Chapter 15

Verify Traffic and Packets through the Router

This chapter describes how to verify traffic and packets entering and passing through your Juniper Networks router. (See Table 36.)

Table 36: Checklist for Verifying Traffic and Packets through the Router

Verify Traffic and Packets Tasks	Command or Action
Monitor Traffic through the Router on page 190	
1. Display Real-Time Statistics about All Interfaces on the Router on page 190	monitor interface traffic
2. Display Real-Time Statistics about an Interface on page 191	monitor interface *interface-name*
Verify Packets on page 193	
1. Monitor Packets Sent from and Received by the Routing Engine on page 193	monitor traffic interface *interface-name*
2. Display Key IP Header Information on page 194	show firewall log
3. Show Packet Count When a Firewall Filter Is Configured with the Count Option on page 195	show firewall filter *filter-name*
4. Display Traffic from the Point of View of the Packet Forwarding Engine on page 196	show pfe statistics traffic

Monitor Traffic through the Router

Purpose To continue your diagnosis of a problem, display real-time statistics about the traffic passing through physical interfaces on the router.

Steps To Take To display real-time statistics about physical interfaces, follow these steps:

1. Display Real-Time Statistics about All Interfaces on the Router on page 190
2. Display Real-Time Statistics about an Interface on page 191

Step 1: Display Real-Time Statistics about All Interfaces on the Router

Action To display real-time statistics about traffic passing through all interfaces on the router, use the following JUNOS command-line interface (CLI) operational mode command:

user@host> **monitor interface traffic**

Sample Output

```
user@host> monitor interface traffic
host name                          Seconds: 15                 Time: 12:31:09

Interface    Link  Input packets        (pps)     Output packets        (pps)
 so-1/0/0    Down              0          (0)                 0          (0)
 so-1/1/0    Down              0          (0)                 0          (0)
 so-1/1/1    Down              0          (0)                 0          (0)
 so-1/1/2    Down              0          (0)                 0          (0)
 so-1/1/3    Down              0          (0)                 0          (0)
 t3-1/2/0    Down              0          (0)                 0          (0)
 t3-1/2/1    Down              0          (0)                 0          (0)
 t3-1/2/2    Down              0          (0)                 0          (0)
 t3-1/2/3    Down              0          (0)                 0          (0)
 so-2/0/0      Up         211035          (1)             36778          (0)
 so-2/0/1      Up         192753          (1)             36782          (0)
 so-2/0/2      Up         211020          (1)             36779          (0)
 so-2/0/3      Up         211029          (1)             36776          (0)
 so-2/1/0      Up         189378          (1)             36349          (0)
 so-2/1/1    Down              0          (0)             18747          (0)
 so-2/1/2    Down              0          (0)             16078          (0)
 so-2/1/3      Up              0          (0)             80338          (0)
 at-2/3/0      Up              0          (0)                 0          (0)
 at-2/3/1    Down              0          (0)                 0          (0)

Bytes=b, Clear=c, Delta=d, Packets=p, Quit=q or ESC, Rate=r, Up=^U, Down=^D
```

What It Means The sample output displays traffic data for active interfaces and the amount that each field has changed since the command started or since the counters were cleared by using the C key. In this example, the monitor interface command has been running for 15 seconds since the command was issued or since the counters last returned to zero.

Step 2: Display Real-Time Statistics about an Interface

Action To display real-time statistics about traffic passing through an interface on the router, use the following JUNOS CLI operational mode command:

user@host> **monitor interface** *interface-name*

Sample Output

```
user@R1> monitor interface so-0/0/1

Next='n', Quit='q' or ESC, Freeze='f', Thaw='t', Clear='c', Interface='i'
R1

Interface: so-0/0/1, Enabled, Link is Up
Encapsulation: PPP, Keepalives, Speed: OC3 Traffic statistics:
  Input bytes:                   5856541 (88 bps)
  Output bytes:                  6271468 (96 bps)
  Input packets:                  157629 (0 pps)
  Output packets:                 157024 (0 pps)
Encapsulation statistics:
  Input keepalives:                42353
  Output keepalives:               42320
  LCP state: Opened
Error statistics:
  Input errors:                        0
  Input drops:                         0
  Input framing errors:                0
  Input runts:                         0
  Input giants:                        0
  Policed discards:                    0
  L3 incompletes:                      0
  L2 channel errors:                   0
  L2 mismatch timeouts:                0
  Carrier transitions:                 1
  Output errors:                       0
  Output drops:                        0
  Aged packets:                        0
Active alarms : None
Active defects: None
SONET error counts/seconds:
  LOS count                            1
  LOF count                            1
  SEF count                            1
  ES-S                                77
  SES-S                               77
SONET statistics:
  BIP-B1                               0
  BIP-B2                               0
  REI-L                                0
  BIP-B3                               0
  REI-P                                0
Received SONET overhead:  F1        : 0x00  J0        : 0xZ
```

What It Means The sample output shows the input and output packets for a particular SONET interface (so-0/0/1). The information can include common interface failures, such as SONET/SDH and T3 alarms, loopbacks detected, and increases in framing errors. For more information, see “Track Error Conditions” on page 273.

