Chapter 9

Monitoring Policy Management

This chapter explains how to set a statistics baseline and use the **show** command to display your policy configuration and monitor policy statistics.

This chapter discusses the following topics:

Monitoring Policy Management Overview

You can set a statistics baseline and use the **show** command to display your policy configuration and monitor policy statistics. When you set baseline statistics, you can retrieve statistics beginning at the time when the baselining is set. 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 the *JUNOSe System Event Logging Reference Guide* for information about logging.

NOTE: You can use the output filtering feature of the **show** command to include or exclude lines of output based on a text string you specify. See *JUNOSe System Basics Configuration Guide, Chapter 2, Command-Line Interface* for details.

Setting a Statistics Baseline

You can set a baseline for policy statistics by using the **baseline interface** command and the **atm policy**, **frame-relay policy**, **gre-tunnel policy**, **ip policy, ipv6 policy**, **l2tp policy**, **mpls policy**, and **vlan policy** commands. If you do not enable baselining, **show** command output fields for baseline counters display the contents of the regular statistics counters.

If you enable statistics, you can enable or disable baselining of the statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline when baseline-relative statistics are retrieved. Unlike other baseline statistics, policy baseline statistics are not stored in nonvolatile storage (NVS).

If you issue the **baseline interface** command for an interface without first enabling policy statistics baselining on that interface, a warning message indicates that policy baseline statistics are not enabled.

Purpose Enable a baseline for the statistics for the attachment of a policy list with statistics enabled to the ingress of an interface.

Action Enable baseline counters.

host1(config)#**interface atm 12/0.1**
host1(config-subif)#**ip policy input routeForXYZCorp statistics enabled baseline enabled**

Run the **show ip interface** command with the **delta** keyword to show baseline counters:

```
host1#show ip interface atm 12/0.1 delta
atm12/0.1 is up, line protocol is up
  Network Protocols: IP
  Internet address is 200.200.1.1/255.255.255.0
  Broadcast address is 255.255.255.255
  Operational MTU = 9180  Administrative MTU = 0
  Operational speed = 155520000  Administrative speed = 0
  Discontinuity Time = 1251181
  Router advertisement = disabled
  Administrative debounce-time = disabled
```

```
Operational debounce-time    = disabled
Access routing = disabled
Multipath mode = hashed

In Received Packets 5, Bytes 540
In Policed Packets 0, Bytes 0
In Error Packets 0
In Invalid Source Address Packets 0
In Discarded Packets 0
Out Forwarded Packets 5, Bytes 540
Out Scheduler Drops Packets 0, Bytes 0
Out Policed Packets 5, Bytes 540
Out Discarded Packets 0

IP Policy input routeForXYZCorp
  classifier-group *
     filter
     5 Packets  540 Bytes dropped
```

Related Topics

- **atm policy** command
- **frame-relay policy** command
- **gre-tunnel policy** command
- **ip policy** command
- **ipv6 policy** command
- **l2tp policy** command
- **mpls policy** command
- **vlan policy** command

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 22 lists the show **atm subinterface** command output fields.

Table 22: 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 Topics

- **show atm interface** command

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 23 lists the **show classifier-list** command output fields.

Table 23: 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
User Priority bits	User priority bits value to match
Traffic Class Field	Traffic class field value to match

Table 23: show classifier-list Output Fields (continued)

Field Name	Field Description
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 Topics

- **show classifier-list** command

Monitoring Color-Mark Profiles

Purpose Display information about color-mark profiles.

Action To display information about color-mark profiles:

```
host1#show color-mark-profile A
                            Color Mark Profile Table
                            ----- ---- ------- -----
IP Color-Mark-Profile: A
    Mask:                        255
    Green mark:                  64
    Yellow mark:                 -
    Red mark:                    8
```

Meaning Table 24 lists the **show color-mark-profile** command output fields.

Table 24: color-mark-profile Output Fields

Field Name	Field Description
Color-Mark-Profile	Name of the color mark profile
filter	Filter policy action

Related Topics

- **show color-mark-profile** command

Monitoring Control Plane Policer Information

Purpose Display information about control plane policer for a specified protocol or all protocols.

