JUNIPER NETWORKS

Network Configuration Example

Configuring Active Flow Monitoring Version 9 on PTX Series Routers Tethered to a CSE2000

Published: 2014-11-06

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

Network Configuration Example Configuring Active Flow Monitoring Version 9 on PTX Series Routers Tethered to a CSE2000
NCE0144

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.

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

About This Network Configuration Example

This network configuration example provides an overview and examples showing how active flow monitoring version 9 can be configured on PTX3000 and PTX5000 routers tethered to a CSE2000. The step-by-step instructions in this document will help you to collect a set of sampled flows from the PTX Series routers and send the v9 records to a specified host.

Active Flow Monitoring on PTX Series Routers with CSE2000 Overview

Although the Monitoring Services PIC can be used in an active flow monitoring topology on various Juniper Networks® routers, the Monitoring Services PIC is not supported on Juniper Networks PTX Series Packet Transport Routers because of challenges in terms of CPU and memory requirements for wired and mobile applications that are supported by the PTX Series routers. Furthermore, PTX Series routers do not support inline sampling. Considering the vast coverage of PTX Series routers, it is necessary to scale the control plane and service plane at a competitive level by using new hardware that has a more powerful processor and a higher service capability.

Juniper Networks Carrier-Grade Service Engine (CSE) is a solution that enables Juniper Networks PTX5000 Packet Transport Routers and Juniper Networks PTX3000 Packet Transport Routers to provide high-performance flow monitoring and accounting services. The CSE2000 device is tethered to the PTX Series router and provides support for active flow monitoring version 9. The CSE2000 enables scaling of the control plane and service plane, without adding components to the existing PTX Series router.

NOTE: You can connect the CSE2000 to PTX Series routers in one of the following ways:

- Connect CSE2000 to a PTX5000 router.
- Connect CSE2000 to a PTX3000 router.
- Connect CSE2000 to two PTX3000 routers.
- Connect CSE2000 to two PTX5000 routers.
- Connect CSE2000 to a PTX5000 router and a PTX3000 router.

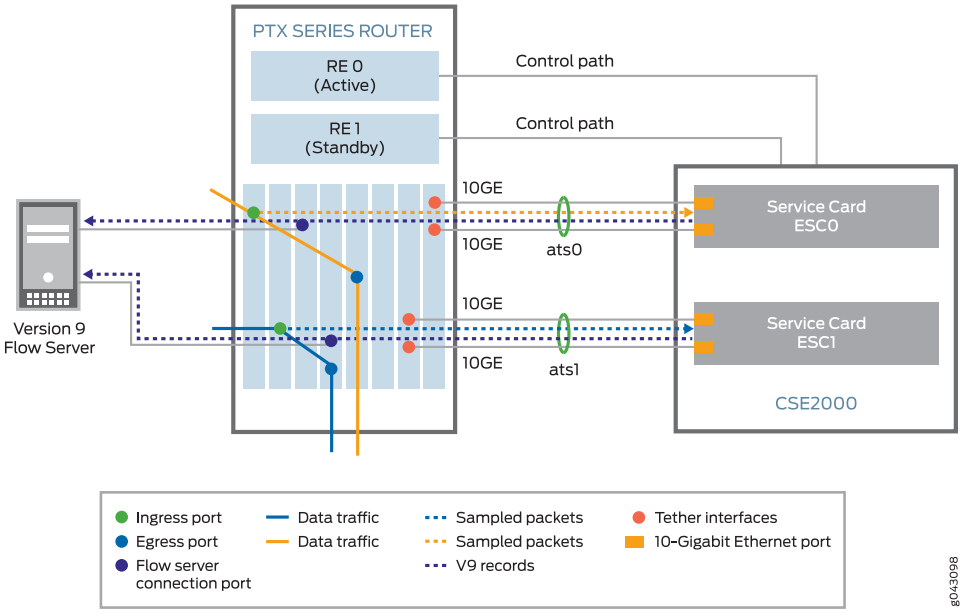
For more information about connecting the CSE2000 to PTX Series routers, see the *CSE2000 Hardware Installation Guide*.

Using the CSE2000 tethered to a PTX Series router, you can perform the following operations:

- Traffic sampling—You can create a copy of traffic and send it to the CSE2000, which performs flow accounting while the PTX Series router forwards the packet to its original destination.

- Active flow monitoring—Active monitoring implies that flow monitoring is carried out on the same router (the CSE2000 is treated as a part of the router) that forwards the packets being monitored.
- Flow aggregation—You can collect an aggregate of sampled flows and send the aggregate to a specified host that runs the version 9 format defined in RFC 3954 *Cisco Systems NetFlow Services Export Version 9*. With the version 9 format, you can sample IPv4, IPv6, and MPLS traffic.

Figure 1: Active Flow Monitoring Version 9 by Tethering CSE2000 to PTX Series Router



The CSE2000 is tethered to a PTX Series router to enable active flow monitoring version 9. Active flow monitoring version 9, which is based on RFC 3954, provides a way to organize flow data into templates. It also provides a way to actively monitor IPv4, IPv6, and MPLS flows. Active flow monitoring version 9 runs as an application on the CSE2000. Control and data path connectivity between a PTX Series router and the CSE2000 is shown in Figure 1 on page 2.

Control path connectivity between the PTX Series router and the CSE2000 is required for generating proper active flow monitoring version 9 records, for downloading templates, and for collecting the statistics.

Data path connectivity from the PTX Series router to the CSE2000 is enabled by means of tethered interfaces. A maximum of two interfaces can be connected to a single CSE2000 service card. These two interfaces must be present on the same Flexible PIC Concentrator (FPC) in the PTX Series router. These tethered interfaces form a logical interface and are called aggregated tethered services (ATS) interfaces. ATS interfaces are similar to aggregated Ethernet interfaces; however, they do not support the Link Aggregation Control Protocol (LACP).

As shown in Figure 1 on page 2, traffic enters through the ingress port on a PTX Series router on which sampling is configured, the sampled packets are sent to the CSE2000 through the tethered interfaces, and traffic goes out through the egress port. Active flow monitoring version 9 operations are performed on the CSE2000, and the packets are exported in the form of v9 records from the CSE2000 to the PTX Series router. The PTX Series router forwards the v9 records to the version 9 flow server.

Related Documentation

- Example: Configuring Active Flow Monitoring Version 9 on a PTX Series Router Tethered to a CSE2000 on page 3
- Example: Configuring Active Flow Monitoring Version 9 on a PTX3000 and PTX5000 When Both Are Tethered to a CSE2000 on page 23

Example: Configuring Active Flow Monitoring Version 9 on a PTX Series Router Tethered to a CSE2000

This example shows how to configure active flow monitoring version 9 for simultaneous IPv4, IPv6, and MPLS flows on a PTX Series Packet Transport Router that is tethered to a CSE2000. All the configurations mentioned in this example are performed on a PTX5000 router. The step-by-step instructions in this example will help you to configure traffic sampling on a PTX5000 router, generate the v9 records, and send these records to a specified host.

NOTE: **The steps to configure active flow monitoring version 9 for simultaneous IPv4, IPv6, and MPLS flows on a PTX3000 router are the same as those required on a PTX5000 router.**

This example contains the following sections:

Requirements

This example requires the following hardware and software components:

- One PTX5000 router running Junos OS Release 13.3R4 or later
- One CSE2000 running CSE Series Release 13.3R4 or later
- Version 9 flow server (to collect sampled flows using the version 9 format)

Before you configure active flow monitoring version 9, connect the CSE2000 to the PTX5000 router. For more information, see the *CSE2000 Hardware Installation Guide*.

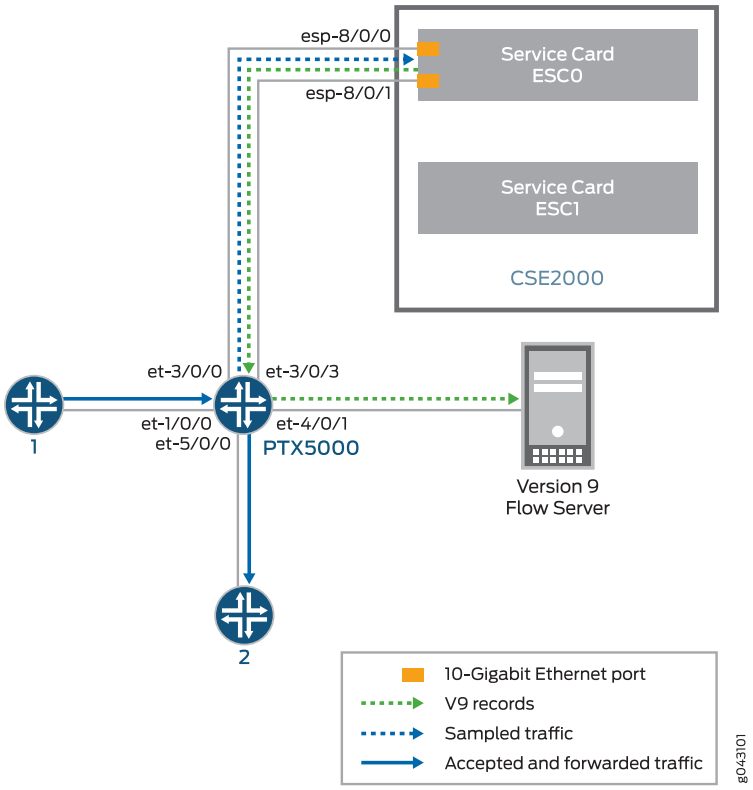
Overview and Topology

This example shows the configuration of active flow monitoring version 9 for simultaneous IPv4, IPv6, and MPLS flows on a PTX5000 router that is tethered to the CSE2000. All the configurations mentioned in this example are performed on the PTX5000 router.

The topology for this example consists of a PTX5000 router on which active flow monitoring version 9 needs to be enabled (see Figure 2 on page 4). Interface et-1/0/0 is the ingress interface through which packets enter the PTX5000 router. Traffic sampling is performed on the interface et-1/0/0. The PTX5000 router forwards the traffic to the egress interface et-5/0/0, and the sampled traffic to the 10-Gigabit Ethernet interfaces et-3/0/0 and et-3/0/3.

The physical connections used in this example are shown Figure 2 on page 4.

Figure 2: Active Flow Monitoring Version 9 for Simultaneous IPv4, IPv6, and MPLS Topology



On the CSE2000, the service card ESC0 has two 10-Gigabit Ethernet interfaces (esp-8/0/0 and esp-8/0/1), which are used to connect to the 10-Gigabit Ethernet PICs on the PTX5000 for the sampled traffic. The CSE2000 performs active flow monitoring on the sampled traffic and exports the version 9 records through esp interfaces to the PTX5000 router. The PTX5000 router forwards the v9 records to the version 9 flow server.

In this example, ats0 is the ATS interface that connects the PTX5000 router and the CSE2000. The interfaces et-3/0/3 and et-3/0/0 need to be configured as the member interfaces of the ats0 interface.

NOTE:

- The CSE2000 service card logically occupies the last slot on the router chassis. A PTX3000 chassis has 16 slots, numbered 0 through 15. The CSE2000 service card occupies slot 16. If the ats0 interface is configured and connected, the external service ports (ESPs) on the CSE2000 are represented as esp-16/0/0 and esp-16/0/1. If the ats1 interface is configured, the ESPs are represented as esp-16/1/0 and esp-16/1/1.
- The CSE2000 connected to a PTX3000 router uses 10-Gigabit Ethernet interfaces (esp-16/0/0 and esp-16/0/1).

Configuration

To configure active flow monitoring version 9 for IPv4, IPv6, and MPLS flows on a PTX5000 router tethered to a CSE2000, perform these tasks:

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces et-3/0/0 gigether-options 802.3ad ats0
set interfaces et-3/0/3 gigether-options 802.3ad ats0
set interfaces ats0 unit 0 family inet
set interfaces ats0 unit 0 family inet6
set interfaces ats0 unit 0 family mpls
set services flow-monitoring version9 template v4-template
set services flow-monitoring version9 template v6-template
set services flow-monitoring version9 template mpls
set services flow-monitoring version9 template v4-template flow-active-timeout 60
set services flow-monitoring version9 template v4-template flow-inactive-timeout 30
set services flow-monitoring version9 template v4-template template-refresh-rate
  packets 480
set services flow-monitoring version9 template v4-template option-refresh-rate packets
  480
```

