp
   host1(config-policy-list)#
   ```

2. Create the classification group to match all packets.

   ```
   host1(config-policy-list)#classifier-group *
   host1(config-policy-list-classifier-group)#
   ```

3. Add a rule to color packets as red, and a second rule that uses the rate-limit profile l2tpRLP10.

   ```
   host1(config-policy-list-classifier-group)#color red
   host1(config-policy-list-classifier-group)#rate-limit-profile l2tpRLP10
   ```

4. Exit Policy List Configuration mode to save the configuration.

   ```
   host1(config-policy-list-classifier-group)#exit
   host1(config-policy-list)#exit
   host1(config)#
   ```

5. Display the policy list.

   ```
   host1#show policy-list routeForl2tp

                                    Policy Table
                                    ------ -----
   L2TP Policy routeForl2tp
      Administrative state: enable
      Reference count:      0
      Classifier control list: *, precedence 100
         color red
         rate-limit-profile l2tpRLP20
   ```

Related Documentation

- Creating or Modifying Classifier Control Lists for L2TP Policy Lists on page 17
- l2tp policy-list

Creating Policy Lists for MPLS

The following example creates an MPLS policy list.

1. Create the policy list routeForMpls.

   ```
   host1(config)#mpls policy-list routeForMpls
   host1(config-policy-list)#
   ```

2. Create the classification group.

   ```
   host1(config-policy-list)#classifier-group * precedence 200
   host1(config-policy-list-classifier-group)#
   ```

3. Add one rule that sets the EXP bits for all packets to 2, and a second rule that uses the rate-limit profile mplsRLP

```
host1(config-policy-list-classifier-group)#mark-exp 2
host1(config-policy-list-classifier-group)#rate-limit-profile mplsRLP5
```

4. Exit Policy List Configuration mode to save the configuration.

```
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#exit
host1(config)#
```

5. Display the policy list.

```
host1#show policy-list routeForMpls

                                    Policy Table
                                    ------ -----
MPLS Policy routeForMpls
   Administrative state: enable
   Reference count:      0
   Classifier control list: *, precedence 200
      mark-exp 2 mask 7
      rate-limit-profile mplsRLP5
```

NOTE: In JunosE releases numbered lower than 11.3.x, when you attached a QoS profile to an interface configured for MPLS on an ES2 10G LM, the egress traffic from the MPLS interface that was classified as non-best-effort traffic was forwarded using the best-effort queue. In higher-numbered releases, when an output policy is specified with a non-best-effort traffic class and applied on an MPLS interface, the correct traffic class is used to classify and forward outgoing packets from the interface. For example, when an output policy is applied on an MPLS interface configured with a non-best-effort class, the outgoing traffic from the interface is correctly categorized according to the defined traffic class and does not use the best-effort queue.

Related Documentation

- Creating or Modifying Classifier Control Lists for MPLS Policy Lists on page 17
- mpls policy-list

Creating Policy Lists for VLANs

The following example creates a VLAN policy list named routeForVlan. The classifier group lowLatencyLowDrop uses the default precedence of 100.

1. Create the policy list routeForVlan.

```
host1(config)#vlan policy-list routeForVlan
host1(config-policy-list)#
```

2. Create the classification group.

```
host1(config-policy-list)#classifier-group lowLatencyLowDrop
host1(config-policy-list-classifier-group)#
```

3. Create a rule that adds the lowLatencyLowDrop traffic class for all packets that fall into the lowLatencyLowDrop classification.

   host1(config-policy-list-classifier-group)#traffic-class lowLatencyLowDrop

4. Add a rule that sets the drop precedence for all packets that fall into the lowLatencyLowDrop classification to green.

   host1(config-policy-list-classifier-group)#color green

5. Add a rule that sets the user-priority bits for all packets that fall into the lowLatencyLowDrop classification to 7.

   host1(config-policy-list-classifier-group)#mark-user-priority 7

6. Exit to Policy List Configuration mode, then add traffic class rules for packets that conform to different CLACLs.

   host1(config-policy-list-classifier-group)#exit
   host1(config-policy-list)#classifier-group lowLatency
   host1(config-policy-list-classifier-group)#traffic-class lowLatency
   host1(config-policy-list-classifier-group)#exit
   host1(config-policy-list)#classifier-group excellentEffort
   host1(config-policy-list-classifier-group)#traffic-class excellentEffort
   host1(config-policy-list-classifier-group)#exit
   host1(config-policy-list)#classifier-group bestEffort
   host1(config-policy-list-classifier-group)#traffic-class bestEffort

7. Exit Policy List Configuration mode to save the configuration.

   host1(config-policy-list-classifier-group)#exit
   host1(config-policy-list)#exit
   host1(config)#

8. Display the policy list.

   host1#show policy-list routeForVlan

```
                                  Policy Table
                                  ------ -----
VLAN Policy routeForVlan
   Administrative state: enable
   Reference count:      0
   Classifier control list: lowLatencyLowDrop, precedence 100
      traffic-class lowLatencyLowDrop
      color green
      mark-user-priority 7
   Classifier control list: lowLatency, precedence 100
      traffic-class lowLatency
   Classifier control list: excellentEffort, precedence 100
      traffic-class excellentEffort
   Classifier control list: bestEffort, precedence 100
      traffic-class bestEffort
```

Related Documentation

- Creating or Modifying Classifier Control Lists for VLAN Policy Lists on page 18
- vlan policy-list

Configuring Statistics Collection for Output Policies on Tunnel Interfaces

To enable collection and preservation of statistics for output policies on tunnel interfaces based on fragments:

- From Global Configuration mode, enable the capability to collect output policy statistics for tunnel interfaces based on the number of fragments.

```
host1(config)#enable-frag-stats
```

To enable collection and preservation of statistics for output policies on tunnel interfaces based on packets:

- From Global Configuration mode, enable the capability to collect output policy statistics for tunnel interfaces based on packets. By default, output policy counters are computed based on the number of packets.

```
host1(config)#no enable-frag-stats
```

You cannot configure fragment-based collection of output policy statistics for tunnel interfaces that are managed by the SRC client running on the router. The fragment-based statistics collection functionality is preserved across unified ISSU, stateful SRP switchover, and stateful line module switchover operations.

You can use the **show enable-frag-stats** command to verify whether collection of output policy statistics for traffic on tunnel interfaces is enabled.

Related Documentation

- Statistics Collection for Output Policies on Tunnel Interfaces Overview on page 8
- Verifying Statistics Collection for Output Policies on Tunnel Interfaces on page 66
- enable-frag-stats
- show enable-frag-stats

PART 3

Administration

CHAPTER 5

Monitoring Tasks for Classifier Control Lists

Monitoring Classifier Control Lists

Purpose Display a list of classifier control lists or details of classifier control lists.

Action To display a list of CLACLs:

```
host1#show classifier-list

                        Classifier Control List Table
                        ---------- ------- ---- -----
GRE Tunnel greClass.1
VLAN lowLatencyLowDrop.1
VLAN excellentEffort.1
VLAN bestEffort.1
VLAN lowLatency.1
IP wstFd.1 source-route-class 44 destination-route-class 55 3 any any
IP XYZCorpPermit.1 local true color green ip any any
IP routeForXYZCorp.1 color red tcp any any
IP XYZCorpIcmpEchoRequests.1 ip any any
IP XYZCorpPrecedence.1 tcp any any tos 5
IP XYZCorpPrecedence67.1 udp any any
IPv6 IPv6Precedence.1 color yellow
IPv6 IPv6Precedence67.1
L2TP l2tpclass.1 color green user-packet-class 8
MPLS mplsClass.1 user-packet-class 10 exp-bits 3 exp-mask 7
Frame relay frMatchDeSet.7 user-packet-class 8 de-bit 0
```

To display details of each CLACL:

```
host1#show classifier-list detailed

                        Classifier Control List Table
                        ---------- ------- ---- -----
IP Classifier Control List XYZCorpPermit
   Reference count:      1
   Entry count:          1

   Classifier-List XYZCorpPermit Entry 1
      Color:                     green
      Protocol:                  ip
      Not Protocol:              false
      Source IP Address:         0.0.0.0
```

```
      Source IP WildcardMask:     255.255.255.255
      Not Source Ip Address:      false
      Destination IP Address:     0.0.0.0
      Destination IP WildcardMask:255.255.255.255
      Not Destination Ip Address: false

GRE Tunnel Classifier Control List greClass
   Reference count:      0
   Entry count:          2

   Classifier-List greClass Entry 1
      User Packet Class:          8
      DS Field:                   3

   Classifier-List greClass Entry 2
      Color:                      yellow

VLAN Classifier Control List bestEffort
   Reference count:      0
   Entry count: 1

   Classifier-List bestEffort Entry 1
      Color:                      red
      User Packet Class:          15
      User Priority bits:         7

IPv6 Classifier Control List IPv6Classifier
   Reference count:      0
   Entry count:          1

   Classifier-List IPv6Classifier Entry 1
      User Packet Class:          3
      Traffic Class Field:        200

L2TP Classifier Control List l2tpclass
   Reference count:      0
   Entry count:          1

   Classifier-List l2tpclass Entry 1
      Color:                      green
      User Packet Class:          8

MPLS Classifier Control List mplsClass
   Reference count:      0
   Entry count:          1

   Classifier-List mplsClass Entry 1
      User Packet Class:          10
      EXP Bits:                   3
      EXP Mask:                   7
Frame relay Classifier Control List frMatchDeSet
   Reference count:      2
   Entry count:          1

   Classifier-List frMatchDeSet Entry 7
      Traffic Class:              toBoston
      User Packet Class:          8
      DE Bit:                     0
```

Meaning Table 4 on page 35 lists the **show classifier-list** command output fields.

Table 4: show classifier-list Output Fields

Field Name	Field Description
Reference count	Number of times the CLACL is referenced by policies
Entry count	Number of entries in the classifier list
Classifier-List	Name of the classifier list
Entry	Entry number of the classifier list rule
Color	Packet color to match: green, yellow, or red
Protocol	Protocol type
Not Protocol	If true, matches any protocol except the preceding protocol; if false, matches the preceding protocol
Source IP Address	Address of the network or host from which the packet is sent
Source IP WildcardMask	Mask that indicates addresses to be matched when specific bits are set
Not Source Ip Address	If true, matches any source IP address and mask except the preceding source IP address and mask; if false, matches the preceding source IP address and mask
Destination IP Address	Number of the network or host from which the packet is sent
Destination IP WildcardMask	Mask that indicates addresses to be matched when specific bits are set
Not Destination Ip Address	If true, matches any destination IP address and mask except the preceding destination IP address and mask; if false, matches the preceding destination IP address and mask
Traffic Class	Name of the traffic class to match
User Packet Class	User packet value to match
DS Field	DS field value to match
TOS Byte	ToS value to match
Precedence	Precedence value to match

Table 4: show classifier-list Output Fields *(continued)*

Field Name	Field Description
User Priority bits	User priority bits value to match
Traffic Class Field	Traffic class field value to match
EXP Bits	MPLS EXP bit value to match
EXP Mask	Mask applied to EXP bits before matching
DE Bit	Frame Relay DE bit value to match
Destination Route Class	Route class used to classify packets based on the packet's destination address
Source Route Class	Route class used to classify packets based on the packet's source address
Local	If true, matches packets destined to a local interface; if false, matches packets that are traversing the router

Related Documentation

- show classifier-list

CHAPTER 6

Monitoring Tasks for Policy Lists

Monitoring Policy Lists

Purpose Display information about policy lists.

Action To display policy lists:

```
host1#show policy-list
                                    Policy Table
                                    ------ -----
IPv6 Policy ipv6-pol8
   Administrative state: enable
   Reference count:      2
   Classifier control list: *, precedence 100
      forward
         Virtual-router: default
         List:
           next-hop 3001:82ab:1020:87ec::/64, order 10, rule 2 (active)
         Virtual-router: vr1
         List:
           next-hop 2001:82ab:1020:87ec::/64, ignore-default-route, order 20,
           rule 3

   Referenced by interface(s):
      GigabitEthernet1/0/2.1  input policy, statistics enabled, virtual-router
default
```

```
      GigabitEthernet1/0/2.1  output policy, statistics enabled, virtual-router
default

   Referenced by profile(s):
      None

   Referenced by merged policies:
      None

IP Policy routeForABCCorp
   Administrative state: enable
   Reference count:      0
 atm-cell-mode: enabled
Classifier control list: ipCLACL10, precedence 75
 exception http-redirect
 forward
Virtual-router: default
         List:
           next-hop 192.0.2.12, order 10, rule 2 (active)
           next-hop 192.0.100.109, order 20, rule 3 (reachable)
           next-hop 192.120.17.5, order 30, rule 4 (reachable)
           interface ip3/1, order 40, rule 5
      mark tos 125
      rate-limit-profile ipRLP25
   Classifier control list: ipCLACL20, precedence 125
      filter

IPv6 Policy routeForIPv6
   Administrative state: enable
   Reference count:      0
   Classifier control list: ipv6tc67, precedence 75
      forward
         Virtual-router: default
         List:
           next-hop 3001:82ab:1020:87ec::/64, order 10, rule 2 (active)
         Virtual-router: vr1
         List:
           next-hop 2001:82ab:1020:87ec::/64, ignore-default-route, order 20,
rule 3
      color red
      mark tc-precedence 7

Frame relay Policy frOutputPolicy
   Administrative state: enable
   Reference count:      0
   Classifier control list: frMatchDeSet, precedence 100
      mark-de 1

Frame relay Policy frInputPolicy
   Administrative state: enable
   Reference count:      0
   Classifier control list: frMatchDeSet, precedence 100
      color red

GRE Tunnel Policy routeGre50
   Administrative state: enable
   Reference count:      0
   Classifier control list: gre8, precedence 150
      color red
      mark dsfield 20
      filter
```



```
L2TP Policy routeForl2tp
   Administrative state: enable
   Reference count:      0
   Classifier control list: *, precedence 100
      color red
      rate-limit-profile l2tpRLP20

MPLS Policy routeForMpls
   Administrative state: enable
   Reference count:      0
   Classifier control list: *, precedence 200
      mark-exp 2 mask 7
      rate-limit-profile mplsRLP5

VLAN Policy routeForVlan
   Administrative state: enable
   Reference count:      0
   Classifier control list: lowLatencyLowDrop, precedence 100
      traffic-class lowLatencyLowDrop
      color green
      mark-user-priority 7
   Classifier control list: lowLatency, precedence 100
      traffic-class lowLatency (suspended)
   Classifier control list: excellentEffort, precedence 100
      traffic-class excellentEffort
   Classifier control list: bestEffort, precedence 100
      traffic-class bestEffort
```

To display component policies:

```
host 1#show policy-list comp_p1

                                  Policy Table
                                  ------ -----
IP Policy comp_p1
   Administrative state: enable
   Reference count:      7
   Classifier control list: C1, precedence 90
      forward
         Virtual-router: default
         List:
           next-hop 10.1.1.1, order 100, rule 2 (active)
   Classifier control list: C2, precedence 10
      filter

   Referenced by interfaces:
      ATM3/0.3  input policy, statistics enabled, virtual-router vr1
      ATM3/0.4  output policy, statistics disabled, virtual-router vr1
      ATM3/0.5  secondary-input policy, statistics enabled, virtual-router vr1

