

# Chapter 11

## Flow Monitoring and Discard Accounting Overview

Using a Juniper Networks M-series router, a selection of PICs (including the Monitoring Services PIC or Adaptive Services PIC and other networking hardware, you can monitor traffic flow and export the monitored traffic. Monitoring traffic allows you to do the following:

- Gather and export detailed information about IPv4 traffic flows between source and destination nodes in your network.

- Sample all incoming IPv4 traffic on the monitoring interface and present the data in cflowd record format.

- Perform discard accounting on an incoming traffic flow.

- Encrypt or tunnel outgoing cflowd records, intercepted IPv4 traffic, or both.

- Direct filtered traffic to different packet analyzers and present the data in its original format (port mirror).

This section provides general information on the following topics:

- Passive Flow Monitoring on page 95

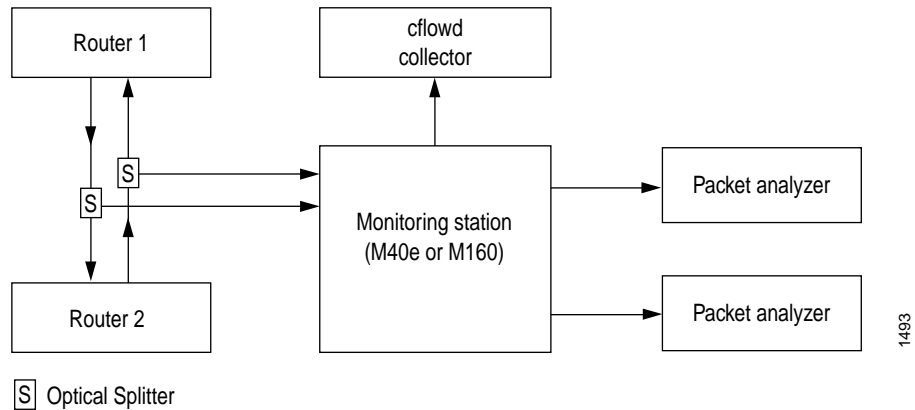
- Active Flow Monitoring on page 96

- Complete Monitoring Services Interface Configuration Hierarchy on page 98

### Passive Flow Monitoring

The M40e or M160 router used for passive monitoring does not route packets from the monitored interface, nor does it run any routing protocols related to those interfaces; it only receives traffic flows, collects intercepted traffic, and exports it to cflowd servers and packet analyzers. Figure 3 shows a typical topology for the passive flow-monitoring application.

Figure 3: Passive Monitoring Application Topology



Traffic travels normally between Router 1 and Router 2. To redirect IPv4 traffic, you insert an optical splitter on the interface between these two routers. The optical splitter copies and redirects the traffic to the monitoring station, which is an M40e or M160 router. The optical cable connects only the receive port on the monitoring station, never the transmit port. This configuration allows the monitoring station to receive traffic from the router being monitored but never to transmit it back.

If you are monitoring traffic flow, the Internet Processor II ASIC in the router forwards a copy of the traffic to the Monitoring Services PIC in the monitoring station. If there is more than one Monitoring Services PIC installed, the monitoring station distributes the load of the incoming traffic across the multiple PICs. The Monitoring Services PICs generate flow records in cflowd version 5 format, and the records are then exported to the cflowd collector.

If you are performing lawful interception of traffic between the two routers, the Internet Processor II ASIC filters the incoming traffic and forwards it to the Tunnel Services PIC. Filter-based forwarding is then applied to direct the traffic to the packet analyzers.

Optionally, the intercepted traffic or the cflowd records can be encrypted by the ES PIC and then sent to a cflowd server or packet analyzer.