```
set services flow-monitoring version9 template v6-template flow-active-timeout 60
set services flow-monitoring version9 template v6-template flow-inactive-timeout 30
set services flow-monitoring version9 template v6-template template-refresh-rate
  packets 480
set services flow-monitoring version9 template v6-template option-refresh-rate packets
  480
set services flow-monitoring version9 template mpls flow-active-timeout 60
set services flow-monitoring version9 template mpls flow-inactive-timeout 30
set services flow-monitoring version9 template mpls template-refresh-rate packets 480
set services flow-monitoring version9 template mpls option-refresh-rate packets 480
set services flow-monitoring version9 template v4-template ipv4-template
set services flow-monitoring version9 template v6-template ipv6-template
set services flow-monitoring version9 template mpls mpls-template
set services flow-monitoring version9 template mpls mpls-template label-position [ 1 2
  ]
set firewall family inet filter ipv4_sample_filter term 1 then count c1
set firewall family inet filter ipv4_sample_filter term 1 then sample
set firewall family inet filter ipv4_sample_filter term 1 then accept
set firewall family inet6 filter ipv6_sample_filter term 1 then count c1
set firewall family inet6 filter ipv6_sample_filter term 1 then sample
set firewall family inet6 filter ipv6_sample_filter term 1 then accept
set firewall family mpls filter mpls_sample_filter term 1 then count c1
set firewall family mpls filter mpls_sample_filter term 1 then sample
set firewall family mpls filter mpls_sample_filter term 1 then accept
set interfaces et-1/0/0 unit 0 family inet filter input ipv4_sample_filter
set interfaces et-1/0/0 unit 0 family inet6 filter input ipv6_sample_filter
set interfaces et-1/0/0 unit 0 family mpls filter input mpls_sample_filter
set forwarding-options sampling instance ins1 input rate 10
set forwarding-options sampling instance ins1 input run-length 1
set forwarding-options sampling instance ins1 input maximum-packet-length 128
set chassis fpc 1 sampling instance ins1
set forwarding-options sampling instance ins1 family inet output flow-server 192.0.2.2
  port 2055
set forwarding-options sampling instance ins1 family inet6 output flow-server 192.0.2.2
  port 2055
set forwarding-options sampling instance ins1 family mpls output flow-server 192.0.2.2
  port 2055
set forwarding-options sampling instance ins1 family inet output flow-server 192.0.2.2
  version9 template v4-template
set forwarding-options sampling instance ins1 family inet6 output flow-server 192.0.2.2
  version9 template v6-template
set forwarding-options sampling instance ins1 family mpls output flow-server 192.0.2.2
  version9 template mpls
set forwarding-options sampling instance ins1 family inet output interface ats0
  source-address 192.0.2.1
set forwarding-options sampling instance ins1 family inet output interface ats0 export-port
  address 192.0.2.1/24
set forwarding-options sampling instance ins1 family inet6 output interface ats0
  source-address 192.0.2.1
set forwarding-options sampling instance ins1 family inet6 output interface ats0
  export-port address 192.0.2.1/24
set forwarding-options sampling instance ins1 family mpls output interface ats0
  source-address 192.0.2.1
set forwarding-options sampling instance ins1 family mpls output interface ats0
  export-port address 192.0.2.1/24
```


Configuring the Member Interfaces and Interface Family for Aggregated Tethered Services Interfaces

Step-by-Step Procedure

The interfaces et-3/0/0 and et-3/0/3 of the PTX5000 router that connect to the CSE2000 are configured as the member interfaces of the ATS interface ats0. This configuration associates the physical links of the router with the logical bundle of the ATS interface. You must also specify the constituent physical links by including the **802.3ad** statement. All the configurations are performed on the PTX5000 router.

To configure the member interfaces and interface family for the ATS interface bundle ats0:

1. Configure the interfaces et-3/0/0 and et-3/0/3 to form the ATS interface bundle ats0.

   ```
   [edit interfaces]
   user@ptx5000# set et-3/0/0 gigether-options 802.3ad ats0
   user@ptx5000# set et-3/0/3 gigether-options 802.3ad ats0
   ```

2. Configure the ats0 interface to process IPv4, IPv6, and MPLS addresses by including the **family** statement and specifying the **inet**, **inet6**, and **mpls** options, respectively, at the **[edit interfaces]** hierarchy level.

   ```
   [edit interfaces]
   user@ptx5000# set ats0 unit 0 family inet
   user@ptx5000# set ats0 unit 0 family inet6
   user@ptx5000# set ats0 unit 0 family mpls
   ```

Configuring the Active Flow Monitoring Version 9 Template for IPv4, IPv6, and MPLS Flows

Step-by-Step Procedure

To activate templates in flow monitoring, you must configure a template and include that template in the version 9 flow monitoring configuration.

To configure a version 9 template for IPv4, IPv6, and MPLS flows:

1. Create a version 9 template for IPv4 flows by including the **flow-monitoring version9 template** statement and specifying **v4_template** as the name of the template at the **[edit services]** hierarchy level.

   ```
   [edit services]
   user@ptx5000# set flow-monitoring version9 template v4_template
   ```

2. Create a version 9 template for IPv6 flows by including the **flow-monitoring version9 template** statement and specifying **v6_template** as the name of the template at the **[edit services]** hierarchy level.

   ```
   [edit services]
   user@ptx5000# set flow-monitoring version9 template v6_template
   ```

3. Create a version 9 template for MPLS flows by including the **flow-monitoring version9 template** statement and specifying **mpls** as the name of the template at the **[edit services]** hierarchy level.

   ```
   [edit services]
   ```

```
user@ptx5000# set flow-monitoring version9 template mpls
```

4. Configure the active timeout and the inactive timeout values for the traffic flows by including the **flow-active-timeout** and **flow-inactive-timeout** statements at the **[edit services flow-monitoring version9 template v4_template]**, **[edit services flow-monitoring version9 template v6_template]**, and **[edit services flow-monitoring version9 template mpls]** hierarchy levels.

   - If the interval between the time the last packet was received and the time the flow was last exported exceeds the configured value, the flow is exported to the flow server.
   - If the interval between the current time and the time that the last packet for this flow was received exceeds the configured inactive timeout value, the flow is allowed to expire.

     In this example, the active timeout value is 60 seconds and the inactive timeout value is 30 seconds.

     ```
     [edit services flow-monitoring version9 template v4_template]
     user@ptx5000# set flow-active-timeout 60
     user@ptx5000# set flow-inactive-timeout 30

     [edit services flow-monitoring version9 template v6_template]
     user@ptx5000# set flow-active-timeout 60
     user@ptx5000# set flow-inactive-timeout 30

     [edit services flow-monitoring version9 template mpls]
     user@ptx5000# set flow-active-timeout 60
     user@ptx5000# set flow-inactive-timeout 30
     ```

5. Enable the template for IPv4, IPV6, and MPLS flows.

   - Enable the template for IPv4 flows by including the **ipv4-template** statement at the **[edit services flow-monitoring version9 template v4_template]** hierarchy level.

     ```
     [edit services flow-monitoring version9 template v4_template]
     user@ptx5000# set ipv4-template
     ```

   - Enable the template for IPv6 flows by including the **ipv6-template** statement at the **[edit services flow-monitoring version9 template v6_template]** hierarchy level.

     ```
     [edit services flow-monitoring version9 template v6_template]
     user@ptx5000# set ipv6-template
     ```

   - Enable the template for MPLS flows by including the **mpls-template** statement at the **[edit services flow-monitoring version9 template mpls]** hierarchy level. Also include the **label-position** statement and specify label positions 1 and 2 at the **[edit services flow-monitoring version9 template mpls mpls-template]** hierarchy level.

     ```
     [edit services flow-monitoring version9 template mpls]
     user@ptx5000# set mpls-template

     [edit services flow-monitoring version9 template mpls mpls-template]
     user@ptx5000# set label-position [ 1 2 ]
     ```

6. Configure the rate at which the router sends IPv4, IPv6, and MPLS template definitions and options to the flow server for IPv4, IPv6, and MPLS traffic. Because

version 9 flow monitoring traffic is unidirectional from the router to the flow server, configure the router to send template definitions and options, such as sampling rate, to the server. In this example, the template definitions and options are refreshed for every 480 packets.

- Include the **template-refresh-rate** and **option-refresh-rate** statements at the **[edit services flow-monitoring version9 template v4_template]** hierarchy level.

```
[edit services flow-monitoring version9 template v4_template]
user@ptx5000# set template-refresh-rate packets 480
user@ptx5000# set option-refresh-rate packets 480
```

- Include the **template-refresh-rate** and **option-refresh-rate** statements at the **[edit services flow-monitoring version9 template v6_template]** hierarchy level.

```
[edit services flow-monitoring version9 template v6_template]
user@ptx5000# set template-refresh-rate packets 480
user@ptx5000# set option-refresh-rate packets 480
```

- Include the **template-refresh-rate** and **option-refresh-rate** statements at the **[edit services flow-monitoring version9 template mpls]** hierarchy level.

```
[edit services flow-monitoring version9 template mpls]
user@ptx5000# set template-refresh-rate packets 480
user@ptx5000# set option-refresh-rate packets 480
```

Configuring the Firewall Filter

Step-by-Step Procedure

The firewall filter identifies the traffic flows that need to be sampled and processed by the CSE2000.

To configure the firewall filter:

1. - To configure the firewall filter for IPv4, include the **filter** statement and specify ipv4_sample_filter as the name of the filter at the **[edit firewall family inet]** hierarchy level. Include the **term** statement and specify 1 as the name of the term. For active monitoring using version 9, you must include the **sample** and **accept** action statements at the **[edit firewall family inet]** hierarchy level.

```
[edit firewall family inet]
user@ptx5000# set filter ipv4_sample_filter term 1 then count c1
user@ptx5000# set filter ipv4_sample_filter term 1 then sample
user@ptx5000# set filter ipv4_sample_filter term 1 then accept
```

   - To configure the firewall filter for IPv6, include the **filter** statement and specify ipv6_sample_filter as the name of the filter at the **[edit firewall family inet6]** hierarchy level. Include the **term** statement and specify 1 as the name of the term. For active monitoring using version 9, you must include the **sample** and **accept** action statements at the **[edit firewall family inet6]** hierarchy level.

```
[edit firewall family inet6]
user@ptx5000# set filter ipv6_sample_filter term 1 then count c1
user@ptx5000# set filter ipv6_sample_filter term 1 then sample
user@ptx5000# set filter ipv6_sample_filter term 1 then accept
```

- To configure the firewall filter for MPLS, include the **filter** statement and specify mpls_sample_filter as the name of the filter at the **[edit firewall family mpls]** hierarchy level. Include the **term** statement and specify 1 as the name of the term. For active monitoring using version 9, you must include the **sample** and **accept** action statements at the **[edit firewall family mpls]** hierarchy level.

  ```
  [edit firewall family mpls]
  user@ptx5000# set filter mpls_sample_filter term 1 then count c1
  user@ptx5000# set filter mpls_sample_filter term 1 then sample
  user@ptx5000# set filter mpls_sample_filter term 1 then accept
  ```

2. Apply the firewall filter to the interface where traffic flow needs to be sampled.

   The filter can be applied to either the ingress or the egress traffic depending on the use case. In this example, the filter is applied to the ingress (input) traffic.

   - To apply the firewall filter to the et-1/0/0 interface for IPv4, include the **input** statement and specify ipv4_sample_filter as the name of the filter at the **[edit interfaces et-1/0/0 unit 0 family inet filter]** hierarchy level.

     ```
     [edit interfaces et-1/0/0 unit 0 family inet filter ]
     user@ptx5000# set input ipv4_sample_filter
     ```

   - To apply the firewall filter to the et-1/0/0 interface for IPv6, include the **input** statement and specify iPv6_sample_filter as the name of the filter at the **[edit interfaces et-1/0/0 unit 0 family inet6 filter]** hierarchy level.

     ```
     [edit interfaces et-1/0/0 unit 0 family inet6 filter]
     user@ptx5000# set input ipv6_sample_filter
     ```

   - To apply the firewall filter to the et-1/0/0 interface for MPLS, include the **input** statement and specify mpls_sample_filter as the name of the filter at the **[edit interfaces et-1/0/0 unit 0 family mpls filter]** hierarchy level.

     ```
     [edit interfaces et-1/0/0 unit 0 family mpls filter]
     user@ptx5000# set input mpls_sample_filter
     ```

Configuring Traffic Sampling

Step-by-Step Procedure

Traffic sampling enables you to copy traffic to the CSE2000, which performs flow accounting while the router forwards the packet to its original destination. You can configure traffic sampling by defining a sampling instance that specifies a name for the sampling parameters and binding the instance name to a particular FPC.

To configure traffic sampling:

1. Configure the sampling instance ins1 with sampling rate 10, run length 1, and the maximum packet length of 128 bytes.

   ```
   [edit forwarding-options]
   user@ptx5000# set sampling instance ins1 input rate 10
   user@ptx5000# set sampling instance ins1 input run-length 1
   user@ptx5000# set sampling instance ins1 input maximum-packet-length 128
   ```

2. Apply the sampling instance to an FPC on the PTX5000 router by including the **sampling-instance** statement at the **[edit chassis]** hierarchy level.

The FPC number must match the FPC portion of the interface name for the interface on which sampling is enabled. In this example, FPC 1 is associated with the interface et-1/0/0 on which sampling is enabled.

```
[edit chassis]
user@ptx5000# set fpc 1 sampling instance ins1
```

Configuring the Flow Server to Collect the Active Flow Monitoring Version 9 Records

Step-by-Step Procedure

To configure the flow server:

1. Configure the flow server for IPv4, IPv6, and MPLS flows.

   - To configure the flow server for IPv4, include the **flow-server** statement and specify 192.0.2.2 as the IPv4 address of the host system that is collecting traffic flows at the **[edit forwarding-options sampling instance ins1 family inet output]** hierarchy level. Also include the **port** statement and specify UDP port 2055 for use by the flow server.

     ```
     [edit forwarding-options sampling instance ins1 family inet output]
     user@ptx5000# set flow-server 192.0.2.2 port 2055
     ```

   - To configure the flow server for IPv6, include the **flow-server** statement and specify 192.0.2.2 as the IPv4 address of the host system that is collecting traffic flows at the **[edit forwarding-options sampling instance ins1 family inet6 output]** hierarchy level. Also include the **port** statement and specify UDP port 2055 for use by the flow server.

     ```
     [edit forwarding-options sampling instance ins1 family inet6 output]
     user@ptx5000# set flow-server 192.0.2.2 port 2055
     ```

   - To configure the flow server for MPLS, include the **flow-server** statement and specify 192.0.2.2 as the IPv4 address of the host system that is collecting traffic flows at the **[edit forwarding-options sampling instance ins1 family mpls output]** hierarchy level. Also include the **port** statement and specify UDP port 2055 for use by the flow server.

     ```
     [edit forwarding-options sampling instance ins1 family mpls output]
     user@ptx5000# set flow-server 192.0.2.2 port 2055
     ```

2. Enable active flow monitoring by using the version 9 template format.

   - To enable active flow monitoring for IPv4 flows by using the version 9 template format, include the **version9 template** statement and specify **v4_template** as the name of the template to use at the **[edit forwarding-options sampling instance ins1 family inet output flow-server 192.0.2.2]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family inet output flow-server
       192.0.2.2]
     user@ptx5000# set version9 template v4_template
     ```

   - To enable active flow monitoring for IPv6 flow by using the version 9 template format, include the **version9 template** statement and specify **v6_template** as the name of the template to use at the **[edit forwarding-options sampling instance ins1 family inet6 output flow-server 192.0.2.2]** hierarchy level.