   Referenced by profiles:
      prof_1  input policy, statistics disabled

   Referenced by merge policies:
      mpl_10
      mpl_11
      mpl_12

host1#show policy-list comp_p2

                                  Policy Table
                                  ------ -----
IP Policy comp_p2
   Administrative state: enable
   Reference count:      1
```

```
   Classifier control list: C1, precedence 90
      color red
   Classifier control list: *, precedence 1000
      filter

   Referenced by interfaces:
      ATM4/0.5  input policy, statistics enabled, virtual-router default

   Referenced by profiles:
      None

   Referenced by merge policies:
      None
```

To display component policies:

```
host1#show policy-list mpl_10

                                  Policy Table
                                  ------ -----

IP Policy mpl_10
   Administrative state: enable
   Reference count:      1
   Classifier control list: C1, precedence 90
      forward
         Virtual-router: default
         List:
           next-hop 10.1.1.1, order 100, rule 2 (active)
           next-hop 20.1.1.1, order 100, rule 3 (reachable)
   Classifier control list: C2, precedence 10
      filter
   Classifier control list: C3, precedence 10
      filter
   Classifier control list: *, precedence 1000
      forward

   Referenced by interfaces:
      ATM5/0.1  input policy, statistics enabled, virtual-router default

   Referenced by profiles:
      None

   Component policies:
      comp_p1
      comp_p3
```

To display the configuration of an IP policy list that contains inactive references to the interface to which it is attached:

```
host1#show policy-list pv4

                                 Policy Table
                                  ------ -----
IP Policy pv4
   Administrative state: enable
   Reference count:      2 (*)
   Classifier control list: cv4, precedence 100
      forward
   Classifier control list: *, precedence 100
      filter

   Referenced by interface(s):
      GigabitEthernet12/1.0  input policy, statistics disabled, virtual-router
default
```



```
   Referenced by profile(s):
      None

   Referenced by merged policies:
      None
```

To display rate limit hierarchy in one policy:

```
host1#show policy-list P1

                                  Policy Table
                                  ------ -----
IP Policy P1
   Administrative state: enable
   Reference count:      2
   Classifier control list: A, precedence 100, parent-group X
      rate-limit-profile A
mark profile A
   Classifier control list: B, precedence 100, parent-group X
      rate-limit-profile B
mark profile B
   Classifier control list: *, precedence 100, parent-group Z
mark profile D
      forward
   Parent group: X, parent-group Z
      rate-limit-profile X
   Parent group: Z
      rate-limit-profile Z

   Referenced by interface(s):
      SERIAL4/0  input policy, statistics disabled, virtual-router default
      SERIAL4/1  input policy, statistics disabled, virtual-router default

   Referenced by profile(s):
      No profile references
```

Meaning Table 5 on page 41 lists the **show policy-list** command output fields.

Table 5: show policy-list Output Fields

Field Name	Field Description
Policy	Name of the policy list.
Administrative state	For SNMP use; state is enabled when the policy list is created. Users modifying the policy list commands via telnet see the state as disabled. Modifications of a policy are not applied to an interface until the administrative state is first disabled and then reenabled.
Reference count	Number of attachments to interfaces or profiles. An asterisk enclosed in parenthesis (*), if displayed, denotes that the policy contains inactive references to interfaces. The absence of an asterisk denotes that all the attachments of this policy to the specified number of interfaces are active.

Table 5: show policy-list Output Fields *(continued)*

Field Name	Field Description
Atm cell mode	State of mode for ATM cell tax used in rate calculations.
Referenced by interfaces	List of interfaces to which policy is attached and is active; indicates whether the attachment is at input or output of interface.
Referenced by profiles	List of profiles to which policy is attached; indicates whether the attachment is at input, secondary-input, or output of interface created by the profile.
Referenced by merge policies	List of merged policies.
Referenced by component policies	List of component policies.
Classifier control list	Name of the classifier control list containing policy rules and the precedence assigned to the classifier control list.
Statistics	Enabled, disabled
Parent group	Name of the parent group.
Rule types are:	
filter	Filter policy action
exception http-redirect	HTTP redirect policy action
forward	Forward policy action
next-interface	Next-interface policy action
next-hop	Next-hop policy action
rate-limit-profile	Rate-limit-profile policy action
color	Color of a packet; green, yellow, or red
traffic-class	Traffic class in a policy list
log	Log policy action
mark tos	ToS byte in the IP header to a specified value
mark DS field	DS field value in the IP header to a specified value

Table 5: show policy-list Output Fields *(continued)*

Field Name	Field Description
mark TC precedence	Traffic class value in the IPv6 header to a specified value
mark EXP	Value assigned to EXP bits action
mark user priority	Value assigned to 802.1p VLAN user priority bit
mark DE	DE bit action
Rule status	Indicates whether the rule is suspended.

Related Documentation

- show policy-list

Monitoring Policy List Parameters

Purpose Display information about policy list parameters.

Action To display policy list information for a hierarchical policy:

```
host1#show policy-parameter
Policy Parameter hierGroup1
    Type: hierarchical
    Reference count: 8
    Aggregation node: vlan
    Referenced by interfaces: 2 references
      IP ATM5/0.1: atm-vc
      IP ATM5/0.2: 5

    Referenced by profiles: 1 references
      profile1

    Referenced by policies: 5 references
      policy1
      policy2
      policy3
Policy Parameter hierGroup2
    Type: hierarchical
    Reference count: 3
    Aggregation node: 3
    Referenced by interfaces: 1 references
      IP ATM5/0.2: atm-vp 1

    Referenced by policies: 2 references
      policy1

    Referenced by parent groups: 1 references
      extPg1
```

To display list information:

```
host1(config)#show policy-parameter

                                Policy Parameter Table
```

```
                                ------ --------- -----
Policy Parameter refRlpRate
    Type: reference-rate
    Rate: 100000
    Reference count: 7
    Referenced by interfaces: 2 references
      IP interface ATM5/0.1: 1000000
      IP interface ATM5/0.2: 200000

    Referenced by rate-limit profiles: 5 references
      rlpData
      rlpVoice
      rlpVideo

Policy Parameter otherRate
    reference-rate: 65536
    Reference count: 3
    Referenced by interfaces: 1 references
      IP interface ATM5/0.2: 100000

    Referenced by rate-limit profiles: 2 references
      rlpOther
```

Meaning Table 6 on page 44 lists the **show policy-parameter** command output fields.

Table 6: show policy-parameter Output Fields

Field Name	Field Description
Type	Type of parameter, such as hierarchical.
Reference count	Number of references in policy, interface, and external parent group profiles.
Aggregation node	Aggregation node value.
Referenced by interfaces	List of interfaces where parameter is referenced.
Referenced by profiles	List of profiles where parameter is referenced
Referenced by policies	List of policies where parameter is referenced.
Referenced by parent groups	List of external parent groups where parameter is referenced.

Related Documentation

- show policy-parameter

Monitoring Interfaces and Policy Lists

Purpose Display information about an interface and its policy lists. The **delta** keyword displays baselined statistics and the **brief** keyword displays the operational status of all configured interfaces

Action To display information about interfaces and policy lists:

NOTE: For tunnel interfaces, the packets field under the IP policy output section in the output of the **show ip interfaces** command displays the number of fragments or packets sent out from the tunnel interface for which an output policy is attached, depending on whether you enabled preservation of output policy statistics using the **enable-frag-stats** command. Although this field displays the unit of measure as packets, it denotes the number of fragments if statistics generation for output policies based on fragments is enabled. Otherwise, this field indicates the number of output policed packets on the tunnel interface.