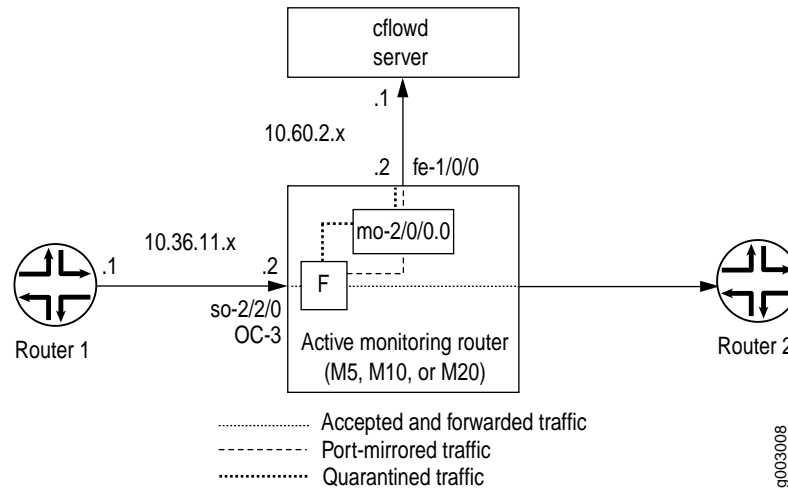
## Active Flow Monitoring

The Monitoring Services PIC can also be used as an active monitor if it is installed in an M-series router. The resulting active monitoring router participates in both the monitoring application and in the normal routing functionality of the network. The traffic to be monitored is captured with next-hop sampling using the JUNOS software's port-mirroring feature.

Specified packets can be filtered and sent to a Monitoring Services PIC. This PIC can be the same one that participates in port mirroring or it can be a different Monitoring Services PIC. To send filtered packets to a specified Monitoring Services PIC interface, you configure sampling, port mirroring, or discard accounting.

Figure 4 shows a sample topology.

Figure 4: Active Monitoring Configuration—Topology Diagram



In Figure 4, traffic from Router 1 arrives on the monitoring router's OC-3 interface. The exit interface on the monitoring router leading to destination Router 2 can be any interface type (such as SONET, Gigabit Ethernet, and so on). The export interface leading to the cflowd server is fe-1/0/0. To enable active monitoring, configure a firewall filter on the SONET interface with the following match conditions:

Traffic matching certain firewall conditions is sent to the Monitoring Services PIC using filter-based forwarding. This traffic is quarantined and not forwarded to other routers.

All other traffic is port-mirrored to the Monitoring Services PIC. Port mirroring copies each packet and sends the copies to the port-mirroring next hop (in this case, a Monitoring Services PIC). The original packets are forwarded out of the router as usual.

## Complete Monitoring Services Interface Configuration Hierarchy

To configure flow monitoring and accounting properties, include the following statements at the [edit interfaces] hierarchy level:

```
[edit interfaces]
mo-fpc/pic/port {
  unit logical-unit-number {
    family inet {
      accounting {
        destination-class-usage;
        source-class-usage direction;
      }
    }
    address address {
      destination address;
    }
    filter {
      group filter-group-number;
      input filter-name;
      output filter-name;
    }
    receive-options-packets;
    receive-ttl-exceeded;
    sampling direction;
  }
}
multiservice-options {
  boot-command filename;
  (core-dump | no-core-dump);
  (syslog | no-syslog);
}
}
so-fpc/pic/port {
  unit logical-unit-number {
    passive-monitor-mode;
  }
}
```

To configure flow monitoring and accounting properties, include the following statements at the [edit forwarding-options] hierarchy level:

```
[edit forwarding-options]
accounting name {
  output {
    aggregate-export-interval seconds;
    cflowd hostname {
      aggregation {
        autonomous-system;
        destination-prefix;
        protocol-port;
        source-destination-prefix {
          caida-compliant;
        }
        source-prefix;
      }
    }
    autonomous-system-type (origin | peer);
    port port-number;
    version format;
  }
}
```



```

sampling {
  disable;
  input {
    family inet{
      max-packets-per-second number;
      rate number;
      run-length number;
    }
  }
  output {
    aggregate-export-interval seconds;
    cflowd hostname {
      aggregation {
        autonomous-system;
        destination-prefix;
        protocol-port;
        source-destination-prefix {
          caida-compliant;
        }
        source-prefix;
      }
      autonomous-system-type (origin | peer);
      (local-dump | no-local-dump);
      port port-number;
      source-address address;
      version format;
    }
    file {
      disable;
      filename filename;
      files number;
      size bytes;
      (stamp | no-stamp);
      (world-readable | no-world-readable);
    }
    flow-active-timeout seconds;
    flow-inactive-timeout seconds;
    interface interface-name {
      engine-id number;
      engine-type number;
      source-address address;
    }
  }
  traceoptions {
    file filename {
      files number;
      size bytes;
      (world-readable | no-world-readable);
    }
  }
}

```

**Note**

For the complete [edit forwarding-options] hierarchy, see the *JUNOS Internet Software Configuration Guide: Policy Framework*. This section documents only the statements used in flow monitoring and accounting services.