```
[edit forwarding-options sampling instance ins1 family inet6 output flow-server
  192.0.2.2 ]
user@ptx5000# set version9 template v6_template
```

- To enable active flow monitoring for MPLS flows by using the version 9 template format, include the **version9 template** statement and specify **mpls** as the name of the template to use at the **[edit forwarding-options sampling instance ins1 family mpls output flow-server 192.0.2.2]** hierarchy level.

```
[edit forwarding-options sampling instance ins1 family mpls output flow-server
  192.0.2.2]
user@ptx5000# set version9 template mpls
```

3. Configure the interface connected to the flow server by specifying the source address for generating the monitored packets.

   - For IPv4 flows, configure the interface connected to the flow server by specifying 192.0.2.1 as the source address for generating the monitored packets at the **[edit forwarding-options sampling instance ins1 family inet output]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family inet output]
     user@ptx5000# set interfaces ats0 source-address 192.0.2.1
     ```

   - For IPv6 flows, configure the interface connected to the flow server by specifying 192.0.2.1 as the source address for generating the monitored packets at the **[edit forwarding-options sampling instance ins1 family inet6 output]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family inet6 output]
     user@ptx5000# set interfaces ats0 source-address 192.0.2.1
     ```

   - For MPLS flows, configure the interface connected to the flow server by specifying 192.0.2.1 as the source address for generating the monitored packets at the **[edit forwarding-options sampling instance ins1 family mpls output]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family mpls output]
     user@ptx5000# set interfaces ats0 source-address 192.0.2.1
     ```

4. Configure the address of the export port that is used by the v9 records to reach the flow server.

   - For IPv4 flows, configure the export port address 192.0.2.1/24 at the **[edit forwarding-options sampling instance ins1 family inet output]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family inet output]
     user@ptx5000# set interface ats0 export-port address 192.0.2.1/24
     ```

   - For IPv6 flows, configure the export port address 192.0.2.1/24 at the **[edit forwarding-options sampling instance ins1 family inet6 output]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family inet6 output]
     user@ptx5000# set interface ats0 export-port address 192.0.2.1/24
     ```

   - For MPLS flows, configure the export port address 192.0.2.1/24 at the **[edit forwarding-options sampling instance ins1 family mpls output]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family mpls output]
     user@ptx5000# set interface ats0 export-port address 192.0.2.1/24
     ```


Results

Display the results of the configuration.

```
user@ptx5000> show configuration
  chassis {
    fpc 1 {
      sampling-instance ins1;
    }
  }
  services {
    flow-monitoring {
      version9 {
        template v4_template {
          flow-active-timeout 60;
          flow-inactive-timeout 30;
          template-refresh-rate {
            packets 480;
          }
          option-refresh-rate {
            packets 480;
          }
          ipv4-template;
        }
        template v6_template {
          flow-active-timeout 60;
          flow-inactive-timeout 30;
          template-refresh-rate {
            packets 480;
          }
          option-refresh-rate {
            packets 480;
          }
          ipv6-template;
        }
        template mpls {
          flow-active-timeout 60;
          flow-inactive-timeout 30;
          template-refresh-rate {
            packets 480;
          }
          option-refresh-rate {
            packets 480;
          }
          mpls-template {
            label-position [ 1 2];
          }
        }
      }
    }
  }
  interfaces {
    et-1/0/0 {
      unit 0 {
        family inet {
```

```
            filter {
              input ipv4_sample_filter;
            }
          }
          family inet6 {
            filter {
              input ipv6_sample_filter;
            }
          }
          family mpls {
            filter {
              input mpls_sample_filter;
            }
          }
        }
      }
      et-3/0/0 {
        gigether-options {
          802.3ad ats0;
        }
      }
      et-3/0/3 {
        gigether-options {
          802.3ad ats0;
        }
      }
      ats0 {
        unit 0 {
          family inet;
          family inet6;
          family mpls;
        }
      }
    }
    forwarding-options {
      sampling {
        instance {
          ins1 {
            input {
              rate 10;
              run-length 1;
              maximum-packet-length 128;
            }
            family inet {
              output {
                flow-server 192.0.2.2 {
                  port 2055;
                  version9 {
                    template {
                      v4_template;
                    }
                  }
                }
                interface ats0 {
                  source-address 192.0.2.1;
                  export-port {
```

```
                address 192.0.2.1/24;
              }
            }
          }
        }
        family inet6 {
          output {
            flow-server 192.0.2.2 {
              port 2055;
              version9 {
                template {
                  v6_template;
                }
              }
            }
            interface ats0 {
              source-address 192.0.2.1;
              export-port {
                address 192.0.2.1/24;
              }
            }
          }
        }
        family mpls{
          output {
            flow-server 192.0.2.2 {
              port 2055;
              version9 {
                template {
                  mpls;
                }
              }
            }
            interface ats0 {
              source-address 192.0.2.1;
              export-port {
                address 192.0.2.1/24;
              }
            }
          }
        }
      }
    }
  }
}
firewall {
  family inet {
    filter ipv4_sample_filter {
      term 1 {
        then {
          count c1;
          sample;
          accept;
        }
      }
    }
```

```
    }
    family inet6 {
      filter ipv6_sample_filter {
        term 1 {
          then {
            count c1;
            sample;
            accept;
          }
        }
      }
    }
    family mpls {
      filter mpls_sample_filter {
        term 1 {
          then {
            count c1;
            sample;
            accept;
          }
        }
      }
    }
  }
```

Verification

Confirm that the configuration is working properly.

Verifying That the Packets Are Received on the Router

Purpose Verify that the packets are received on the router.

Action In operational mode, enter the **show interface et-1/0/0** command.

```
user@ptx5000> show interface et-1/0/0
username@router> show interfaces et-1/0/0
Physical interface: et-1/0/0, Enabled, Physical link is Up
  Interface index: 325, SNMP ifIndex: 537
  Link-level type: Ethernet, MTU: 1514, Speed: 10Gbps, BPDU Error: None,
MAC-REWRITE Error: None, Loopback: Disabled, Source filtering: Disabled,
  Flow control: Enabled
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Current address: f8:c0:01:3a:c6:98, Hardware address: f8:c0:01:3a:c6:98
  Last flapped   : 2012-12-18 06:53:45 PST (14:44:49 ago)
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)
  Active alarms  : None
  Active defects : None
  Interface transmit statistics: Disabled
  Logical interface et-1/0/0.0 (Index 76) (SNMP ifIndex 583)
    Flags: SNMP-Traps 0x4004000 Encapsulation: ENET2
    Input packets : 108
    Output packets: 108
    Protocol inet, MTU: 1500
      Flags: Sendbcast-pkt-to-re
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 1.1.1/24, Local: 1.1.1.1, Broadcast: 1.1.1.255
    Protocol multiservice, MTU: Unlimited
      Flags: Is-Primary
```

Meaning The status **et-1/0/0, Enabled, Physical link is Up** indicates that interface et-1/0/0 is working.

The status **Input packets : 108** indicates that the interface is receiving packets.

Verifying That the Packets Are Matched and Filtered According to the Configuration

Purpose Verify that the packets are matched and filtered according to the configuration.

Action In operational mode, enter the **show firewall** command.

```
user@ptx5000> show firewall
Filter: ipv4_sample_filter
Counters:
Name                                                Bytes              Packets
c1                                                  11880                  108

Filter: ipv6_sample_filter
Counters:
Name                                                Bytes              Packets
c1                                                  11980                  192

Filter: mpls_sample_filter
Counters:
Name                                                Bytes              Packets
c1                                                  12880                  208
```

Meaning The **Bytes** field displays the number of bytes that match the filter term under which the counter action is specified.

The **Packets** field displays the number of packets that match the filter term under which the counter action is specified.

The results indicate that the packets are matched and filtered according to the configuration.

Verifying That the ATS Interface Is Forwarding Packets

Purpose Verify that the ats0 interface is forwarding packets.

Action In operational mode, enter the **show interfaces ats0** command.

```
user@ptx5000> show interfaces ats0
Physical interface: ats0, Enabled, Physical link is Up
  Interface index: 129, SNMP ifIndex: 574
  Type: Ethernet, Link-level type: Ethernet, MTU: 9536, Speed: 10Gbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link type      : Full-Duplex
  Link flags     : None
  Current address: f8:c0:01:3a:e4:8d, Hardware address: f8:c0:01:3a:e4:8d
  Last flapped   : 2012-12-18 21:35:22 PST (00:03:19 ago)
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)
  Logical interface ats0.0 (Index 72) (SNMP ifIndex 600)
    Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: Tether-Enet-Svcs
    Statistics        Packets        pps         Bytes          bps
    Bundle:
        Input :           108          0         13392            0
        Output:           108          0         13392            0
    Protocol inet, MTU: 9536
      Flags: Sendbcast-pkt-to-re
    Protocol inet6, MTU: 9536
      Flags: Is-Primary
    Protocol mpls, MTU: 9536, Maximum labels: 3
      Flags: Is-Primary
```

Meaning The **Packets** and **Bytes** fields under the **Bundle** statistics show that the ats0 interface is forwarding the packets (**Output** field) to the CSE2000.

Verifying That Active Flow Monitoring Is Working

Purpose Verify that active flow monitoring is working.

Action To verify that active flow monitoring is working, use the **show services accounting flow** command.

```
user@ptx5000> show services accounting flow
  Flow information
    Service Accounting interface: ats0, Local interface index: 149
    Flow packets: 87168293, Flow bytes: 5578770752
    Flow packets 10-second rate: 45762, Flow bytes 10-second rate: 2928962
    Active flows: 1000, Total flows: 2000
    Flows exported: 19960, Flows packets exported: 582
    Flows inactive timed out: 1000, Flows active timed out: 29000
```

Meaning The output shows that active flows exist and that flow packets are being exported. This indicates that flow monitoring is working. If flow monitoring is not working, verify that the CSE2000 is operational.

Verifying That the CSE2000 Service Card Is Operational for Active Flow Monitoring

Purpose Verify that the CSE2000 service card configured for active flow monitoring is present in the chassis and is operational.

Action To verify that the CSE2000 service card configured is operational, use the **show chassis hardware** command.

```
user@ptx5000> show chassis hardware
Item             Version  Part number  Serial number     Description
Chassis                                JN11FF811AJA      PTX5000
Midplane         REV 11   750-035893   ACAW6233          Midplane-8S
FPM              REV 12   760-030647   BBAX0093          Front Panel Display
PDU 0            Rev 07   740-032019   1E002220031       DC Power Dist Unit
  PSM 0          Rev 06   740-032022   1E002280079       DC 12V Power Supply
  PSM 1          Rev 06   740-032022   1E002280070       DC 12V Power Supply
  PSM 2          Rev 06   740-032022   1E002280080       DC 12V Power Supply
  PSM 3          Rev 06   740-032022   1E002280069       DC 12V Power Supply
PDU 1            Rev 07   740-032019   1E002220052       DC Power Dist Unit
  PSM 0          Rev 06   740-032022   1E002280040       DC 12V Power Supply
  PSM 2          Rev 06   740-032022   1E002280071       DC 12V Power Supply
Routing Engine 0 REV 10   740-026942   P737A-003458      RE-DUO-2600
Routing Engine 1 REV 10   740-026942   P737A-003388      RE-DUO-2600
CB 0             REV 16   750-030625   BBAW8988          Control Board
  Xcvr 0         REV 01   740-031980   1Y3363A02396      SFP+-10G-SR
  Xcvr 2         REV 02   740-013111   A430887           SFP-T
  Xcvr 3         REV 01   740-038291   C489070           SFP-T
CB 1             REV 16   750-030625   BBAV3847          Control Board
  Xcvr 0         REV 01   740-031980   1Y3363A02054      SFP+-10G-SR
  Xcvr 2         REV 01   740-013111   60901034          SFP-T
  Xcvr 3         REV 01   740-038291   C489072           SFP-T
FPC 0            REV 22   750-036844   BBAV9151          FPC
  CPU            REV 13   711-030686   BBAW8899          SNG PMB
  PIC 0          REV 21   750-031913   BBAX1097          24x 10GE(LAN) SFP+
    Xcvr 10      REV 01   740-031980   ANF08QE           SFP+-10G-SR
    Xcvr 11      REV 01   740-031980   AMB0WKG           SFP+-10G-SR
    Xcvr 12      REV 01   740-031980   B11J04031         SFP+-10G-SR
    Xcvr 13      REV 01   740-031980   AMB0TD9           SFP+-10G-SR
  PIC 1          REV 21   750-031913   BBAW4241          24x 10GE(LAN) SFP+
FPC 3            REV 03   711-035673   EF4357            Vaudville FPC P1
  CPU            REV 06   711-030686   EF3468            SNG PMB
  PIC 0          REV 21   750-031913   BBBA1821          24x 10GE(LAN) SFP+
    Xcvr 10      REV 01   740-031980   1Y3363A02069      SFP+-10G-SR
    Xcvr 11      REV 01   740-031980   063363A00044      SFP+-10G-SR
  PIC 1          REV 18   750-031916   BBBA2677          2x 100GE CFP
ESC 0            REV 00   650-049328   CJ2313AL0050      CSE2000-32G-S
  Backplane      REV 00   650-049327   CH2313AL0050      CSE2000 Chassis
SPMB 0           REV 13   711-030686   BBAW9018          SNG PMB
SPMB 1           REV 13   711-030686   BBAW2165          SNG PMB
SIB 0            REV 12   750-030631   BBAW9889          SIB-I-8S
SIB 1            REV 12   750-030631   BBAW4352          SIB-I-8S
SIB 2            REV 12   750-030631   BBAW4363          SIB-I-8S
SIB 3            REV 12   750-030631   BBAW9919          SIB-I-8S
SIB 4            REV 12   750-030631   BBAW4404          SIB-I-8S
SIB 5            REV 12   750-030631   BBAX0348          SIB-I-8S
SIB 6            REV 12   750-030631   BBAW9861          SIB-I-8S
SIB 7            REV 12   750-030631   BBAW9852          SIB-I-8S
SIB 8            REV 12   750-030631   BBAW4308          SIB-I-8S
Fan Tray 0       REV 10   760-032784   BBAW8152          Vertical Fan Tray
Fan Tray 1       REV 13   760-030642   BBAV8820          Horizontal Fan Tray
Fan Tray 2       REV 13   760-030642   BBAV3612          Horizontal Fan Tray
```

Meaning The output **ESC 0** shows that CSE2000 service card has completed booting and is operational. If the service card is operational but flow monitoring is not working, verify

that sampling is enabled on the media interface on which traffic flow is expected and that the sampling filter direction is correct.

Verifying That Sampling Is Enabled and the Filter Direction Is Correct for Active Flow Monitoring

Purpose Verify that sampling is enabled on the media interface on which traffic flow is expected and that the sampling filter direction is correct.

Action To verify that sampling is enabled on the media interface on which traffic flow is expected and that the sampling filter direction is correct, use the **show interfaces *interface-name* extensive | grep filters** command.