```
host1#show interfaces fastEthernet 1/0.1
FastEthernet1/0.1 is Up, Administrative status is Up
  VLAN ID: 100

  In: Bytes 4156, Packets 30
   Errors 0, Discards 0
  Out: Bytes 6406, Packets 45
   Errors 0, Discards 0

VLAN policy input vlanPol1
  classifier-group vlan20 entry 1
    5 packets, 730 bytes
    filter
```

```
host1#show ip interfaces atm 5/0.2
ATM5/0.2 line protocol Atm1483 is down, ip is down (ready)
  Network Protocols: IP
  Internet address is 2.2.2.2/255.255.255.255
  Broadcast address is 255.255.255.255
  Operational MTU = 0  Administrative MTU = 0
  Operational speed = 100000000  Administrative speed = 0
  Discontinuity Time = 0
  Router advertisement = disabled
  Proxy Arp = disabled
  Network Address Translation is disabled
  TCP MSS Adjustment = disabled
  Administrative debounce-time = disabled
  Operational debounce-time    = disabled
  Access routing = disabled
  Multipath mode = hashed
  Auto Configure = disabled
  Auto Detect = disabled
  Inactivity Timer = disabled

  In Received Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Packets 0, Bytes 0
  In Policed Packets 0, Bytes 0
  In Error Packets 0
  In Invalid Source Address Packets 0
  In Discarded Packets 0
  Out Forwarded Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Routed Packets 0, Bytes 0
  Out Scheduler Dropped Packets 0, Bytes 0
  Out Policed Packets 0, Bytes 0
  Out Discarded Packets 0
```

```
IP policy input P
  classifier-group data entry 1
    0 packets, 0 bytes
    rate-limit-profile rlpData
         committed rate: 10000 bps, committed burst: 8192 bytes (default)
         peak Rate: 100000 bps, peak burst: 1875 bytes
      committed: 0 packets, 0 bytes, action: transmit
      conformed: 0 packets, 0 bytes, action: transmit
      exceeded:  0 packets, 0 bytes, action: drop
  classifier-group voice entry 1
    0 packets, 0 bytes
    rate-limit-profile rlpVoice
         committed rate: 64000 bps, committed burst: 100000 bytes (default)
         peak Rate: 100000 bps, peak burst: 1875 bytes
      committed: 0 packets, 0 bytes, action: transmit
      conformed: 0 packets, 0 bytes, action: transmit
      exceeded:  0 packets, 0 bytes, action: drop
  classifier-group video entry 1
    0 packets, 0 bytes
    rate-limit-profile rlpVideo
         committed rate: 70000 bps, committed burst: 875 bytes
         peak Rate: 100000 bps, peak burst: 1875 bytes
      committed: 0 packets, 0 bytes, action: transmit
      conformed: 0 packets, 0 bytes, action: transmit
      exceeded:  0 packets, 0 bytes, action: drop
IP policy output P
  classifier-group data entry 1
    0 packets, 0 bytes
    rate-limit-profile rlpData
         committed rate: 20000 bps, committed burst: 150 bytes
         peak Rate: 200000 bps, peak burst: 3750 bytes
      committed: 0 packets, 0 bytes, action: transmit
      conformed: 0 packets, 0 bytes, action: transmit
      exceeded:  0 packets, 0 bytes, action: drop
  classifier-group voice entry 1
    0 packets, 0 bytes
    rate-limit-profile rlpVoice
         committed rate: 64000 bps, committed burst: 100000 bytes
         peak Rate: 200000 bps, peak burst: 3750 bytes
      committed: 0 packets, 0 bytes, action: transmit
      conformed: 0 packets, 0 bytes, action: transmit
      exceeded:  0 packets, 0 bytes, action: drop
  classifier-group video entry 1
    0 packets, 0 bytes
    rate-limit-profile rlpVideo
         committed rate: 140000 bps, committed burst: 850 bytes
         peak Rate: 200000 bps, peak burst: 3750 bytes
      committed: 0 packets, 0 bytes, action: transmit
      conformed: 0 packets, 0 bytes, action: transmit
      exceeded:  0 packets, 0 bytes, action: drop
```

Meaning Table 7 on page 46 lists the **show interfaces** command output fields.

Table 7: show interfaces Output Fields

Field Name	Field Description
Subinterface number	Location of the subinterface that carries the VLAN traffic

Table 7: show interfaces Output Fields *(continued)*

Field Name	Field Description
Administrative status	Operational state that you configured for this interface: up or down
VLAN ID	Domain number of the VLAN
In Bytes	Number of bytes received on the VLAN subinterface
In Packets	Sum of all unicast, broadcast, and multicast packets received on the VLAN or S-VLAN subinterface
In Errors	Value is always 0 (zero)
In Discards	Value is always 0 (zero)
Out Bytes	Number of bytes sent on the VLAN or stacked VLAN (S-VLAN) subinterface
Out Packets	Number of packets sent on the VLAN or S-VLAN subinterface
Out Errors	Value is always 0 (zero)
Out Discards	Value is always 0 (zero)
VLAN policy	Type and name of the VLAN policy

Related Documentation

- show interfaces

Monitoring the Policy Configuration of ATM Subinterfaces

Purpose Display information about a subinterface's ATM policy lists.

Action To display information about ATM policy lists:

```
host1#show atm subinterface
ATM policy input PolCbr
  classifier-group *
3096packets, 377678 bytes
traffic-class best-effort
color green
```

Meaning Table 8 on page 48 lists the **show atm subinterface** command output fields.

Table 8: show atm subinterface Output Fields

Field Name	Field Description
ATM policy	Type and name of the ATM policy
mark-clp	CLP bit value, 0 or 1
color	Color applied to packet flow for queuing: green, yellow, or red
classifier-group	Name of the classifier control list used by the policy
filter	Filter policy action
forward	Forward policy action
traffic-class	Traffic class in the policy list
user packet class	User packet class in the policy list

Related Documentation

- show atm interface

Monitoring the Policy Configuration of Frame Relay Subinterfaces

Purpose Display information about a subinterface's Frame Relay policy lists.

Action To display information about Frame Relay policy lists:

```
host1#show frame-relay subinterface
Frame relay sub-interface SERIAL5/0:1/1.1, status is up
Number of sub-interface down transitions is 0
Time since last status change 03:04:59
No baseline has been set
  In bytes: 660                    Out bytes: 660
  In frames: 5                     Out frames: 5
  In errors: 0                     Out errors: 0
  In discards: 0                   Out discards: 0
  In unknown protos: 0
Frame relay policy output frOutputPolicy
  classifier-group frGroupA entry 1
     5 packets, 640 bytes
     mark-de 1
Frame relay sub-interface SERIAL5/1:1/1.1, status is up
Number of sub-interface down transitions is 0
Time since last status change 03:05:09
No baseline has been set
  In bytes: 660                    Out bytes: 660
  In frames: 5                     Out frames: 5
  In errors: 0                     Out errors: 0
  In discards: 0                   Out discards: 0
  In unknown protos: 0
Frame relay policy input frInputPolicy
```

```
classifier-group frMatchDeSet entry 1
    5 packets, 660 bytes
    color red
```

Meaning Table 9 on page 49 lists the **show frame-relay subinterface** command output fields.

Table 9: show frame-relay subinterface Output Fields

Field Name	Field Description
Frame Relay policy	Type and name of the VLAN policy
mark-de	DE bit value
color	Color applied to packet flow for queuing: green, yellow, or red
classifier-group	Name of the classifier control list used by the policy
filter	Filter policy action
forward	Forward policy action
traffic class	Traffic class in the policy list
user-packet-class	User packet class in the policy list

Related Documentation
- show frame-relay subinterface

Monitoring GRE Tunnel Information

Purpose Display information about GRE tunnels. The **state** keyword displays tunnels that are in a specific state: **disabled**, **down**, **enabled**, **not-present**, or **up**. The **ip** keyword to display tunnels associated with an IP address. To display information about a specific tunnel, include the name of the tunnel. To display information about tunnels on a specific virtual router, include the name of the virtual router.

Action To display information about GRE Tunnel policy lists:

```
host1#show gre tunnel detail tunnelGre50
GRE tunnel tunnelGre50 is Down
Tunnel operational configuration
  Tunnel mtu is '10240'
  Tunnel source address is '0.0.0.0'
  Tunnel destination address is '0.0.0.0'
  Tunnel transport virtual router is source
  Tunnel checksum option is disabled
  Tunnel sequence number option is disabled
  Tunnel up/down trap is enabled
  Tunnel-server location is 6/0
  Tunnel administrative state is Up
Statistics    packets       octets       discards   errors
```

```
  Data rx     0              0           0          0
  Data tx     0              0           0          0
GRE tunnel policy input routeGre25
  classifier-group gre6 entry 1
     0 packets, 0 bytes
     traffic-class best-effort
     mark 4 mask 255
GRE tunnel policy output routeGre35
  classifier-group gre14 entry 1
     0 packets, 0 bytes
     traffic-class best-effort
     mark 4 mask 255
```

Meaning Table 10 on page 50 lists the **show gre tunnel** command output fields.

Table 10: show gre tunnel Output Fields

Field Name	Field Description
GRE tunnel policy input	Policy for outbound traffic
GRE tunnel policy output	Policy for inbound traffic
traffic-class	Name of traffic class
classifier-group	Name of classifier group
entry	Identifier for the entry in the classifier group
packets	Number of packets
bytes	Number of bytes
mark	ToS byte setting for the classifier control list
mask	Mask value corresponding to the ToS

Related Documentation

- show gre tunnel

Monitoring the Policy Configuration of IP Interfaces

Purpose Display information about an IP interface (including policy list statistics).

Action To display information about IP policy lists on ATM interfaces:

```
host1#show ip interface atm 11/0.6

ATM11/0.6 line protocol Atm1483 is down, ip is down (ready)
  Network Protocols: IP
  Internet address is 10.12.1.1/255.255.255.0
  Broadcast address is 255.255.255.255
  Operational MTU = 0  Administrative MTU = 0
  Operational speed = 100000000  Administrative speed = 0
```

```
Discontinuity Time = 0
Router advertisement = disabled
Proxy Arp = disabled
ARP spoof checking = enabled
Network Address Translation is disabled
TCP MSS Adjustment = disabled
Administrative debounce-time = disabled
Operational debounce-time    = disabled
Access routing = disabled
Multipath mode = hashed
Auto Configure = disabled
Auto Detect = disabled
Re-Authenticate Auto Detect = disabled
Inactivity Timer = disabled
Use Framed Routes = disabled
Warm-restart initial-sequence-preference: Operational = 0 Administrative = 0

In Received Packets 0, Bytes 0
  Unicast Packets 0, Bytes 0
  Multicast Packets 0, Bytes 0
In Policed Packets 0, Bytes 0
In Error Packets 0
In Invalid Source Address Packets 0
In Discarded Packets 0
Out Forwarded Packets 0, Bytes 0
  Unicast Packets 0, Bytes 0
  Multicast Routed Packets 0, Bytes 0
Out Scheduler Dropped Packets 0, Bytes 0
Out Policed Packets 0, Bytes 0
Out Discarded Packets 0

IP policy output testPol
  classifier-group *
    0 packets, 0 bytes
    forward
       Virtual-router: default
       List:
         interface ATM11/0.1, order 100, rule 2 (not supported in output
         policy)
         next-hop 1.1.1.1, order 100, rule 3 (active) (not supported in
         output policy)
    rate-limit-profile R2
      committed rate: 0 bps, committed burst: 0 bytes (default)
      peak rate: 0 bps, peak burst: 0 bytes (default)
      committed: 0 packets, 0 bytes, action: transmit conditional
      conformed: 0 packets, 0 bytes, action: transmit conditional
      exceeded:  0 packets, 0 bytes, action: drop
    log
  classifier-group video entry 1
    0 packets, 0 bytes
    filter
```

To display information about IP policy lists on tunnel interfaces:

NOTE: If you enable scheduler profile–based computation of service session accounting by using the **service-accounting- statistics scheduler-based** command, the forwarded packets and bytes fields, and the dropped packets and bytes fields are displayed in the rate-limit-profile section under the IP policy output heading for policies with hierarchical parent groups. The committed, conformed, exceeded, saturated, and unconditional packets and bytes fields are not displayed in the rate-limit-profile section in the output of the command for policies with hierarchical parent groups. These fields are displayed instead of the forwarded packets and bytes fields, and the dropped packets and bytes fields only if you disable scheduler profile-based computation of service session accounting.

NOTE: The packets field in the IP policy output section displays the number of fragments or packets sent out from the tunnel interface for which an output policy is attached, depending on whether you enabled preservation of output policy statistics using the **enable-frag-stats** command. Although this field displays the unit of measure as packets, it denotes the number of fragments if statistics generation for output policies based on fragments is enabled. Otherwise, this field indicates the number of output policed packets on the tunnel interface.

```
host1#show ip interface tunnel l2tp:1/19/21

Out Forwarded Packets 1, Bytes 1500
    Unicast Packets 1, Bytes 1500
    Multicast Routed Packets 0, Bytes 0
  Out Scheduler Dropped Packets 0, Bytes 0
  Out Policed Packets 0, Bytes 0
  Out Discarded Packets 0