To control the output of the command while it is running, use the keys shown in Table 37.

Table 37: Monitor Interface Output Control Keys

Action	Key
Display information about the next interface. The monitor interface command scrolls through the physical or logical interfaces in the same order that they are displayed by the show interfaces terse command.	N
Display information about a different interface. The command prompts you for the name of a specific interface.	I
Freeze the display, halting the display of updated statistics.	F
Thaw the display, resuming the display of updated statistics.	T
Clear (zero) the current delta counters since monitor interface was started. It does not clear the accumulative counter.	C
Stop the monitor interface command.	Q

See the *JUNOS System Basics and Services Command Reference* for details on using match conditions with the monitor traffic command.

Verify Packets

Purpose You can check the flow of packets to and from the router to further your investigation of issues on the router.

Steps To Take To verify packets, follow these steps:

1. Monitor Packets Sent from and Received by the Routing Engine on page 193
2. Display Key IP Header Information on page 194
3. Show Packet Count When a Firewall Filter Is Configured with the Count Option on page 195
4. Display Traffic from the Point of View of the Packet Forwarding Engine on page 196

Step 1: Monitor Packets Sent from and Received by the Routing Engine

Action To print packet headers transmitted through network interfaces sent from or received by the Routing Engine, enter the following JUNOS CLI operational mode command:

user@host> **monitor traffic interface** *interface-name*

Sample Output

```
user@R1> monitor traffic interface so-0/0/1
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Listening on so-0/0/1, capture size 96 bytes

11:23:01.666720  In IP 10.1.15.2 > OSPF-ALL.MCAST.NET: OSPFv2 Hello length: 48
11:23:01.666884 Out IP 10.1.15.1 > OSPF-ALL.MCAST.NET: OSPFv2 Hello length: 48
11:23:01.681330 Out IP 10.0.0.1.bgp > 10.0.0.5.3813: P 3821434885:3821434904(19)
ack 165811073 win 16417 <nop,nop,timestamp 42120056 42108995>: BGP, length: 19
11:23:01.682041  In IP 10.0.0.5.3813 > 10.0.0.1.bgp: P 1:20(19) ack 19 win 16398
<nop,nop,timestamp 42111985 42120056>: BGP, length: 19
11:23:01.781132 Out IP 10.0.0.1.bgp > 10.0.0.5.3813: . ack 20 win 16398
<nop,nop,timestamp 42120066 42111985>
11:23:03.996629  In LCP echo request            (type 0x09  id 0x67  len 0x0008)
11:23:03.996645 Out LCP echo reply              (type 0x0a  id 0x67  len 0x0008)
11:23:04.801130 Out LCP echo request            (type 0x09  id 0x6d  len 0x0008)
11:23:04.801694  In LCP echo reply              (type 0x0a  id 0x6d  len 0x0008)
^C
11 packets received by filter
0 packets dropped by kernel
```

What It Means The sample output shows the actual packets entering and leaving the Routing Engine, not the transit packets passing through the router. You can use this information to diagnose issues such as Point-to-Point Protocol negotiation, Border Gateway Protocol negotiation, and Open Shortest Path First hellos.

The monitor traffic command is similar to the UNIX tcpdump command. For more information about the monitor traffic command, see the *JUNOS System Basics and Services Command Reference*.

CAUTION: Use the monitor traffic command to diagnose problems on your router. Do not to leave this command on because it consumes Routing Engine resources.

Step 2: Display Key IP Header Information

Action To display key IP header information if you have a firewall configured with a log action, enter the following JUNOS CLI operational mode command:

```
user@host> show firewall log
```

Sample Output

```
user@R1> show firewall log
Time     Filter     A Interface       Pro Source address  Destination address
16:08:04 pfe        A so-1/1/0.0      ICM 123.168.10.65   123.168.10.66:24373
16:08:03 pfe        A so-1/1/0.0      ICM 123.168.10.65   123.168.10.66:29531
16:08:02 pfe        A so-1/1/0.0      ICM 123.168.10.65   123.168.10.66:27265
16:08:01 pfe        A so-1/1/0.0      OSP 123.168.10.65   212.0.0.5:48
16:08:01 pfe        A so-1/1/0.0      ICM 123.168.10.65   123.168.10.66:43943
16:08:00 pfe        A so-1/1/0.0      ICM 123.168.10.65   123.168.10.66:58572
16:07:59 pfe        A so-1/1/0.0      ICM 123.168.10.65   123.168.10.66:56307
16:07:58 pfe        A so-1/1/0.0      ICM 123.168.10.65   123.168.10.66:60185
16:07:57 pfe        A so-1/1/0.0      ICM 123.168.10.65   123.168.10.66:1600
16:07:56 pfe        A so-1/1/0.0      ICM 123.168.10.65   123.168.10.66:6502
16:07:55 pfe        A so-1/1/0.0      ICM 123.168.10.65   123.168.10.66:17548
16:07:54 pfe        A so-1/1/0.0      ICM 123.168.10.65   123.168.10.66:5298
16:07:53 pfe        A so-1/1/0.0      ICM 123.168.10.65   123.168.10.66:24536
16:07:52 sample-test A so-1/1/0.0      ICM 123.168.10.65   123.168.10.66:24373
16:07:52 sample-test A local           ICM 123.168.10.66   123.168.10.65:22325
16:07:52 pfe        A so-1/1/0.0      ICM 123.168.10.65   123.168.10.66:27900
16:07:51 pfe        A so-1/1/0.0      OSP 123.168.10.65   212.0.0.5:48
16:07:51 sample-test A so-1/1/0.0      ICM 123.168.10.65   123.168.10.66:29531
16:07:51 sample-test A local           ICM 123.168.10.66
123.168.10.65:27483
```