```
user@ptx5000> show interfaces et-1/0/0 extensive | grep filters
    CAM destination filters: 3, CAM source filters: 0
      Input Filters: ipv4_sample_filter
      Input Filters: ipv6_sample_filter
      Input Filters: mpls_sample_filter
```

Meaning The command output shows that the sample filter is applied to the media interface on which traffic flow is expected (**et-1/0/0**) and that the sampling filter direction is **Input**. If the CSE2000 service card is operational and the filters are correct, but flow monitoring is not working, verify that the sampling instance is applied to the FPC where the media interface resides.

TIP: If a firewall filter is used to enable sampling, add a counter as an action in the firewall filter. Then, check whether the counter is incrementing. An incrementing counter confirms that the traffic is present and that the filter direction is correct.

Verifying That the Sampling Instance Is Applied to the Correct FPC for Active Flow Monitoring

Purpose Verify that the sampling instance is applied to the FPC where the media interface resides.

Action To verify that the sampling instance is applied to the correct FPC, use the **show configuration chassis** command.

```
user@ptx5000> show configuration chassis

fpc 1 {
  sampling-instance ins1;
}
```

Meaning The output shows that the sampling instance is applied to the correct FPC. If the CSE2000 service card is operational, the filters are correct, and the sampling instance is applied to the correct FPC, but flow monitoring is not working, verify that the route record set of data is being created.

Verifying That the Route Record Is Being Created for Active Flow Monitoring

Purpose Verify that the route record set of data is being created.

Action To verify that the route record set of data is being created, use the **show services accounting status** command.

```
user@ptx5000> show services accounting status
Service Accounting interface: ats0
  Export format: 9, Route record count: 40
  IFL to SNMP index count: 11, AS count: 1
  Configuration set: Yes, Route record set: Yes, IFL SNMP map set: Yes
```

Meaning The output shows that the **Route record set** field is set to **Yes**. This confirms that the route record set is created.

TIP: If the route record set field is set to no, the record might not have been downloaded yet. Wait for 60–100 seconds and check again. If the route record is still not created, verify that the sampling process is running, that the connection between the CSE2000 service card and the process is operational, and that the CSE2000 service card memory is not overloaded.

Verifying That the Sampling Process Is Running for Active Flow Monitoring

Purpose Verify that the sampling process is running.

Action To verify that the sampling process is running, use the **show system processes extensive | grep sampled** command.

```
user@ptx5000> show system processes extensive | grep sampled
PID USERNAME  THR PRI NICE   SIZE    RES   STATE    TIME   WCPU   COMMAND
1581 root     1   1   111    5660K  5108K select   0:00  0.00%   sampled
```

Meaning The output shows that **sampled** is listed as a running system process. In addition to verifying that the process is running, verify that the TCP connection between the sampled process and the CSE2000 service card is operational.

Verifying That the TCP Connection Is Operational for Active Flow Monitoring

Purpose Verify that the TCP connection between the sampled process and the CSE2000 service card is operational.

Action To verify that the TCP connection is operational, use the **show system connections inet | grep 6153** command.

```
user@ptx5000> show system connections inet | grep 6153
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
~
```

```
~
~
tcp        0      0  128.0.0.1.6153       128.0.2.17.11265    ESTABLISHED
tcp4       0      0  *.6153                 *.*                   LISTEN
```

Meaning The output shows that the TCP connection between the sampled process socket (**6153**) and the CSE2000 service card (**128.0.0.1**) is **ESTABLISHED**.

TIP: If the TCP connection between the sampled process and the CSE2000 service card is not established, restart the sampled process by using the restart sampling command.

Related Documentation

- Active Flow Monitoring on PTX Series Routers with CSE2000 Overview on page 1
- Example: Configuring Active Flow Monitoring Version 9 on a PTX3000 and PTX5000 When Both Are Tethered to a CSE2000 on page 23

Example: Configuring Active Flow Monitoring Version 9 on a PTX3000 and PTX5000 When Both Are Tethered to a CSE2000

This example shows how to configure active flow monitoring version 9 for simultaneous IPv4, IPv6 and MPLS flows on a PTX5000 router and a PTX3000 router when both are tethered to a CSE2000. The step-by-step instructions in this example will help you to configure traffic sampling on a PTX5000 router and a PTX3000 router, generate the v9 records, and send these records to a specified host.

This example contains the following sections:

Requirements

This example requires the following hardware and software components:

- One PTX5000 router running Junos OS Release 13.3R4 or later
- One PTX3000 router running Junos OS Release 13.3R4 or later
- One CSE2000 running CSE Series Release 13.3R4 or later
- Version 9 flow server (to collect sampled flows using the version 9 format)

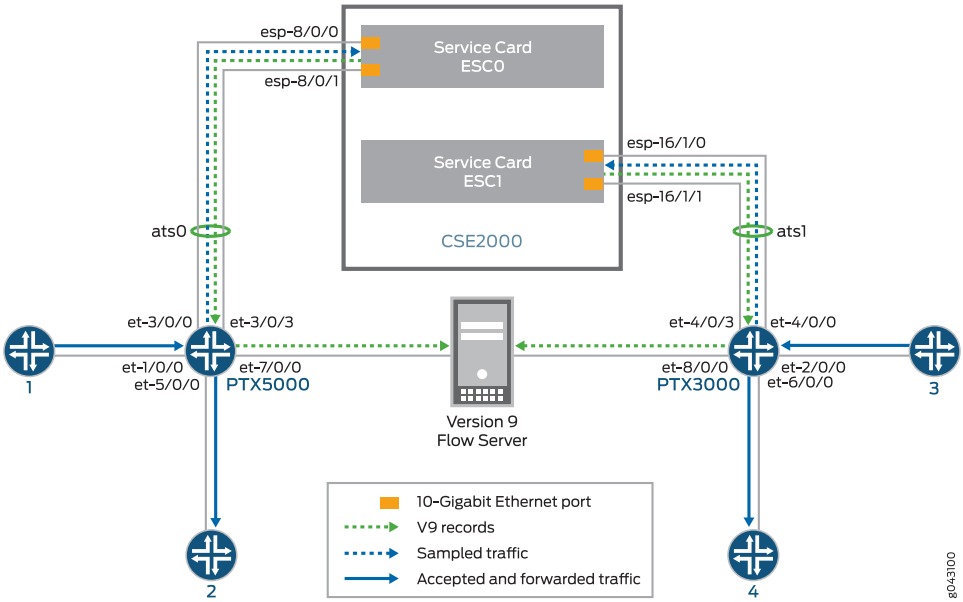
Before you configure active flow monitoring version 9, connect the CSE2000 to the PTX5000 router and the PTX3000 router. For more information, see the *CSE2000 Hardware Installation Guide*.

Overview and Topology

This example shows the configuration of active flow monitoring version 9 for simultaneous IPv4, IPv6, and MPLS flows on a PTX5000 router and a PTX3000 router when both are tethered to a CSE2000. All the configurations shown in this example are performed on the PTX5000 and PTX3000 routers.

The topology for this example consists of a PTX5000 router and a PTX3000 router on which active flow monitoring version 9 needs to be enabled (see Figure 3 on page 24). These routers are tethered to a CSE2000 device.

Figure 3: Active Flow Monitoring Version 9 on PTX3000 and PTX5000 Connected to CSE2000



Interface et-1/0/0 is the ingress interface through which packets enter the PTX5000 router. Traffic sampling is performed on interface et-1/0/0. The PTX5000 router forwards the traffic to the egress interface et-5/0/0, and the sampled traffic to the 10-Gigabit Ethernet interfaces et-3/0/0 and et-3/0/3. The sampled packets are transmitted through the ATS interface of the CSE2000.

Interface et-2/0/0 is the ingress interface through which packets enter the PTX3000 router. Traffic sampling is performed on interface et-2/0/0. The PTX3000 router forwards the traffic to the egress interface et-6/0/0, and the sampled traffic to the 10-Gigabit Ethernet interfaces et-4/0/0 and et-4/0/3. The sampled packets are transmitted through the ATS interface of the CSE2000.

In this example, service card ESC0 of the CSE2000 is connected to the PTX5000 router. The service card ESC0 has two 10-Gigabit Ethernet interfaces (esp-8/0/0 and esp-8/0/1), which are used to connect to the 10-Gigabit Ethernet PICs on the PTX5000 for the sampled traffic. The CSE2000 performs active flow monitoring on the sampled traffic and exports the version 9 records through esp interfaces (esp-8/0/0 or esp-8/0/1) to the PTX5000 router. The PTX5000 router forwards the v9 records to the version 9 flow server.

In this example, service card ESC1 of the CSE2000 is connected to the PTX3000 router. The service card ESC1 has two 10-Gigabit Ethernet interfaces (esp-16/1/0 and esp-16/1/1), which are used to connect to the 10-Gigabit Ethernet PICs on the PTX3000 for the sampled traffic. The CSE2000 performs active flow monitoring on the sampled traffic and exports the version 9 records through ESP interfaces (esp-16/1/0 or esp-16/1/1) to the PTX3000 router. The PTX3000 router forwards the v9 records to the version 9 flow server.

In this example, ats0 is the ATS interface that connects the PTX5000 router and the CSE2000. The interfaces et-3/0/3 and et-3/0/0 need to be configured as the member interfaces of the ats0 interface.

The ATS interface ats1 connects the PTX3000 router and the CSE2000. The interfaces et-4/0/3 and et-4/0/0 need to be configured as the member interfaces of the ats1 interface.

The physical connections used in this example are shown in Figure 3 on page 24.

Configuring Active Flow Monitoring Version 9 on a PTX5000 Router

To configure active flow monitoring version 9 for IPv4, IPv6, and MPLS flows on the PTX5000 router tethered to the CSE2000, perform these tasks:

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces et-3/0/0 gigether-options 802.3ad ats0
set interfaces et-3/0/3 gigether-options 802.3ad ats0
set interfaces ats0 unit 0 family inet
set interfaces ats0 unit 0 family inet6
set interfaces ats0 unit 0 family mpls
```

```
set services flow-monitoring version9 template v4-template
set services flow-monitoring version9 template v6-template
set services flow-monitoring version9 template mpls
set services flow-monitoring version9 template v4-template flow-active-timeout 60
set services flow-monitoring version9 template v4-template flow-inactive-timeout 30
set services flow-monitoring version9 template v4-template template-refresh-rate
  packets 480
set services flow-monitoring version9 template v4-template option-refresh-rate packets
  480
set services flow-monitoring version9 template v6-template flow-active-timeout 60
set services flow-monitoring version9 template v6-template flow-inactive-timeout 30
set services flow-monitoring version9 template v6-template template-refresh-rate
  packets 480
set services flow-monitoring version9 template v6-template option-refresh-rate packets
  480
set services flow-monitoring version9 template mpls flow-active-timeout 60
set services flow-monitoring version9 template mpls flow-inactive-timeout 30
set services flow-monitoring version9 template mpls template-refresh-rate packets 480
set services flow-monitoring version9 template mpls option-refresh-rate packets 480
set services flow-monitoring version9 template mpls mpls-template label-position [ 1 2
  ]
set services flow-monitoring version9 template v4-template ipv4-template
set services flow-monitoring version9 template v6-template ipv6-template
set services flow-monitoring version9 template mpls mpls-template
set firewall family inet filter ipv4_sample_filter term 1 then count c1
set firewall family inet filter ipv4_sample_filter term 1 then sample
set firewall family inet filter ipv4_sample_filter term 1 then accept
set firewall family inet6 filter ipv6_sample_filter term 1 then count c1
set firewall family inet6 filter ipv6_sample_filter term 1 then sample
set firewall family inet6 filter ipv6_sample_filter term 1 then accept
set firewall family mpls filter mpls_sample_filter term 1 then count c1
set firewall family mpls filter mpls_sample_filter term 1 then sample
set firewall family mpls filter mpls_sample_filter term 1 then accept
set interfaces et-1/0/0 unit 0 family inet filter input ipv4_sample_filter
set interfaces et-1/0/0 unit 0 family inet6 filter input ipv6_sample_filter
set interfaces et-1/0/0 unit 0 family mpls filter input mpls_sample_filter
set forwarding-options sampling instance ins1 input rate 10
set forwarding-options sampling instance ins1 input run-length 1
set forwarding-options sampling instance ins1 input maximum-packet-length 128
set chassis fpc 1 sampling instance ins1
set forwarding-options sampling instance ins1 family inet output flow-server 192.0.2.2
  port 2055
set forwarding-options sampling instance ins1 family inet6 output flow-server 192.0.2.2
  port 2055
set forwarding-options sampling instance ins1 family mpls output flow-server 192.0.2.2
  port 2055
set forwarding-options sampling instance ins1 family inet output flow-server 192.0.2.2
  version9 template v4-template
set forwarding-options sampling instance ins1 family inet6 output flow-server 192.0.2.2
  version9 template v6-template
set forwarding-options sampling instance ins1 family mpls output flow-server 192.0.2.2
  version9 template mpls
set forwarding-options sampling instance ins1 family inet output interface ats0
  source-address 192.0.2.1
set forwarding-options sampling instance ins1 family inet output interface ats0 export-port
  address 192.0.2.1/24
```



```
set forwarding-options sampling instance ins1 family inet6 output interface ats0
  source-address 192.0.2.1
set forwarding-options sampling instance ins1 family inet6 output interface ats0
  export-port address 192.0.2.1/24
set forwarding-options sampling instance ins1 family mpls output interface ats0
  source-address 192.0.2.1
set forwarding-options sampling instance ins1 family mpls output interface ats0
  export-port address 192.0.2.1/24
```

Configuring the Member Interfaces and Interface Family for Aggregated Tethered Services Interfaces

Step-by-Step Procedure

The interfaces et-3/0/0 and et-3/0/3 of the PTX5000 router that connect to the CSE2000 are configured as the member interfaces of the ATS interface ats0. This configuration associates the physical links of the router with the logical bundle of the ATS interface. You must also specify the constituent physical links by including the **802.3ad** statement. All the configurations are performed on the PTX5000 router.