Action To display information about control plane policer:

```
host1#show control-plane policer protocol
                                          Burst
                                   Rate   Size   Packets    Packets
          Protocol          Enabled (pps) (pkts) Committed  Exceeded
----------------------------- ------- ----- ------ ---------- ----------
PppEchoRequest                  false    50     50          0          0
PppEchoReply                    false    50     50          0          0
PppEchoReplyFast                false    50     50          0          0
PppControl                      false    50     50          0          0
AtmControl                      false    50     50          0          0
AtmOam                          false    50     50          0          0
AtmDynamicIf                    false    50     50          0          0
AtmInverseArp                   false    50     50          0          0
FrameRelayControl               false    50     50          0          0
FrameRelayArp                   false    50     50          0          0
PppoeControl                    false    50     50          0          0
PppoePppConfig                  false    50     50          0          0
EthernetArp                     false    50     50          0          0
EthernetArpMiss                 false    50     50          0          0
EthernetLacp                    false    50     50          0          0
EthernetDynamicIf               false    50     50          0          0
```

Meaning Table 25 lists the **show control-plane policer** command output fields.

Table 25: show control-plane policer Output Fields

Field Name	Field Description
Protocol	Name of the protocol
Enabled	True or False
Rate (pps)	Rate, in packets per second in the range 0–10000
Burst Size (pkts)	Burst size, in packets, in the range 0–10000
Packets Committed	Number of packets committed
Packets Exceeded	Number of packets exceeded

Related Topics

- **show control-plane policer** command

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 26 lists the **show frame-relay subinterface** command output fields.

Table 26: 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 Topics

- **show frame-relay subinterface** command

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 27 lists the **show gre tunnel** command output fields.

Table 27: 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 Topics

- **show gre tunnel** command

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:

```
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 28 lists the **show interfaces** command output fields.

Table 28: show interfaces Output Fields

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

Table 28: show interfaces Output Fields (continued)

Field Name	Field Description
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 Topics

- **show interfaces** command

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:

```
host1#show ip interface serial 2/1:28/24.1
serial2/1:28/24.1 is up, line protocol is up
  Network Protocols: IP
  Internet address is 172.24.1.101/255.255.255.0
  Broadcast address is 255.255.255.255
  Operational MTU = 1600 Administrative MTU = 0
  Operational speed = 155520000  Administrative speed = 0
  Discontinuity Time = 14695
  Router advertisement = disabled
  Administrative debounce-time = disabled
  Operational debounce-time    = disabled
  Access routing = disabled

  In Received Packets 15, Bytes 3135
  In Policed Packets 0, Bytes 0
  In Error Packets 0
  In Invalid Source Address Packets 0
  Out Forwarded Packets 0, Bytes 0
  Out Scheduler Drops Packets 0, Bytes 0

IP Policy input pl28241
Classifier-group clacl28241X01 entry 1
    0 packets, 0 bytes
exception http-redirect
Classifier-group clacl28241X01 entry 1
    0 packets, 0 bytes
    filter
```

```
Classifier-group clacl28241X02 entry 1
  1 packets, 202 bytes
  filter
Classifier-group clacl28241X03 entry 1
  1 packets, 203 bytes
  filter
Classifier-group clacl28241X04 entry 1
  1 packets, 204 bytes
  filter
Classifier-group clacl28241X05 entry 1
  1 packets, 205 bytes
  filter
```

Meaning Table 29 lists the **show ip interfaces** command output fields.

Table 29: show ip interfaces Output Fields

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

Table 29: show ip interfaces Output Fields (continued)

Field Name	Field Description
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
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
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 Topics

- **show ip interface** command

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:

```
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
    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 30 lists the **show ipv6 interface** command output fields.

Table 30: 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
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

Table 30: show ipv6 interface Output Fields (continued)

Field Name	Field Description
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
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

Table 30: show ipv6 interface Output Fields (continued)

Field Name	Field Description
IPv6 policy	Type (input, output, local-input) and name of the policy
rate-limit-profile	Name of the profile
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 Topics

- **show ipv6 interface** command

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 31 lists the **show mpls l2transport interface** command output fields.

Table 31: 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
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

Table 31: show mpls l2transport interface Output Fields (continued)

Field Name	Field Description
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 Topics

- **show mpls l2transport interface** command

Monitoring External Parent Groups

Purpose Display information about external parent groups.