  IP policy output POLICY-USER-OUT
    classifier-group USER-OUT-PERMIT entry 1
      2 packets, 1596 bytes
      forward
  queue 0: traffic class best-effort, bound to ip TUNNEL l2tp:1/19/21
    Queue length 0 bytes
    Forwarded packets 2, bytes 1590
```

Meaning Table 11 on page 52 lists the **show ip interfaces** command output fields.

Table 11: show ip interfaces Output Fields

Field Name	Field Description
Network Protocols	Protocols configured on the interface
Internet address	IP address of the interface

Table 11: show ip interfaces Output Fields *(continued)*

Field Name	Field Description
Broadcast address	Broadcast address used by the interface
Operational MTU	Operational maximum transmission unit (MTU) for packets sent on this interface
Administrative MTU	Administrative maximum transmission unit for packets sent on this interface
Operational speed	Speed known to the IP layer in bits per second; equal to the administrative speed if configured, otherwise inherited from the lower layer
Administrative speed	Configured speed known to the IP layer in bits per second
Discontinuity Time	Time since the counters on the interface became invalid; for example, when the line module was reset
Router Advertisement	When enabled by the **ip irdp** command, the router advertises its presence via the ICMP Router Discovery Protocol (IRDP)
Administrative debounce-time	Administrative time delay that an interface must remain in a new state before the routing protocols react to the state change
Operational debounce-time	Time delay that an interface must remain in a new state before the routing protocols react to the state change
Access routing	When enabled, an access route is installed to the host on the other end of the interface
In Received Packets	Number of packets received on the interface; indicates whether packets are unicast or multicast
In Received Bytes	Number of bytes received on the interface; indicates whether bytes are unicast or multicast
In Policed Packets	Number of packets policed on the interface; discarded because they exceeded a traffic contract to their destination
In Policed Bytes	Number of bytes policed on the interface; discarded because they exceeded a traffic contract to their destination
In Error Packets	Number of packets determined to be in error at the interface

Table 11: show ip interfaces Output Fields *(continued)*

Field Name	Field Description
In Invalid Source Address Packets	Number of packets determined to have originated from an invalid source address
Out Forwarded Packets	Number of packets forwarded from the interface; indicates whether packets are unicast or multicast
Out Forwarded Bytes	Number of bytes forwarded from the interface; indicates whether bytes are unicast or multicast
Out Scheduler Drops Packets	Number of packets dropped by the out scheduler; indicates whether packets are committed, conformed, or exceeded
Out Scheduler Drops Bytes	Number of bytes dropped by the out scheduler; indicates whether bytes are committed, conformed, or exceeded
Policy	Indicates which policy is attached and whether it is on the input or output of the interface
classifier-group	Name of a CLACL attached to the interface and number of entry
exception http-redirect	Number of packets and bytes assigned to http-redirect
filter	Number of packets and bytes dropped because of the CLACL
color	Explicit color applied to packet flow for queuing; green, yellow, or red:
Packets logged	Number of packets colored
Bytes logged	Number of bytes colored
next hop	Address of the next-hop destination:
Packets transmitted	Number of packets sent to the next-hop address
Bytes transmitted	Number of bytes sent to the next-hop address
forward	Number of packets and bytes forwarded because of the CLACL
interface	Interface rule to forward all packets that match the current classifier control list

Table 11: show ip interfaces Output Fields *(continued)*

Field Name	Field Description
next-hop	Next-hop IP addresses are used as forwarding solutions, and the order of the rule within the classifier that the router uses to choose the solutions. The phrase in parentheses describes whether the rule entry is reachable, active, and supported for the configured policy
rate-limit-profile	Name of the rate-limit profile
committed	Number of packets and bytes within the committed rate limit
conformed	Number of packets and bytes exceeding the committed rate limit but within the peak rate
exceeded	Number of packets and bytes exceeding the peak rate
action	Action performed on the packets matched by the rules in the rate-limit profile

Related Documentation

- show ip interface

Monitoring the Policy Configuration of IPv6 Interfaces

Purpose Display detailed or summary information, including policy and classifier information, for a particular IPv6 interface or for all interfaces. The default for the **show ipv6 interface** command is all interface types and all interfaces. The **brief** or **detail** keywords with the **show ipv6 interface** command displays different levels of information.

Action To display information about IPv6 policy lists:

NOTE: If you enable scheduler profile–based computation of service session accounting by using the **service-accounting- statistics scheduler-based** command, the forwarded packets and bytes fields, and the dropped packets and bytes fields are displayed in the rate-limit-profile section under the IPv6 policy output heading for policies with hierarchical parent groups. The committed, conformed, exceeded, saturated, and unconditional packets and bytes fields are not displayed in the rate-limit- profile section in the output of the command for policies with hierarchical parent groups. These fields are displayed instead of the forwarded packets and bytes fields, and the dropped packets and bytes fields only if you disable scheduler profile-based computation of service session accounting.

```
host1#show ipv6 interface FastEthernet 9/0.6
FastEthernet9/0.6 line protocol VlanSub is up, ipv6 is up
  Description: IPv6 interface in Virtual Router Hop6
  Network Protocols: IPv6
  Link local address: fe80::90:1a00:740:31cd
  Internet address: 2001:db8:1::/48
  Operational MTU 1500 Administrative MTU 0
  Operational speed 100000000 Administrative speed 0
  Creation type Static
  ND reachable time is 3600000 milliseconds
  ND duplicate address detection attempts is 100
  ND neighbor solicitation retransmission interval is 1000 milliseconds
  ND proxy is enabled
  ND RA source link layer is advertised
  ND RA interval is 200 seconds, lifetime is 1800 seconds
  ND RA managed flag is disabled, other config flag is disabled
  ND RA advertising prefixes configured on interface

  In Received Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Packets 0, Bytes 0
  In Total Dropped Packets 0, Bytes 0
    In Policed Packets 0
    In Invalid Source Address Packets 0
    In Error Packets 0
    In Discarded Packets 0

  Out Forwarded Packets 8, Bytes 768
    Unicast Packets 8, Bytes 768
    Multicast Routed Packets 0, Bytes 0
  Out Total Dropped Packets 5, Bytes 0
    Out Scheduler Dropped Packets 0, Bytes 0
    Out Policed Packets 0
    Out Discarded Packets 5

  IPv6 policy input ipv6InPol25
   classifier-group *
      0 packets, 0 bytes
      forward
         Virtual-router: default
         List:
           next-hop 2001:82ab:1020:87ec::/64, order 100, rule 3 (active)
           (not supported in output policy)
   rate-limit-profile Rlp2Mb classifier-group clgA entry 1
```

```
    Committed: 0 packets, 0 bytes
    Conformed: 0 packets, 0 bytes
    Exceeded:  0 packets, 0 bytes
  rate-limit-profile Rlp8Mb
    Committed: 0 packets, 0 bytes
    Conformed: 0 packets, 0 bytes
    Exceeded:  0 packets, 0 bytes
IPv6 policy output ipv6PolOut2
  rate-limit-profile RlpOutA classifier-group clgB entry 1
    Committed: 0 packets, 0 bytes
    Conformed: 0 packets, 0 bytes
    Exceeded:  0 packets, 0 bytes
  rate-limit-profile RlpOutB
    Committed: 0 packets, 0 bytes
    Conformed: 0 packets, 0 bytes
    Exceeded:  0 packets, 0 bytes
IPv6 policy local-input ipv6PolLocIn5
  rate-limit-profile Rlp1Mb classifier-group clgC entry 1
    Committed: 0 packets, 0 bytes
    Conformed: 0 packets, 0 bytes
    Exceeded:  0 packets, 0 bytes
  rate-limit-profile Rlp5Mb
    Committed: 0 packets, 0 bytes
    Conformed: 0 packets, 0 bytes
    Exceeded:  0 packets, 0 bytes
queue 0: traffic class best-effort, bound to ipv6 FastEthernet9/0.6
  Queue length 0 bytes
  Forwarded packets 0, bytes 0
  Dropped committed packets 0, bytes 0
  Dropped conformed packets 0, bytes 0
  Dropped exceeded packets 0, bytes 0
```

Meaning Table 12 on page 57 lists the **show ipv6 interface** command output fields.

Table 12: show ipv6 interface Output Fields

Field Name	Field Description
Description	Optional description for the interface or address specified
Network Protocols	Network protocols configured on this interface
Link local address	Local IPv6 address of this interface
Internet address	External address of this interface
Operational MTU	Value of the MTU
Administrative MTU	Value of the MTU if it has been administratively overridden using the configuration
Operational speed	Speed of the interface
Administrative speed	Value of the speed if it has been administratively overridden using the configuration

Table 12: show ipv6 interface Output Fields *(continued)*

Field Name	Field Description
Creation type	Method by which the interface was created (static or dynamic)
ND reachable time	Amount of time (in milliseconds) that the neighbor is expected to remain reachable
ND duplicate address detection attempts	Number of times that the router attempts to determine a duplicate address
ND neighbor solicitation retransmission interval	Amount of time (in milliseconds) during which the router retransmits neighbor solicitations
ND proxy	Whether the router replies to solicitations on behalf of a known neighbor, enabled or disabled
ND RA source link layer	Whether the RA includes the link layer
ND RA interval	Amount of time (in seconds) of the neighbor discovery router advertisement
ND RA lifetime	Amount of time (in seconds) of the neighbor discovery router advertisement
ND RA managed flag	State of the neighbor discovery router advertisement managed flag, enabled or disabled
ND RA other config flag	State of the neighbor discovery router advertisement other config flag, enabled or disabled
ND RA advertising prefixes	Whether advertisement prefixes for neighbor discovery router advertisement are configured
In Received Packets, Bytes	Total number of packets and bytes received on this interface
Unicast Packets, Bytes	Number of unicast packets and bytes received on the IPv6 interface; link-local received multicast packets (non-multicast-routed frames) are counted as unicast packets
Multicast Packets, Bytes	Number of multicast packets and bytes received on the IPv6 interface, which are then multicast-routed and counted as multicast packets
In Total Dropped Packets, Bytes	Total number of inbound packets and bytes dropped on this interface

Table 12: show ipv6 interface Output Fields *(continued)*

Field Name	Field Description
In Policed Packets	Number of packets that were received and dropped because of rate limits
In Invalid Source Address Packets	Number of packets received with invalid source address (for example, spoofed packets)
In Error Packets	Number of packets received with errors
In Discarded Packets	Number of packets received that were discarded for reasons other than rate limits, errors, and invalid source address
Out Forwarded Packets, Bytes	Total number of packets and bytes that were sent from this interface
Unicast Packets, Bytes	Number of unicast packets and bytes that were sent from this interface
Multicast Routed Packets, Bytes	Number of multicast packets and bytes that were sent from this interface
Out Total Dropped Packets	Total number of outbound packets and bytes dropped by this interface
Out Scheduler Dropped Packets, Bytes	Number of outbound packets and bytes dropped by the scheduler
Out Policed Packets, Bytes	Number of outbound packets and bytes dropped because of rate limits
Out Discarded Packets	Number of outbound packets that were discarded for reasons other than those dropped by the scheduler and those dropped because of rate limits
IPv6 policy	Type (input, output, local-input) and name of the policy
forward	Number of packets and bytes forwarded because of the CLACL
next-hop	Next-hop IPv6 addresses are used as forwarding solutions, and the order of the rule within the classifier that the router uses to choose the solutions. The phrase in parentheses describes whether the rule entry is reachable, active, and supported for the configured policy
rate-limit-profile	Name of the profile

Table 12: show ipv6 interface Output Fields *(continued)*

Field Name	Field Description
classifier-group entry	Entry index
Committed	Number of packets and bytes that conform to the committed access rate
Conformed	Number of packets and bytes that exceed the committed access rate but conform to the peak access rate
Exceeded	Number of packets and bytes that exceed the peak access rate
queue, traffic class, bound to ipv6	Queue and traffic class bound to the specified IPv6 interface
Queue length	Number of bytes in the queue
Dropped committed packets, bytes	Total number of committed packets and bytes dropped by this interface
Dropped conformed packets, bytes	Total number of conformed packets and bytes dropped by this interface
Dropped exceeded packets, bytes	Total number of exceeded packets and bytes dropped by this interface

Related Documentation

- show ipv6 interface

Monitoring the Policy Configuration of Layer 2 Services over MPLS

Purpose Display status and configuration information about layer 2 services over MPLS (also known as Martini, or layer 2 transport) on the router or on specific interfaces. Displays only layer 2 circuits for the specified interface.

Action To display information about layer 2 services over MPLS policy lists:

```
host1#show mpls l2transport interface
FastEthernet9/0.1
  routed to 222.9.1.3  on base LSP  tun mpls:lsp-de090100-24-37
  group-id 2 vc-id 900001 mtu 1500
  State UP
  In  Label 48 on stack
    0 pkts, 0 hcPkts, 0 octets
    0 hcOctets, 0 errors, 0 discardPkts

  Out Label 49 on  tun mpls:lsp-de090100-24-37
    0 pkts, 0 hcPkts, 0 octets
    0 hcOctets, 0 errors, 0 discardPkts
    queue 0: traffic class best-effort, bound to atm-vc ATM1/0.1
```

```
    Queue length 0 bytes
    Forwarded packets 0, bytes 0
    Dropped committed packets 0, bytes 0
    Dropped conformed packets 0, bytes 0
    Dropped exceeded packets 0, bytes 0

  MPLS policy input mplsInputPolicy
    classifier-group claclWst50 entry 1
      0 packets, 0 bytes
      rate-limit-profile rlp
        committed: 0 packets, 0 bytes, action: transmit
        conformed: 0 packets, 0 bytes, action: transmit
        exceeded:  0 packets, 0 bytes, action drop
  MPLS policy output mplsOutputPolicy
    classifier-group claclWst75 entry 1
      0 packets, 0 bytes
      rate-limit-profile rlp
        committed: 0 packets, 0 bytes, action: transmit
        conformed: 0 packets, 0 bytes, action: transmit
        exceeded:  0 packets, 0 bytes, action: drop
```

Meaning Table 13 on page 61 lists the **show mpls l2transport interface** command output fields.

Table 13: show mpls l2transport interface Output Fields

Field Name	Field Description
Interface	Specifier and status of each interface
base-LSP/remote-addr	Identifies either the tunnel that is selected to forward the traffic or the address of the router at the other end
group-id	Group ID number for the interface
vc-id	VC ID number for the interface
mtu	Maximum transmission unit for the interface
state/in/out-label	Status of the Layer 2-over-MPLS connection or the incoming/outgoing VC label
Mpls Statistics	
pkts	Number of packets received or sent
hcPkts	Number of high-capacity (64-bit) packets received or sent
octets	Number of octets received or sent
hcOctets	Number of high-capacity (64-bit) octets received or sent
errors	Number of packets that are dropped for some reason at receipt or before being sent

Table 13: show mpls l2transport interface Output Fields *(continued)*

Field Name	Field Description
discardPkts	Number of packets that are discarded due to lack of buffer space at receipt or before being sent
queue, traffic class, bound to	Queue and traffic class bound to the specified interface
Queue length	Number of bytes in queue
Forwarded packets, bytes	Total number of packets and bytes forwarded by this interface
Dropped committed packets, bytes	Total number of committed packets and bytes dropped by this interface
Dropped conformed packets, bytes	Total number of conformed packets and bytes dropped by this interface
Dropped exceeded packets, bytes	Total number of exceeded packets and bytes dropped by this interface
MPLS policy	Type (input, output) and name of policy
classifier-group	Name of a CLACL attached to the interface and number of entry
rate-limit-profile	Name of profile
Committed	Number of packets and bytes conforming to the committed access rate
Conformed	Number of packets and bytes that exceed the committed access rate but conform to the peak access rate
Exceeded	Number of packets and bytes exceeding the peak access rate

Related Documentation

- show mpls

Monitoring the Policy Configuration of VLAN Subinterfaces

Purpose Display information about a subinterface's VLAN policy lists.

Action To display information about VLAN policy lists:

```
host1#show vlan subinterface fastEthernet 1/0.1
VLAN ID is 100
```

```
VLAN policy input vlanPol1
  classifier-group claclVlanBos entry 1
    5 packets, 730 bytes
    filter
```

Meaning Table 14 on page 63 lists the **show vlan subinterface** command output fields.

Table 14: show vlan subinterface Output Fields

Field Name	Field Description
Subinterface number	Location of the subinterface that carries the VLAN traffic
VLAN ID	Domain number of the VLAN
VLAN policy	Type and name of the VLAN policy
filter	Number of packets and bytes that have been policed by the policy

Related Documentation

- show vlan subinterface

Packet Flow Monitoring Overview

The policy log rule provides a way to monitor a packet flow by capturing a sample of the packets that satisfy the classification of the rule in the system log. See *JunosE System Event Logging Reference Guide* for information about logging.

To capture the interface, protocol, source address, destination address, source port, and destination port, set the policyMgrPacketLog event category to log at severity info and at low verbosity. To capture the version, ToS, len ID, flags, time to live (TTL), protocol, and checksum in addition to the information captured at low verbosity, set the verbosity to medium or high.

When the policy is configured, all packets are examined and the matching packets are placed in the log. No more than 512 packets are logged every 3 seconds. The router maintains a count of the total number of matching packets. This count is incremental even if the packet cannot be stored in the log (for example, because the count exceeds the 512-packet threshold).

This example shows how you might use classification to specify the ingress packets that are logged in to an interface.