To configure the member interfaces and interface family for the ATS interface bundle ats0:

1. Configure the interfaces et-3/0/0 and et-3/0/3 to form the ATS interface bundle ats0.

   ```
   [edit interfaces]
   user@ptx5000# set et-3/0/0 gigether-options 802.3ad ats0
   user@ptx5000# set et-3/0/3 gigether-options 802.3ad ats0
   ```

2. Configure the ats0 interface to process IPv4, IPv6, and MPLS addresses by including the **family** statement and specifying the **inet**, **inet6**, and **mpls** options, respectively, at the **[edit interfaces]** hierarchy level.

   ```
   [edit interfaces]
   user@ptx5000# set ats0 unit 0 family inet
   user@ptx5000# set ats0 unit 0 family inet6
   user@ptx5000# set ats0 unit 0 family mpls
   ```

Configuring the Active Flow Monitoring Version 9 Template for IPv4, MPLS, and IPv6 Flows

Step-by-Step Procedure

To activate templates in flow monitoring, configure a template and include that template in the version 9 flow monitoring configuration:

1. Configure a version 9 template for IPv4, IPv6, and MPLS flows.

   - Create a version 9 template for IPv4 flows by including the **flow-monitoring version9 template** statement and specifying **v4_template** as the name of the template at the **[edit services]** hierarchy level.

     ```
     [edit services]
     user@ptx5000# set flow-monitoring version9 template v4_template
     ```

   - Create a version 9 template for IPv6 flows by including the **flow-monitoring version9 template** statement and specifying **v6_template** as the name of the template at the **[edit services]** hierarchy level.

     ```
     [edit services]
     user@ptx5000# set flow-monitoring version9 template v6_template
     ```

   - Create a version 9 template for MPLS flows by including the **flow-monitoring version9 template** statement and specifying **mpls** as the name of the template at the **[edit services]** hierarchy level.

     ```
     [edit services]
     user@ptx5000# set flow-monitoring version9 template mpls
     ```

2. Configure the active timeout and the inactive timeout values for the traffic flows by including the **flow-active-timeout** and **flow-inactive-timeout** statements at the **[edit services flow-monitoring version9 template v4_template]**, **[edit services flow-monitoring version9 template v6_template]**, and **[edit services flow-monitoring version9 template mpls]** hierarchy levels.

   - If the interval between the time the last packet was received and the time the flow was last exported exceeds the configured active timeout value, the flow is exported to the flow server.
   - If the interval between the current time and the time that the last packet for this flow was received exceeds the configured inactive timeout value, the flow is allowed to expire.

     In this example, the active timeout value is 60 seconds and the inactive timeout value is 30 seconds.

     ```
     [edit services flow-monitoring version9 template v4_template]
     user@ptx5000# set flow-active-timeout 60
     user@ptx5000# set flow-inactive-timeout 30

     [edit services flow-monitoring version9 template v6_template]
     user@ptx5000# set flow-active-timeout 60
     user@ptx5000# set flow-inactive-timeout 30

     [edit services flow-monitoring version9 template mpls]
     user@ptx5000# set flow-active-timeout 60
     user@ptx5000# set flow-inactive-timeout 30
     ```

3. Enable the templates for IPv4, IPv6, and MPLS flows.

   - Enable the template for IPv4 flows by including the **ipv4-template** statement at the **[edit services flow-monitoring version9 template v4_template]** hierarchy level.

     ```
     [edit services flow-monitoring version9 template v4_template]
     user@ptx5000# set ipv4-template
     ```

   - Enable the template for IPv6 flows by including the **ipv6-template** statement at the **[edit services flow-monitoring version9 template v6_template]** hierarchy level.

     ```
     [edit services flow-monitoring version9 template v6_template]
     user@ptx5000# set ipv6-template
     ```

   - Enable the template for MPLS flows by including the **mpls-template** statement at the **[edit services flow-monitoring version9 template mpls]** hierarchy level. Also include the **label-position** statement and specify label positions 1 and 2 at the **[edit services flow-monitoring version9 template mpls mpls-template]** hierarchy level.

     ```
     [edit services flow-monitoring version9 template mpls]
     user@ptx5000# set mpls-template

     [edit services flow-monitoring version9 template mpls mpls-template]
     user@ptx5000# set label-position [ 1 2 ]
     ```

4. Configure the rate at which the router sends IPv4, IPv6, and MPLS template definitions and options to the flow server for IPv4, IPv6, and MPLS traffic. Because version 9 flow monitoring traffic is unidirectional from the router to the flow server, configure the router to send template definitions and options, such as sampling rate, to the server. In this example, the template definitions and options are refreshed for every 480 packets.

   - Include the **template-refresh-rate** and **option-refresh-rate** statements at the **[edit services flow-monitoring version9 template v4_template]** hierarchy level.

     ```
     [edit services flow-monitoring version9 template v4_template]
     user@ptx5000# set template-refresh-rate packets 480
     user@ptx5000# set option-refresh-rate packets 480
     ```

   - Include the **template-refresh-rate** and **option-refresh-rate** statements at the **[edit services flow-monitoring version9 template v6_template]** hierarchy level.

     ```
     [edit services flow-monitoring version9 template v6_template]
     user@ptx5000# set template-refresh-rate packets 480
     user@ptx5000# set option-refresh-rate packets 480
     ```

   - Include the **template-refresh-rate** and **option-refresh-rate** statements at the **[edit services flow-monitoring version9 template mpls]** hierarchy level.

     ```
     [edit services flow-monitoring version9 template mpls]
     user@ptx5000# set template-refresh-rate packets 480
     user@ptx5000# set option-refresh-rate packets 480
     ```

Configuring the Firewall Filter

Step-by-Step Procedure

The firewall filter identifies the traffic flows that need to be sampled and processed by the CSE2000.

To configure the firewall filter:

1. Configure the firewall filter for IPv4, IPv6, and MPLS traffic.

   - To configure the firewall filter for IPv4, include the **filter** statement and specify ipv4_sample_filter as the name of the filter at the **[edit firewall family inet]** hierarchy level. Include the **term** statement and specify 1 as the name of the term. For active monitoring using version 9, you must include the **sample** and **accept** action statements at the **[edit firewall family inet]** hierarchy level.

     ```
     [edit firewall family inet]
     user@ptx5000# set filter ipv4_sample_filter term 1 then count c1
     user@ptx5000# set filter ipv4_sample_filter term 1 then sample
     user@ptx5000# set filter ipv4_sample_filter term 1 then accept
     ```

   - To configure the firewall filter for IPv6, include the **filter** statement and specify ipv6_sample_filter as the name of the filter at the **[edit firewall family inet6]** hierarchy level. Include the **term** statement and specify 1 as the name of the term. For active monitoring using version 9, you must include the **sample** and **accept** action statements at the **[edit firewall family inet6]** hierarchy level.

     ```
     [edit firewall family inet6]
     user@ptx5000# set filter ipv6_sample_filter term 1 then count c1
     user@ptx5000# set filter ipv6_sample_filter term 1 then sample
     user@ptx5000# set filter ipv6_sample_filter term 1 then accept
     ```

   - To configure the firewall filter for MPLS, include the **filter** statement and specify mpls_sample_filter as the name of the filter at the **[edit firewall family mpls]** hierarchy level. Include the **term** statement and specify 1 as the name of the term. For active monitoring using version 9, you must include the **sample** and **accept** action statements at the **[edit firewall family mpls]** hierarchy level.

     ```
     [edit firewall family mpls]
     user@ptx5000# set filter mpls_sample_filter term 1 then count c1
     user@ptx5000# set filter mpls_sample_filter term 1 then sample
     user@ptx5000# set filter mpls_sample_filter term 1 then accept
     ```

2. Apply the firewall filter to the interface where traffic flow needs to be sampled.

   The filter can be applied to either ingress or egress traffic depending on the use case. In this example, the filter is applied to the ingress (input) traffic.

   - To apply the firewall filter to the et-1/0/0 interface for IPv4, include the **input** statement and specify ipv4_sample_filter as the name of the filter at the **[edit interfaces et-1/0/0 unit 0 family inet filter]** hierarchy level.

     ```
     [edit interfaces et-1/0/0 unit 0 family inet filter ]
     user@ptx5000# set input ipv4_sample_filter
     ```

- To apply the firewall filter to the et-1/0/0 interface for IPv6, include the **input** statement and specify ipv6_sample_filter as the name of the filter at the **[edit interfaces et-1/0/0 unit 0 family inet6 filter]** hierarchy level.

  ```
  [edit interfaces et-1/0/0 unit 0 family inet6 filter]
  user@ptx5000# set input ipv6_sample_filter
  ```

- To apply the firewall filter to the et-1/0/0 interface for MPLS, include the **input** statement and specify mpls_sample_filter as the name of the filter at the **[edit interfaces et-1/0/0 unit 0 family mpls filter]** hierarchy level.

  ```
  [edit interfaces et-1/0/0 unit 0 family mpls filter]
  user@ptx5000# set input mpls_sample_filter
  ```

Configuring Traffic Sampling

Step-by-Step Procedure

Traffic sampling enables you to copy traffic to the CSE2000, which performs flow accounting while the router forwards the packet to its original destination. You can configure traffic sampling by defining a sampling instance that specifies a name for the sampling parameters and binding the instance name to a particular FPC.

To configure traffic sampling:

1. Configure the sampling instance ins1 with sampling rate 10, run length 1, and the maximum packet length of 128 bytes.

   ```
   [edit forwarding-options]
   user@ptx5000# set sampling instance ins1 input rate 10
   user@ptx5000# set sampling instance ins1 input run-length 1
   user@ptx5000# set sampling instance ins1 input maximum-packet-length 128
   ```

2. Apply the sampling instance to an FPC on the PTX5000 router by including the **sampling-instance** statement at the **[edit chassis]** hierarchy level.

   The FPC number must match the FPC portion of the interface name for the interface on which sampling is enabled. In this example, FPC 1 is associated with the interface et-1/0/0 on which sampling is enabled.

   ```
   [edit chassis]
   user@ptx5000# set fpc 1 sampling instance ins1
   ```

Configuring the Flow Server to Collect the Active Flow Monitoring Version 9 Records

Step-by-Step Procedure

To configure the flow server:

1. Configure the flow server for IPv4, IPv6, and MPLS flows.

   - To configure the flow server for IPv4, include the **flow-server** statement and specify 192.0.2.2 as the IPv4 address of the host system that is collecting traffic flows at the **[edit forwarding-options sampling instance ins1 family inet output]** hierarchy level. Also include the **port** statement and specify UDP port 2055 for use by the flow server.

     ```
     [edit forwarding-options sampling instance ins1 family inet output]
     user@ptx5000# set flow-server 192.0.2.2 port 2055
     ```

   - To configure the flow server for IPv6, include the **flow-server** statement and specify 192.0.2.2 as the IPv4 address of the host system that is collecting traffic flows at the **[edit forwarding-options sampling instance ins1 family inet6 output]** hierarchy level. Also include the **port** statement and specify UDP port 2055 for use by the flow server.

     ```
     [edit forwarding-options sampling instance ins1 family inet6 output]
     user@ptx5000# set flow-server 192.0.2.2 port 2055
     ```

   - To configure the flow server for MPLS, include the **flow-server** statement and specify 192.0.2.2 as the IPv4 address of the host system that is collecting traffic flows at the **[edit forwarding-options sampling instance ins1 family mpls output]** hierarchy level. Also include the **port** statement and specify UDP port 2055 for use by the flow server.

     ```
     [edit forwarding-options sampling instance ins1 family mpls output]
     user@ptx5000# set flow-server 192.0.2.2 port 2055
     ```

2. Enable active flow monitoring by using the version 9 template format.

   - To enable active flow monitoring for IPv4 flows by using the version 9 template format, include the **version9 template** statement and specify v4_template as the name of the template to use at the **[edit forwarding-options sampling instance ins1 family inet output flow-server 192.0.2.2]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family inet output flow-server
       192.0.2.2]
     user@ptx5000# set version9 template v4_template
     ```

   - To enable active flow monitoring for IPv6 flows by using the version 9 template format, include the **version9 template** statement and specify v6_template as the name of the template to use at the **[edit forwarding-options sampling instance ins1 family inet6 output flow-server 192.0.2.2]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family inet6 output flow-server
       192.0.2.2 ]
     user@ptx5000# set version9 template v6_template
     ```

   - To enable active flow monitoring for MPLS flows by using the version 9 template format, include the **version9 template** statement and specify mpls as the name

of the template to use at the **[edit forwarding-options sampling instance ins1 family mpls output flow-server 192.0.2.2]** hierarchy level.

```
[edit forwarding-options sampling instance ins1 family mpls output flow-server
  192.0.2.2]
user@ptx5000# set version9 template mpls
```

3. Configure the interface connected to the flow server by specifying the source address for generating the monitored packets.