What It Means The sample output shows key IP header information about firewall filters on the router. The source and destination addresses of packets provide important information when you investigate problems on the router.

The Filter field contains information about how a packet traveled through the router before it was handled by either the Routing Engine or the Packet Forwarding Engine.

- If the filter name appears in the Filter field, the Routing Engine handled the packet. For example, sample-test is a firewall filter configured at the [edit firewall] hierarchy level.

- If the word pfe appears in the Filter field, the Packet Forwarding Engine handled the packet. The Packet Forwarding Engine receives information about the name of the firewall filter.

All packets were accepted (A). Other actions are discard (D) and reject (R).

The Interface column shows that all packets came through so-1/1/0.0, and icm or osp are the represented protocols. Other possible protocol names are: egp, gre, ipip, pim, resp, tcp, or udp.

Step 3: Show Packet Count When a Firewall Filter Is Configured with the Count Option

Action To show the packet count when a firewall filter is configured with the count option, enter the following JUNOS CLI operational mode command:

user@host> **show firewall filter** *filter-name*

Sample Output 1 The following sample output shows the icmp filter incrementing:

```
user@R1> show firewall filter icmp
Filter: icmp
Counters:
Name                                                Bytes              Packets
count-icmp                                            252                    3
```

Sample Output 2 The following sample output shows a configuration of the count option:

```
[edit]
user@R1# show firewall filter icmp
term a {
    from {
        protocol icmp;
    }
    then count count-icmp;
}
term b {
    then accept;
}
```

What It Means The sample output shows that the packet matched a criteria in the icmp filter and the filter had a count action applied to it.

Step 4: Display Traffic from the Point of View of the Packet Forwarding Engine

Action To display traffic from the point of view of the Packet Forwarding Engine, enter the following JUNOS CLI operational mode command:

```
user@host> show pfe statistics traffic
```

Sample Output 1 The following sample output was taken before packets were sent:

```
user@R2> show pfe statistics traffic
PFE Traffic statistics:
               635392 packets input  (0 packets/sec)
               829862 packets output (0 packets/sec)

PFE Local Traffic statistics:
     579278 local packets input
     773747 local packets output
          0 software input high drops
          0 software input medium drops
          0 software input low drops
          1 software output drops
          0 hardware input drops

PFE Local Protocol statistics:
          0 hdlc keepalives
          0 atm oam
          0 fr lmi
     254613 ppp lcp/ncp
          0 ospf hello
          0 rsvp hello
     107203 isis iih

PFE Hardware Discard statistics:
          0 timeout
          0 truncated key
          0 bits to test
          0 data error
          0 stack underflow
          0 stack overflow
          0 normal discard
          0 extended discard
          0 invalid iif
          0 info cell drops
          0 fabric drops
```

Sample Output 2 The following sample output was taken after 100 packets were sent to router R2:

```
user@R2> show pfe statistics traffic
PFE Traffic statistics:
               635595 packets input  (2 packets/sec)
               829990 packets output (2 packets/sec)

PFE Local Traffic statistics:
     579373 local packets input
     773869 local packets output
          0 software input high drops
          0 software input medium drops
          0 software input low drops
          1 software output drops
          0 hardware input drops
```

```
PFE Local Protocol statistics:
          0 hdlc keepalives
          0 atm oam
          0 fr lmi
     254655 ppp lcp/ncp
          0 ospf hello
          0 rsvp hello
     107220 isis iih

PFE Hardware Discard statistics:
          0 timeout
          0 truncated key
          0 bits to test
          0 data error
          0 stack underflow
          0 stack overflow
        100 normal discard
          0 extended discard
          0 invalid iif
          0 info cell drops
          0 fabric drops
```

What It Means The sample output shows the number and rate of packets entering and leaving the Packet Forwarding Engine. For example, the 100 packets sent to R2 were discarded due to a route that had a discard next hop configured, as shown in the PFE Hardware Discard statistics field. All counters increased as a result of the 100 packets.