```
host1(config)#ip policy-list testPolicy
host1(config-policy-list)#classifier-group logA
host1(config-policy-list-classifier-group)#log
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#exit
host1(config)#interface atm 0/0.0
host1(config-subif)#ip policy input testPolicy statistics enabled
```

```
host1(config-subif)#exit
host1(config)#log destination console severity info
host1(config)#log severity info policyMgrPacketLog
host1(config)#log verbosity low policyMgrPacketLog
host1(config)#log here
```

This example provides a more detailed procedure that an ISP might use to log information during a ping attack on the network. The procedure includes the creation of the classifier and policy lists to specify the desired packet flow to monitor, the logging of the output of the classification operation, and the output of the **show** command.

In this example, a customer has reported to their ISP that an attack is occurring on their internal servers. The attack is a simple ping flood.

1. The ISP creates a classifier list to define an ICMP echo request packet flow.

```
host1:vr2(config)#ip classifier-list icmpEchoReq icmp any any 8 0
host1:vr2(config)#ip policy-list pingAttack
host1:vr2(config-policy-list)#classifier-group icmpEchoReq
host1:vr2(config-policy-list-classifier-group)#log
host1:vr2(config-policy-list-classifier-group)#exit
host1:vr2(config-policy-list)#exit

host1:vr2(config)#interface gigabitEthernet 2/0
host1:vr2(config-if)#ip address 10.10.10.2 255.255.255.0
host1:vr2(config-if)#exit

host1:vr2(config)#virtual-router vr1
host1:vr1(config)#interface gigabitEthernet 0/0
host1:vr1(config-if)#ip address 10.10.10.1 255.255.255.0
host1:vr1(config-if)#ip policy input pingAttack statistics enabled
host1:vr1(config-if)#exit
host1:vr1(config)#exit
```

2. The ISP configures standard logging on the E Series router.

```
host1(config)#log destination console severity info
host1(config)#log severity info policyMgrPacketLog
host1(config)#log here

INFO 12/16/2003 12:59:47 policyMgrPacketLog ():
icmpEchoReq icmp GigabitEthernet0/0 10.10.10.2 10.10.10.1 forwarded
INFO 12/16/2003 12:59:47 policyMgrPacketLog ():
icmpEchoReq GigabitEthernet0/0 number of hits = 21551
INFO 12/16/2003 12:59:50 policyMgrPacketLog ():
icmpEchoReq icmp GigabitEthernet0/0 10.10.10.2 10.10.10.1 forwarded
INFO 12/16/2003 12:59:50 policyMgrPacketLog ():
icmpEchoReq GigabitEthernet0/0 number of hits = 21851
INFO 12/16/2003 12:59:53 policyMgrPacketLog ():
icmpEchoReq icmp GigabitEthernet0/0 10.10.10.2 10.10.10.1 forwarded
INFO 12/16/2003 12:59:53 policyMgrPacketLog ():
icmpEchoReq GigabitEthernet0/0 number of hits = 22151
```

3. The ISP displays statistics for the interface.

```
host1:vr1#show ip interface gigabitEthernet 0/0
GigabitEthernet0/0 line protocol Ethernet is up, ip is up
  Network Protocols: IP
  Internet address is 10.10.10.1/255.255.255.0
  Broadcast address is 255.255.255.255
  Operational MTU = 1500  Administrative MTU = 0
  Operational speed = 1000000000  Administrative speed = 0
  Discontinuity Time = 1092358
  Router advertisement = disabled
  Proxy Arp = enabled
  Network Address Translation is disabled
  Administrative debounce-time = disabled
  Operational debounce-time    = disabled
  Access routing = disabled
  Multipath mode = hashed
  Auto Configure = disabled
  Auto Detect = disabled
  Inactivity Timer = disabled

  In Received Packets 488421, Bytes 62517888
    Unicast Packets 488421, Bytes 62517888
    Multicast Packets 0, Bytes 0
  In Policed Packets 0, Bytes 0
  In Error Packets 0
  In Invalid Source Address Packets 0
  In Discarded Packets 0
  Out Forwarded Packets 486152, Bytes 62232048
    Unicast Packets 486152, Bytes 62232048
    Multicast Routed Packets 0, Bytes 0
  Out Scheduler Dropped Packets 0, Bytes 0
  Out Policed Packets 0, Bytes 0
  Out Discarded Packets 2269

  IP policy input pingAttack
    classifier-group icmpEchoReq entry 1
      488421 packets, 69355782 bytes
      log

  queue 0: traffic class best-effort, bound to ip GigabitEthernet0/0
    Queue length 0 bytes
    Forwarded packets 485988, bytes 70954248
    Dropped committed packets 0, bytes 0
    Dropped conformed packets 0, bytes 0
    Dropped exceeded packets 0, bytes 0
```

You can also capture traffic that transits through the router by using the policyMgrPacketLog category. When you set the logging severity level to info, you have the following options

- interface—filter on an interface
- interface-type—filter on an interface type
- policy-list—filter on a policy list

The policy list must contain the log keyword in the classifier group you want to monitor. You must also enable logging for policyMgrPacketLog and for the specific interface or policy list.

```
host1(config)#log severity info policyMgrPacketLog
host1(config)#log severity info policyMgrPacketLog policy-list all
```

```
host(config)#ip policy-list test
host(config-policy-list)#classifier-group *
host1(config-policy-list-classifier-group)#log

host1(config)#interface fastEthernet 2/0.100
host1(config-if)#vlan id 100
host1(config-if)#ip address 100.1.1.1 255.255.255.0
host1(config-if)#ip policy input test
host1(config-if)#ip policy output test
```

The packet capture can also be done for any source and destination defined in the classifier list. If the logging verbosity is set to low, you can obtain the following level of detail from the packet capture:

```
INFO 02/20/2008 10:10:23 policyMgrPacketLog:
test icmp FastEthernet2/2.100 100.1.1.2 100.1.2.2 forwarded
INFO 02/20/2008 10:10:26 ppolicyMfrPacketLog:
test icmp FastEthernet2.2.100.100.1.2.2 100.1.1.2 forwarded
```

If the logging verbosity is set to medium or high, you can obtain the following level of detail from the packet capture:

```
INFO 02/20/2008 10:15:11 policyMgrPacketLog: Classifier: test.1, prot: icmp,
intf:  FastEthernet2/2.100, sa: 100.1.1.2, da: 100.1.2.2 version: 0x45, tos:
0x0, len: 0x3e8, id: 0x714, flags: 0x0, ttl: 0x20, proto; 0x1, chksum: 0xc4fb,
forwarded

INFO 02/20/2008 10:15:14 ppolicyMfrPacketLog: classifier: test.1, prot: icmp,
intf: FastEthernet2/2.100, sa: 100.1.1.2 da: 100.1.2.2 version: 0x45, tos:
0x0, len: 0x3e8, id: 0xbe8, flags: 0x0, ttl: 0x7e, proto; 0x1, chksum: 0x6227,
forwarded
```

Related Documentation

- Monitoring the Policy Configuration of ATM Subinterfaces on page 47
- Monitoring the Policy Configuration of Frame Relay Subinterfaces on page 48
- Monitoring the Policy Configuration of IP Interfaces on page 50

Verifying Statistics Collection for Output Policies on Tunnel Interfaces

Purpose Display whether the mechanism to generate and preserve statistics based on fragments for traffic on tunnel interfaces to which output policies are attached is enabled. By default, output policy counters for tunnel interfaces are displayed as a measure of the number of packets.

Action To determine whether collection of output policy statistics based on fragments for traffic on tunnel interfaces is enabled:

```
host1#show enable frag-stats
Enabled
```

Related Documentation

- Statistics Collection for Output Policies on Tunnel Interfaces Overview on page 8
- Configuring Statistics Collection for Output Policies on Tunnel Interfaces on page 30
- enable-frag-stats

- show enable-frag-stats

PART 4

Index

Index