   - For IPv4 flows, configure the interface connected to the flow server by specifying 192.0.2.1 as the source address for generating the monitored packets at the **[edit forwarding-options sampling instance ins1 family inet output]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family inet output]
     user@ptx5000# set interfaces ats0 source-address 192.0.2.1
     ```

   - For IPv6 flows, configure the interface connected to the flow server by specifying 192.0.2.1 as the source address for generating the monitored packets at the **[edit forwarding-options sampling instance ins1 family inet6 output]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family inet6 output]
     user@ptx5000# set interfaces ats0 source-address 192.0.2.1
     ```

   - For MPLS flows, configure the interface connected to the flow server by specifying 192.0.2.1 as the source address for generating the monitored packets at the **[edit forwarding-options sampling instance ins1 family mpls output]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family mpls output]
     user@ptx5000# set interfaces ats0 source-address 192.0.2.1
     ```

4. Configure the address of the export port that is used by the v9 records to reach the flow server.

   - For IPv4 flows, configure the export port address 192.0.2.1/24 at the **[edit forwarding-options sampling instance ins1 family inet output]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family inet output]
     user@ptx5000# set interface ats0 export-port address 192.0.2.1/24
     ```

   - For IPv6 flows, configure the export port address 192.0.2.1/24 at the **[edit forwarding-options sampling instance ins1 family inet6 output]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family inet6 output]
     user@ptx5000# set interface ats0 export-port address 192.0.2.1/24
     ```

   - For MPLS flows, configure the export port address 192.0.2.1/24 at the **[edit forwarding-options sampling instance ins1 family mpls output]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family mpls output]
     user@ptx5000# set interface ats0 export-port address 192.0.2.1/24
     ```

Results

Display the results of the configuration.

```
user@ptx5000> show configuration
  chassis {
    fpc 1 {
```

```
      sampling-instance ins1;
    }
  }
  services {
    flow-monitoring {
      version9 {
        template v4_template {
          flow-active-timeout 60;
          flow-inactive-timeout 30;
          template-refresh-rate {
            packets 480;
          }
          option-refresh-rate {
            packets 480;
          }
          ipv4-template;
        }
        template v6_template {
          flow-active-timeout 60;
          flow-inactive-timeout 30;
          template-refresh-rate {
            packets 480;
          }
          option-refresh-rate {
            packets 480;
          }
          ipv6-template;
        }
        template mpls {
          flow-active-timeout 60;
          flow-inactive-timeout 30;
          template-refresh-rate {
            packets 480;
          }
          option-refresh-rate {
            packets 480;
          }
          mpls-template {
            label-position [ 1 2];
          }
        }
      }
    }
  }
  interfaces {
    et-1/0/0 {
      unit 0 {
        family inet {
          filter {
            input ipv4_sample_filter;
          }
        }
        family inet6 {
          filter {
            input ipv6_sample_filter;
          }
```

```
        }
        family mpls {
          filter {
            input mpls_sample_filter;
          }
        }
      }
    }
    et-3/0/0 {
      gigether-options {
        802.3ad ats0;
      }
    }
    et-3/0/3 {
      gigether-options {
        802.3ad ats0;
      }
    }
    ats0 {
      unit 0 {
        family inet;
        family inet6;
        family mpls;
      }
    }
}
forwarding-options {
    sampling {
      instance {
        ins1 {
          input {
            rate 10;
            run-length 1;
            maximum-packet-length 128;
          }
          family inet {
            output {
              flow-server 192.0.2.2 {
                port 2055;
                version9 {
                  template {
                    v4_template;
                  }
                }
              }
              interface ats0 {
                source-address 192.0.2.1;
                export-port {
                  address 192.0.2.1/24;
                }
              }
            }
          }
          family inet6 {
            output {
              flow-server 192.0.2.2 {
```

```
                port 2055;
                version9 {
                  template {
                    v6_template;
                  }
                }
              }
              interface ats0 {
                source-address 192.0.2.1;
                export-port {
                  address 192.0.2.1/24;
                }
              }
            }
          }
          family mpls{
            output {
              flow-server 192.0.2.2 {
                port 2055;
                version9 {
                  template {
                    mpls;
                  }
                }
              }
              interface ats0 {
                source-address 192.0.2.1;
                export-port {
                  address 192.0.2.1/24;
                }
              }
            }
          }
        }
      }
    }
    firewall {
      family inet {
        filter ipv4_sample_filter {
          term 1 {
            then {
              count c1;
              sample;
              accept;
            }
          }
        }
      }
      family inet6 {
        filter ipv6_sample_filter {
          term 1 {
            then {
              count c1;
              sample;
              accept;
```

```
            }
          }
        }
      }
      family mpls {
        filter mpls_sample_filter {
          term 1 {
            then {
              count c1;
              sample;
              accept;
            }
          }
        }
      }
    }
```

Configuring Active Flow Monitoring Version 9 on a PTX3000 Router

To configure active flow monitoring version 9 for IPv4, IPv6, and MPLS flows on the PTX3000 router tethered to the CSE2000, perform these tasks:

- Configuring the Member Interfaces and Interface Family for Aggregated Tethered Services Interfaces on page 39
- Configuring the Active Flow Monitoring Version 9 Template for IPv4, IPv6, and MPLS Flows on page 40
- Configuring the Firewall Filter on page 42
- Configuring Traffic Sampling on page 43
- Configuring the Flow Server to Collect the Active Flow Monitoring Version 9 Records on page 44
- Results on page 45

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces et-4/0/0 gigether-options 802.3ad ats1
set interfaces et-4/0/3 gigether-options 802.3ad ats1
set interfaces ats1 unit 0 family inet
set interfaces ats1 unit 0 family inet6
set interfaces ats1 unit 0 family mpls
set services flow-monitoring version9 template v4-template
set services flow-monitoring version9 template v6-template
set services flow-monitoring version9 template mpls
set services flow-monitoring version9 template v4-template flow-active-timeout 60
set services flow-monitoring version9 template v4-template flow-inactive-timeout 30
set services flow-monitoring version9 template v4-template template-refresh-rate
  packets 480
set services flow-monitoring version9 template v4-template option-refresh-rate packets
  480
set services flow-monitoring version9 template v6-template flow-active-timeout 60
```

```
set services flow-monitoring version9 template v6-template flow-inactive-timeout 30
set services flow-monitoring version9 template v6-template template-refresh-rate
  packets 480
set services flow-monitoring version9 template v6-template option-refresh-rate packets
  480
set services flow-monitoring version9 template mpls flow-active-timeout 60
set services flow-monitoring version9 template mpls flow-inactive-timeout 30
set services flow-monitoring version9 template mpls template-refresh-rate packets 480
set services flow-monitoring version9 template mpls option-refresh-rate packets 480
set services flow-monitoring version9 template v4-template ipv4-template
set services flow-monitoring version9 template v6-template ipv6-template
set services flow-monitoring version9 template mpls mpls-template
set services flow-monitoring version9 template mpls mpls-template label-position [ 1 2
  ]
set firewall family inet filter ipv4_sample_filter term 1 then count c1
set firewall family inet filter ipv4_sample_filter term 1 then sample
set firewall family inet filter ipv4_sample_filter term 1 then accept
set firewall family inet6 filter ipv6_sample_filter term 1 then count c1
set firewall family inet6 filter ipv6_sample_filter term 1 then sample
set firewall family inet6 filter ipv6_sample_filter term 1 then accept
set firewall family mpls filter mpls_sample_filter term 1 then count c1
set firewall family mpls filter mpls_sample_filter term 1 then sample
set firewall family mpls filter mpls_sample_filter term 1 then accept
set interfaces et-2/0/0 unit 0 family inet filter input ipv4_sample_filter
set interfaces et-2/0/0 unit 0 family inet6 filter input ipv6_sample_filter
set interfaces et-2/0/0 unit 0 family mpls filter input mpls_sample_filter
set forwarding-options sampling instance ins1 input rate 10
set forwarding-options sampling instance ins1 input run-length 1
set forwarding-options sampling instance ins1 input maximum-packet-length 128
set chassis fpc 1 sampling instance ins1
set forwarding-options sampling instance ins1 family inet output flow-server 192.0.2.2
  port 2055
set forwarding-options sampling instance ins1 family inet6 output flow-server 192.0.2.2
  port 2055
set forwarding-options sampling instance ins1 family mpls output flow-server 192.0.2.2
  port 2055
set forwarding-options sampling instance ins1 family inet output flow-server 192.0.2.2
  version9 template v4-template
set forwarding-options sampling instance ins1 family inet6 output flow-server 192.0.2.2
  version9 template v6-template
set forwarding-options sampling instance ins1 family mpls output flow-server 192.0.2.2
  version9 template mpls
set forwarding-options sampling instance ins1 family inet output interface ats1
  source-address 192.0.2.1
set forwarding-options sampling instance ins1 family inet output interface ats1 export-port
  address 192.0.2.1/24
set forwarding-options sampling instance ins1 family inet6 output interface ats1
  source-address 192.0.2.1
set forwarding-options sampling instance ins1 family inet6 output interface ats1
  export-port address 192.0.2.1/24
set forwarding-options sampling instance ins1 family mpls output interface ats1
  source-address 192.0.2.1
set forwarding-options sampling instance ins1 family mpls output interface ats1 export-port
  address 192.0.2.1/24
```


Configuring the Member Interfaces and Interface Family for Aggregated Tethered Services Interfaces

Step-by-Step Procedure

The interfaces et-4/0/0 and et-4/0/3 of the PTX3000 router that connect to the CSE2000 are configured as the member interfaces of the ATS interface ats1. This configuration associates the physical links of the router with the logical bundle of the ATS interface. You must also specify the constituent physical links by including the **802.3ad** statement. All the configurations are performed on the PTX3000 router.

To configure the member interfaces and interface family for the ATS interface bundle ats1:

1. Configure the interfaces et-4/0/0 and et-4/0/3 to form the ATS interface bundle ats1.

   ```
   [edit interfaces]
   user@ptx3000# set et-4/0/0 gigether-options 802.3ad ats1
   user@ptx3000# set et-4/0/3 gigether-options 802.3ad ats1
   ```

2. Configure the ats1 interface to process IPv4, IPv6, and MPLS addresses by including the **family** statement and specifying the **inet**, **inet6**, and **mpls** options, respectively, at the **[edit interfaces]** hierarchy level.

   ```
   [edit interfaces]
   user@ptx3000# set ats1 unit 0 family inet
   user@ptx3000# set ats1 unit 0 family inet6
   user@ptx3000# set ats1 unit 0 family mpls
   ```

Configuring the Active Flow Monitoring Version 9 Template for IPv4, IPv6, and MPLS Flows

Step-by-Step Procedure

To activate templates in flow monitoring, configure a template and include that template in the version 9 flow monitoring configuration:

1. Configure a version 9 template for IPv4, IPv6, and MPLS flows.

   - Create a version 9 template for IPv4 flows by including the **flow-monitoring version9 template** statement and specifying **v4_template** as the name of the template at the **[edit services]** hierarchy level.

     ```
     [edit services]
     user@ptx3000# set flow-monitoring version9 template v4_template
     ```

   - Create a version 9 template for IPv6 flows by including the **flow-monitoring version9 template** statement and specifying **v6_template** as the name of the template at the **[edit services]** hierarchy level.

     ```
     [edit services]
     user@ptx3000# set flow-monitoring version9 template v6_template
     ```

   - Create a version 9 template for MPLS flows by including the **flow-monitoring version9 template** statement and specifying **mpls** as the name of the template at the **[edit services]** hierarchy level.

     ```
     [edit services]
     user@ptx3000# set flow-monitoring version9 template mpls
     ```

2. Configure the active timeout and the inactive timeout values for the traffic flows by including the **flow-active-timeout** and **flow-inactive-timeout** statements at the **[edit services flow-monitoring version9 template v4_template]**, **[edit services flow-monitoring version9 template v6_template]**, and **[edit services flow-monitoring version9 template mpls]** hierarchy levels.

   - If the interval between the time the last packet was received and the time the flow was last exported exceeds the configured active timeout value, the flow is exported to the flow server.
   - If the interval between the current time and the time that the last packet for this flow was received exceeds the configured inactive timeout value, the flow is allowed to expire.

     In this example, the active timeout value is 60 seconds and the inactive timeout value is 30 seconds.

     ```
     [edit services flow-monitoring version9 template v4_template]
     user@ptx3000# set flow-active-timeout 60
     user@ptx3000# set flow-inactive-timeout 30

     [edit services flow-monitoring version9 template v6_template]
     user@ptx3000# set flow-active-timeout 60
     user@ptx3000# set flow-inactive-timeout 30

     [edit services flow-monitoring version9 template mpls]
     user@ptx3000# set flow-active-timeout 60
     user@ptx3000# set flow-inactive-timeout 30
     ```

3. Enable the templates for IPv4, IPv6, and MPLS flows.

   - Enable the template for IPv4 flows by including the **ipv4-template** statement at the **[edit services flow-monitoring version9 template v4_template]** hierarchy level.

     ```
     [edit services flow-monitoring version9 template v4_template]
     user@ptx3000# set ipv4-template
     ```

   - Enable the template for IPv6 flows by including the **ipv6-template** statement at the **[edit services flow-monitoring version9 template v6_template]** hierarchy level.

     ```
     [edit services flow-monitoring version9 template v6_template]
     user@ptx3000# set ipv6-template
     ```

   - Enable the template for MPLS flows by including the **mpls-template** statement at the **[edit services flow-monitoring version9 template mpls]** hierarchy level. Also include the **label-position** statement and specify label positions 1 and 2 at the **[edit services flow-monitoring version9 template mpls mpls-template]** hierarchy level.

     ```
     [edit services flow-monitoring version9 template mpls]
     user@ptx3000# set mpls-template

     [edit services flow-monitoring version9 template mpls mpls-template]
     user@ptx3000# set label-position [ 1 2 ]
     ```

4. Configure the rate at which the router sends IPv4, IPv6, and MPLS template definitions and options to the flow server for IPv4, IPv6, and MPLS traffic. Because version 9 flow monitoring traffic is unidirectional from the router to the flow server, configure the router to send template definitions and options, such as sampling rate, to the server. In this example, the template definitions and options are refreshed for every 480 packets.

   - For IPv4 flows, include the **template-refresh-rate** and **option-refresh-rate** statements at the **[edit services flow-monitoring version9 template v4_template]** hierarchy level.

     ```
     [edit services flow-monitoring version9 template v4_template]
     user@ptx3000# set template-refresh-rate packets 480
     user@ptx3000# set option-refresh-rate packets 480
     ```

   - For IPv6 flows, include the **template-refresh-rate** and **option-refresh-rate** statements at the **[edit services flow-monitoring version9 template v6_template]** hierarchy level.

     ```
     [edit services flow-monitoring version9 template v6_template]
     user@ptx3000# set template-refresh-rate packets 480
     user@ptx3000# set option-refresh-rate packets 480
     ```

   - For MPLS flows, include the **template-refresh-rate** and **option-refresh-rate** statements at the **[edit services flow-monitoring version9 template mpls]** hierarchy level.

     ```
     [edit services flow-monitoring version9 template mpls]
     user@ptx3000# set template-refresh-rate packets 480
     user@ptx3000# set option-refresh-rate packets 480
     ```

Configuring the Firewall Filter

Step-by-Step Procedure

The firewall filter identifies the traffic flows that need to be sampled and processed by the CSE2000.

To configure the firewall filter:

1. Configure the firewall filter.

   - To configure the firewall filter for IPv4, include the **filter** statement and specify ipv4_sample_filter as the name of the filter at the **[edit firewall family inet]** hierarchy level. Include the **term** statement and specify 1 as the name of the term. For active monitoring using version 9, you must include the **sample** and **accept** action statements at the **[edit firewall family inet]** hierarchy level.

     ```
     [edit firewall family inet]
     user@ptx3000# set filter ipv4_sample_filter term 1 then count c1
     user@ptx3000# set filter ipv4_sample_filter term 1 then sample
     user@ptx3000# set filter ipv4_sample_filter term 1 then accept
     ```

   - To configure the firewall filter for IPv6, include the **filter** statement and specify ipv6_sample_filter as the name of the filter at the **[edit firewall family inet6]** hierarchy level. Include the **term** statement and specify 1 as the name of the term. For active monitoring using version 9, you must include the **sample** and **accept** action statements at the **[edit firewall family inet6]** hierarchy level.

     ```
     [edit firewall family inet6]
     user@ptx3000# set filter ipv6_sample_filter term 1 then count c1
     user@ptx3000# set filter ipv6_sample_filter term 1 then sample
     user@ptx3000# set filter ipv6_sample_filter term 1 then accept
     ```

   - To configure the firewall filter for MPLS, include the **filter** statement and specify mpls_sample_filter as the name of the filter at the **[edit firewall family mpls]** hierarchy level. Include the **term** statement and specify 1 as the name of the term. For active monitoring using version 9, you must include the **sample** and **accept** action statements at the **[edit firewall family mpls]** hierarchy level.

     ```
     [edit firewall family mpls]
     user@ptx3000# set filter mpls_sample_filter term 1 then count c1
     user@ptx3000# set filter mpls_sample_filter term 1 then sample
     user@ptx3000# set filter mpls_sample_filter term 1 then accept
     ```

2. Apply the firewall filter to the interface where traffic flow needs to be sampled.

   The filter can be applied to either ingress or egress traffic depending on the use case. In this example, the filter is applied to the ingress (input) traffic.

   - To apply the firewall filter to the et-2/0/0 interface for IPv4, include the **input** statement and specify ipv4_sample_filter as the name of the filter at the **[edit interfaces et-2/0/0 unit 0 family inet filter]** hierarchy level.

     ```
     [edit interfaces et-2/0/0 unit 0 family inet filter ]
     user@ptx3000# set input ipv4_sample_filter
     ```

- To apply the firewall filter to the et-2/0/0 interface for IPv6, include the **input** statement and specify ipv6_sample_filter as the name of the filter at the **[edit interfaces et-2/0/0 unit 0 family inet6 filter]** hierarchy level.