Action To display information about external parent groups:

```
host1#show parent-group name EPG2

                                    Parent Group Table
                                    ------ ----- ------
Parent Group EPG2
   Reference count: 1
   Rate limit profile: VLAN_RATE
   Next parent group: EPG1 parameter C

   Referenced by policies:
     P1
```

Meaning Table 32 lists the **show parent-group** command output fields.

Table 32: show parent-group Output Fields

Field Name	Field Description
Reference count	Number of references within policies and other external parent groups.
Rate limit profile	Name of hierarchical rate limit profile.
Next parent group	Name of the next parent group and parameter.

Table 32: show parent-group Output Fields (continued)

Field Name	Field Description
Referenced by policies	List of policies where this parent group is referenced.
Referenced by parent groups	List of parent groups where the parent group is referenced.

Related Topics

- **show parent-group** command

Monitoring Policy Lists

Purpose Display information about policy lists.

Action To display policy lists:

```
host1#show policy-list
                                    Policy Table
                                    ------ -----
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
      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 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 33 lists the **show policy list** command output fields.

Table 33: 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.
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; 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.

Table 33: show policy-list Output Fields (continued)

Field Name	Field Description
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
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 Topics

- **show policy-list** command

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 dislay 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 34 lists the **show policy-parameter** command output fields.

Table 34: 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 Topics

- **show policy-parameter** command

Monitoring Rate-Limit Profiles

Purpose Display information about rate-limit profiles.

Action To display information about rate-limit profiles:

```
host1#show rate-limit-profile
                            Rate Limit Profile Table
                            ---- ----- ------- -----
IP Rate-Limit-Profile: rlp
   Profile Type:                  one-rate
   Reference count:               0
   Committed rate:                0
   Committed burst:               8192
   Excess burst:                  0
   Mask:                          255
   Committed rate action:         transmit
   Conformed rate action:         transmit
   Exceeded rate action:          drop
IP Rate-Limit-Profile: rlp
   Profile Type:                  two-rate hierarchical
   Color-aware                    no
   Reference count:               0
   Committed rate:                0
   Committed burst:               8192
   Peak rate:                     0
   Peak burst:                    8192
   Mask:                          255
   Committed rate action:         transmit unconditional
   Conformed rate action:         transmit conditional
   Exceeded rate action:          drop
L2TP Rate-Limit-Profile: L2tpRlp
   Profile Type:                  two-rate
   Reference count:               0
   Committed rate:                0
   Committed burst:               8192
   Peak rate:                     0
   Peak burst:                    8192
   Committed rate action:         transmit
   Conformed rate action:         transmit
   Exceeded rate action:          drop
```

Meaning Table 35 lists the **show rate-limit-profile** command output fields.

Table 35: show rate-limit-profile Output Fields

Field Name	Field Description
Rate-Limit-Profile	Create a rate limit profile
Profile Name	Name of the rate-limit profile
Profile Type	One-rate, two-rate, or hierarchical profile
Reference count	Number of policy lists that reference this rate-limit profile

Table 35: show rate-limit-profile Output Fields (continued)

Field Name	Field Description
Color-aware	Color-aware action (yes or no) taken for profile
Committed rate	Target rate for the traffic, in bits per second
Committed burst	Amount of bandwidth allocated to accommodate bursty traffic, in bytes
Excess burst	Amount of bandwidth allocated to accommodate a packet in progress when the rate is in excess of the burst, in bytes
Peak rate	Amount of bandwidth allocated to accommodate traffic flow in excess of the committed rate, in bits per second
Peak burst	Amount of bandwidth allocated to accommodate bursty traffic in excess of the peak rate, in bytes
Mask	Value of mask applied to ToS byte in IP packet header
Committed rate action	Policy action (drop, transmit, or mark) taken when traffic flow does not exceed the committed rate
Conformed rate action	Policy action (drop, transmit, or mark) taken when traffic flow exceeds the committed rate but remains below the peak rate
Exceeded rate action	Policy action (drop, transmit, or mark) taken when traffic flow exceeds the peak rate

Related Topics

- **show rate-limit-profile** command

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 36 lists the **show vlan subinterface** command output fields.

Table 36: 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

Table 36: show vlan subinterface Output Fields (continued)

Field Name	Field Description
VLAN policy	Type and name of the VLAN policy
filter	Number of packets and bytes that have been policed by the policy

Related Topics

- **show vlan subinterface** command

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 the *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 on 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
```