  ```
  [edit interfaces et-2/0/0 unit 0 family inet6 filter]
  user@ptx3000# set input ipv6_sample_filter
  ```

- To apply the firewall filter to the et-2/0/0 interface for MPLS, include the **input** statement and specify mpls_sample_filter as the name of the filter at the **[edit interfaces et-2/0/0 unit 0 family mpls filter]** hierarchy level.

  ```
  [edit interfaces et-2/0/0 unit 0 family mpls filter]
  user@ptx3000# set input mpls_sample_filter
  ```

Configuring Traffic Sampling

Step-by-Step Procedure

Traffic sampling enables you to copy traffic to the CSE2000, which performs flow accounting while the router forwards the packet to its original destination. You can configure traffic sampling by defining a sampling instance that specifies a name for the sampling parameters and binding the instance name to a particular FPC.

To configure traffic sampling:

1. Configure the sampling instance ins1 with sampling rate 10, run length 1, and the maximum packet length of 128 bytes.

   ```
   [edit forwarding-options]
   user@ptx3000# set sampling instance ins1 input rate 10
   user@ptx3000# set sampling instance ins1 input run-length 1
   user@ptx3000# set sampling instance ins1 input maximum-packet-length 128
   ```

2. Apply the sampling instance to an FPC on the PTX3000 router by including the **sampling-instance** statement at the **[edit chassis]** hierarchy level.

   The FPC number must match the FPC portion of the interface name for the interface on which sampling is enabled. In this example, FPC 1 is associated with the interface et-2/0/0 on which sampling is enabled.

   ```
   [edit chassis]
   user@ptx3000# set fpc 1 sampling instance ins1
   ```

Configuring the Flow Server to Collect the Active Flow Monitoring Version 9 Records

Step-by-Step Procedure

To configure the flow server:

1. Configure the flow server for IPv4, IPv6, and MPLS flows.

   - To configure the flow server for IPv4, include the **flow-server** statement and specify 192.0.2.2 as the IPv4 address of the host system that is collecting traffic flows at the **[edit forwarding-options sampling instance ins1 family inet output]** hierarchy level. Also include the **port** statement and specify UDP port 2055 for use by the flow server.

     ```
     [edit forwarding-options sampling instance ins1 family inet output]
     user@ptx3000# set flow-server 192.0.2.2 port 2055
     ```

   - To configure the flow server for IPv6, include the **flow-server** statement and specify 192.0.2.2 as the IPv4 address of the host system that is collecting traffic flows at the **[edit forwarding-options sampling instance ins1 family inet6 output]** hierarchy level. Also include the **port** statement and specify UDP port 2055 for use by the flow server.

     ```
     [edit forwarding-options sampling instance ins1 family inet6 output]
     user@ptx3000# set flow-server 192.0.2.2 port 2055
     ```

   - To configure the flow server for MPLS, include the **flow-server** statement and specify 192.0.2.2 as the IPv4 address of the host system that is collecting traffic flows at the **[edit forwarding-options sampling instance ins1 family mpls output]** hierarchy level. Also include the **port** statement and specify UDP port 2055 for use by the flow server.

     ```
     [edit forwarding-options sampling instance ins1 family mpls output]
     user@ptx3000# set flow-server 192.0.2.2 port 2055
     ```

2. Enable active flow monitoring by using the version 9 template format.

   - To enable active flow monitoring for IPv4 flows by using the version 9 template format, include the **version9 template** statement and specify v4_template as the name of the template to use at the **[edit forwarding-options sampling instance ins1 family inet output flow-server 192.0.2.2]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family inet output flow-server
       192.0.2.2]
     user@ptx3000# set version9 template v4_template
     ```

   - To enable active flow monitoring for IPv6 flows by using the version 9 template format, include the **version9 template** statement and specify v6_template as the name of the template to use at the **[edit forwarding-options sampling instance ins1 family inet6 output flow-server 192.0.2.2]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family inet6 output flow-server
       192.0.2.2 ]
     user@ptx3000# set version9 template v6_template
     ```

   - To enable active flow monitoring for MPLS flows by using the version 9 template format, include the **version9 template** statement and specify mpls as the name

of the template to use at the **[edit forwarding-options sampling instance ins1 family mpls output flow-server 192.0.2.2]** hierarchy level.

```
[edit forwarding-options sampling instance ins1 family mpls output flow-server
  192.0.2.2]
user@ptx3000# set version9 template mpls
```

3. Configure the interface connected to the flow server by specifying the source address for generating the monitored packets.

   - For IPv4 flows, configure the interface connected to the flow server by specifying 192.0.2.1 as the source address for generating the monitored packets at the **[edit forwarding-options sampling instance ins1 family inet output]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family inet output]
     user@ptx3000# set interfaces ats1 source-address 192.0.2.1
     ```

   - For IPv6 flows, configure the interface connected to the flow server by specifying 192.0.2.1 as the source address for generating the monitored packets at the **[edit forwarding-options sampling instance ins1 family inet6 output]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family inet6 output]
     user@ptx3000# set interfaces ats1 source-address 192.0.2.1
     ```

   - For MPLS flows, configure the interface connected to the flow server by specifying 192.0.2.1 as the source address for generating the monitored packets at the **[edit forwarding-options sampling instance ins1 family mpls output]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family mpls output]
     user@ptx3000# set interfaces ats1 source-address 192.0.2.1
     ```

4. Configure the address of the export port that is used by the v9 records to reach the flow server.

   - For IPv4 flows, configure the export port address 192.0.2.1/24 at the **[edit forwarding-options sampling instance ins1 family inet output]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family inet output]
     user@ptx3000# set interface ats1 export-port address 192.0.2.1/24
     ```

   - For IPv6 flows, configure the export port address 192.0.2.1/24 at the **[edit forwarding-options sampling instance ins1 family inet6 output]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family inet6 output]
     user@ptx3000# set interface ats1 export-port address 192.0.2.1/24
     ```

   - For MPLS flows, configure the export port address 192.0.2.1/24 at the **[edit forwarding-options sampling instance ins1 family mpls output]** hierarchy level.

     ```
     [edit forwarding-options sampling instance ins1 family mpls output]
     user@ptx3000# set interface ats1 export-port address 192.0.2.1/24
     ```

Results

Display the results of the configuration.

```
user@ptx3000> show configuration
  chassis {
    fpc 1 {
```

```
      sampling-instance ins1;
    }
  }
  services {
    flow-monitoring {
      version9 {
        template v4_template {
          flow-active-timeout 60;
          flow-inactive-timeout 30;
          template-refresh-rate {
            packets 480;
          }
          option-refresh-rate {
            packets 480;
          }
          ipv4-template;
        }
        template v6_template {
          flow-active-timeout 60;
          flow-inactive-timeout 30;
          template-refresh-rate {
            packets 480;
          }
          option-refresh-rate {
            packets 480;
          }
          ipv6-template;
        }
        template mpls {
          flow-active-timeout 60;
          flow-inactive-timeout 30;
          template-refresh-rate {
            packets 480;
          }
          option-refresh-rate {
            packets 480;
          }
          mpls-template {
            label-position [ 1 2];
          }
        }
      }
    }
  }
  interfaces {
    et-2/0/0 {
      unit 0 {
        family inet {
          filter {
            input ipv4_sample_filter;
          }
        }
        family inet6 {
          filter {
            input ipv6_sample_filter;
          }
```

```
        }
        family mpls {
          filter {
            input mpls_sample_filter;
          }
        }
      }
    }
    et-4/0/0 {
      gigether-options {
        802.3ad ats1;
      }
    }
    et-4/0/3 {
      gigether-options {
        802.3ad ats1;
      }
    }
    ats1 {
      unit 0 {
        family inet;
        family inet6;
        family mpls;
      }
    }
}
forwarding-options {
    sampling {
      instance {
        ins1 {
          input {
            rate 10;
            run-length 1;
            maximum-packet-length 128;
          }
          family inet {
            output {
              flow-server 192.0.2.2 {
                port 2055;
                version9 {
                  template {
                    v4_template;
                  }
                }
              }
              interface ats1 {
                source-address 192.0.2.1;
                export-port {
                  address 192.0.2.1/24;
                }
              }
            }
          }
          family inet6 {
            output {
              flow-server 192.0.2.2 {
```

```
                port 2055;
                version9 {
                  template {
                    v6_template;
                  }
                }
              }
              interface ats1 {
                source-address 192.0.2.1;
                export-port {
                  address 192.0.2.1/24;
                }
              }
            }
          }
          family mpls{
            output {
              flow-server 192.0.2.2 {
                port 2055;
                version9 {
                  template {
                    mpls;
                  }
                }
              }
              interface ats1 {
                source-address 192.0.2.1;
                export-port {
                  address 192.0.2.1/24;
                }
              }
            }
          }
        }
      }
    }
    firewall {
      family inet {
        filter ipv4_sample_filter {
          term 1 {
            then {
              count c1;
              sample;
              accept;
            }
          }
        }
      }
      family inet6 {
        filter ipv6_sample_filter {
          term 1 {
            then {
              count c1;
              sample;
              accept;
```

```
            }
          }
        }
      }
      family mpls {
        filter mpls_sample_filter {
          term 1 {
            then {
              count c1;
              sample;
              accept;
            }
          }
        }
      }
    }
```

Verification

Confirm that the configuration is working properly.

Verifying That the Packets Are Received on the Routers

Purpose Verify that the packets are received on the PTX5000 and PTX3000 routers.

Action In operational mode, enter the **show interface et-1/0/0** command on the PTX5000 router.

```
user@ptx5000> show interface et-1/0/0
Physical interface: et-1/0/0, Enabled, Physical link is Up
  Interface index: 325, SNMP ifIndex: 537
  Link-level type: Ethernet, MTU: 1514, Speed: 10Gbps, BPDU Error: None,
MAC-REWRITE Error: None, Loopback: Disabled, Source filtering: Disabled,
  Flow control: Enabled
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Current address: f8:c0:01:3a:c6:98, Hardware address: f8:c0:01:3a:c6:98
  Last flapped   : 2012-12-18 06:53:45 PST (14:44:49 ago)
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)
  Active alarms  : None
  Active defects : None
  Interface transmit statistics: Disabled
  Logical interface et-1/0/0.0 (Index 76) (SNMP ifIndex 583)
    Flags: SNMP-Traps 0x4004000 Encapsulation: ENET2
    Input packets : 108
    Output packets: 108
    Protocol inet, MTU: 1500
      Flags: Sendbcast-pkt-to-re
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 1.1.1/24, Local: 1.1.1.1, Broadcast: 1.1.1.255
    Protocol multiservice, MTU: Unlimited
      Flags: Is-Primary
```

In operational mode, enter the **show interface et-2/0/0** command on the PTX3000 router.

```
user@ptx3000> show interface et-2/0/0
Physical interface: et-2/0/0, Enabled, Physical link is Up
  Interface index: 130, SNMP ifIndex: 511
  Link-level type: Ethernet, MTU: 1514, MRU: 0, LAN-PHY mode, Speed: 10Gbps, BPDU
 Error: None, MAC-REWRITE Error: None, Loopback: None, Source filtering: Disabled,

  Flow control: Enabled
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Current address: 08:81:f4:3c:ec:72, Hardware address: 08:81:f4:3c:ec:72
  Last flapped   : 2014-07-14 03:30:36 PDT (1d 21:18 ago)
    Input packets : 138
    Output packets: 138
  Active alarms  : None
  Active defects : None
  PCS statistics                      Seconds
    Bit errors                             3
    Errored blocks                         3
  Interface transmit statistics: Disabled
```

Meaning The following command output values of the **Physical interface** field indicates that interface et-1/0/0 on the PTX5000 router and interface et-2/0/0 on the PTX3000 router are working.

- **et-1/0/0, Enabled, Physical link is Up**

- et-2/0/0, Enabled, Physical link is Up

The following command output values on the PTX5000 and PTX3000 routers indicate that the interfaces on the routers are receiving packets.

- Input packets : 108
- Input packets : 138

Verifying That the Packets Are Matched and Filtered According to the Configuration

Purpose Verify that the packets are matched and filtered according to the configuration.

Action In operational mode, enter the **show firewall** command on the PTX5000 router.

```
user@ptx5000> show firewall
Filter: ipv4_sample_filter
Counters:
Name                                                Bytes              Packets
c1                                                  11880                  108


Filter: ipv6_sample_filter
Counters:
Name                                                Bytes              Packets
c1                                                  11980                  192


Filter: mpls_sample_filter
Counters:
Name                                                Bytes              Packets
c1                                                  12880                  208
```

In operational mode, enter the **show firewall** command on the PTX3000 router.

```
user@ptx3000> show firewall
Filter: ipv4_sample_filter
Counters:
Name                                                Bytes              Packets
c1                                                  11880                  130


Filter: ipv6_sample_filter
Counters:
Name                                                Bytes              Packets
c1                                                  11980                  192


Filter: mpls_sample_filter
Counters:
Name                                                Bytes              Packets
c1                                                  12880                  208
```

Meaning The **Bytes** field displays the number of bytes that match the filter term under which the counter action is specified.

The **Packets** field displays the number of packets that match the filter term under which the counter action is specified.

The results indicate that the packets are matched and filtered according to the configuration.

Verifying That the ATS Interface Is Forwarding Packets

Purpose Verify that the ats0 and ats1 interfaces are forwarding packets.

Action In operational mode, enter the **show interfaces ats0** command on the PTX5000 router.

```
user@ptx5000> show interfaces ats0
Physical interface: ats0, Enabled, Physical link is Up
  Interface index: 129, SNMP ifIndex: 574
  Type: Ethernet, Link-level type: Ethernet, MTU: 9536, Speed: 10Gbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link type      : Full-Duplex
  Link flags     : None
  Current address: f8:c0:01:3a:e4:8d, Hardware address: f8:c0:01:3a:e4:8d
  Last flapped   : 2012-12-18 21:35:22 PST (00:03:19 ago)
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)
  Logical interface ats0.0 (Index 72) (SNMP ifIndex 600)
    Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: Tether-Enet-Svcs
    Statistics        Packets        pps         Bytes          bps
    Bundle:
        Input :           108          0         13392            0
        Output:           108          0         13392            0
    Protocol inet, MTU: 9536
      Flags: Sendbcast-pkt-to-re
    Protocol inet6, MTU: 9536
      Flags: Is-Primary
    Protocol mpls, MTU: 9536, Maximum labels: 3
      Flags: Is-Primary
```

In operational mode, enter the **show interfaces ats1** command on the PTX3000 router.

```
user@ptx3000> show interfaces ats1
Physical interface: ats1, Enabled, Physical link is Up
  Interface index: 129, SNMP ifIndex: 574
  Type: Ethernet, Link-level type: Ethernet, MTU: 9536, Speed: 10Gbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link type      : Full-Duplex
  Link flags     : None
  Current address: f8:c0:01:3a:e4:8d, Hardware address: f8:c0:01:3a:e4:8d
  Last flapped   : 2012-12-18 21:35:22 PST (00:03:19 ago)
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)
  Logical interface ats0.0 (Index 72) (SNMP ifIndex 600)
    Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: Tether-Enet-Svcs
    Statistics        Packets        pps         Bytes          bps
    Bundle:
        Input :           144          0         17856            0
        Output:           144          0         17856            0
    Protocol inet, MTU: 9536
      Flags: Sendbcast-pkt-to-re
    Protocol inet6, MTU: 9536
      Flags: Is-Primary
    Protocol mpls, MTU: 9536, Maximum labels: 3
      Flags: Is-Primary
```

Meaning The **Packets** and **Bytes** fields under the **Bundle** statistics show that the ats0 and ats1 interfaces are forwarding the packets (**Output** field) to the CSE2000.

Verifying That Active Flow Monitoring Is Working

Purpose Verify that active flow monitoring is working.

Action To verify that active flow monitoring is working, use the **show services accounting flow** command on the PTX5000 and PTX3000 routers.

```
user@ptx5000> show services accounting flow
  Flow information
    Service Accounting interface: ats0, Local interface index: 149
    Flow packets: 87168293, Flow bytes: 5578770752
    Flow packets 10-second rate: 45762, Flow bytes 10-second rate: 2928962
    Active flows: 1000, Total flows: 2000
    Flows exported: 19960, Flows packets exported: 582
    Flows inactive timed out: 1000, Flows active timed out: 29000

user@ptx3000> show services accounting flow
  Flow information
    Service Accounting interface: ats1, Local interface index: 149
    Flow packets: 87168293, Flow bytes: 5578770752
    Flow packets 10-second rate: 45762, Flow bytes 10-second rate: 2928962
    Active flows: 1000, Total flows: 2000
    Flows exported: 19960, Flows packets exported: 582
    Flows inactive timed out: 1000, Flows active timed out: 29000
```

Meaning The output of the PTX5000 and PTX3000 routers shows that active flows exist and that flow packets are being exported. This indicates that flow monitoring is working. If flow monitoring is not working, verify that the CSE2000 is operational.

Verifying That the CSE2000 Service Cards Are Operational

Purpose Verify that the configured CSE2000 service cards are present in the chassis and are operational.

Action To verify that the configured CSE2000 service cards (connected to the two routers) are operational, use the **show chassis hardware** command on the PTX5000 and PTX3000 routers.

```
user@ptx5000> show chassis hardware
Item             Version  Part number  Serial number     Description
Chassis                               JN11FF811AJA      PTX5000
Midplane         REV 11   750-035893   ACAW6233          Midplane-8S
FPM              REV 12   760-030647   BBAX0093          Front Panel Display
PDU 0            Rev 07   740-032019   1E002220031       DC Power Dist Unit
  PSM 0          Rev 06   740-032022   1E002280079       DC 12V Power Supply
  PSM 1          Rev 06   740-032022   1E002280070       DC 12V Power Supply
  PSM 2          Rev 06   740-032022   1E002280080       DC 12V Power Supply
  PSM 3          Rev 06   740-032022   1E002280069       DC 12V Power Supply
PDU 1            Rev 07   740-032019   1E002220052       DC Power Dist Unit
  PSM 0          Rev 06   740-032022   1E002280040       DC 12V Power Supply
  PSM 2          Rev 06   740-032022   1E002280071       DC 12V Power Supply
Routing Engine 0 REV 10   740-026942   P737A-003458      RE-DUO-2600
Routing Engine 1 REV 10   740-026942   P737A-003388      RE-DUO-2600
CB 0             REV 16   750-030625   BBAW8988          Control Board
  Xcvr 0         REV 01   740-031980   1Y3363A02396      SFP+-10G-SR
  Xcvr 2         REV 02   740-013111   A430887           SFP-T
```

```
  Xcvr 3          REV 01   740-038291   C489070           SFP-T
CB 1              REV 16   750-030625   BBAV3847          Control Board
  Xcvr 0          REV 01   740-031980   1Y3363A02054      SFP+-10G-SR
  Xcvr 2          REV 01   740-013111   60901034          SFP-T
  Xcvr 3          REV 01   740-038291   C489072           SFP-T
FPC 0             REV 22   750-036844   BBAV9151          FPC
  CPU             REV 13   711-030686   BBAW8899          SNG PMB
  PIC 0           REV 21   750-031913   BBAX1097          24x 10GE(LAN) SFP+
    Xcvr 10       REV 01   740-031980   ANF08QE           SFP+-10G-SR
    Xcvr 11       REV 01   740-031980   AMB0WKG           SFP+-10G-SR
    Xcvr 12       REV 01   740-031980   B11J04031         SFP+-10G-SR
    Xcvr 13       REV 01   740-031980   AMB0TD9           SFP+-10G-SR
  PIC 1           REV 21   750-031913   BBAW4241          24x 10GE(LAN) SFP+
FPC 3             REV 03   711-035673   EF4357            Vaudville FPC P1
  CPU             REV 06   711-030686   EF3468            SNG PMB
  PIC 0           REV 21   750-031913   BBBA1821          24x 10GE(LAN) SFP+
    Xcvr 10       REV 01   740-031980   1Y3363A02069      SFP+-10G-SR
    Xcvr 11       REV 01   740-031980   063363A00044      SFP+-10G-SR
  PIC 1           REV 18   750-031916   BBBA2677          2x 100GE CFP
ESC 0             REV 00   650-049328   CJ2313AL0050      CSE2000-32G-S
  Backplane       REV 00   650-049327   CH2313AL0050      CSE2000 Chassis
SPMB 0            REV 13   711-030686   BBAW9018          SNG PMB
SPMB 1            REV 13   711-030686   BBAW2165          SNG PMB
SIB 0             REV 12   750-030631   BBAW9889          SIB-I-8S
SIB 1             REV 12   750-030631   BBAW4352          SIB-I-8S
SIB 2             REV 12   750-030631   BBAW4363          SIB-I-8S
SIB 3             REV 12   750-030631   BBAW9919          SIB-I-8S
SIB 4             REV 12   750-030631   BBAW4404          SIB-I-8S
SIB 5             REV 12   750-030631   BBAX0348          SIB-I-8S
SIB 6             REV 12   750-030631   BBAW9861          SIB-I-8S
SIB 7             REV 12   750-030631   BBAW9852          SIB-I-8S
SIB 8             REV 12   750-030631   BBAW4308          SIB-I-8S
Fan Tray 0        REV 10   760-032784   BBAW8152          Vertical Fan Tray
Fan Tray 1        REV 13   760-030642   BBAV8820          Horizontal Fan Tray
Fan Tray 2        REV 13   760-030642   BBAV3612          Horizontal Fan Tray
```

```
user@ptx3000> show chassis hardware
Item             Version  Part number  Serial number     Description
Chassis                                JN11FF811AJA      PTX5000
Midplane         REV 11   750-035893   ACAW6233          Midplane-8S
FPM              REV 12   760-030647   BBAX0093          Front Panel Display
PDU 0            Rev 07   740-032019   1E002220031       DC Power Dist Unit
  PSM 0          Rev 06   740-032022   1E002280079       DC 12V Power Supply
  PSM 1          Rev 06   740-032022   1E002280070       DC 12V Power Supply
  PSM 2          Rev 06   740-032022   1E002280080       DC 12V Power Supply
  PSM 3          Rev 06   740-032022   1E002280069       DC 12V Power Supply
PDU 1            Rev 07   740-032019   1E002220052       DC Power Dist Unit
  PSM 0          Rev 06   740-032022   1E002280040       DC 12V Power Supply
  PSM 2          Rev 06   740-032022   1E002280071       DC 12V Power Supply
Routing Engine 0 REV 10   740-026942   P737A-003458      RE-DUO-2600
Routing Engine 1 REV 10   740-026942   P737A-003388      RE-DUO-2600
CB 0             REV 16   750-030625   BBAW8988          Control Board
  Xcvr 0         REV 01   740-031980   1Y3363A02396      SFP+-10G-SR
  Xcvr 2         REV 02   740-013111   A430887           SFP-T
  Xcvr 3         REV 01   740-038291   C489070           SFP-T
CB 1             REV 16   750-030625   BBAV3847          Control Board
  Xcvr 0         REV 01   740-031980   1Y3363A02054      SFP+-10G-SR
  Xcvr 2         REV 01   740-013111   60901034          SFP-T
  Xcvr 3         REV 01   740-038291   C489072           SFP-T
FPC 0            REV 22   750-036844   BBAV9151          FPC
```

```
  CPU            REV 13   711-030686   BBAW8899          SNG PMB
  PIC 0          REV 21   750-031913   BBAX1097          24x 10GE(LAN) SFP+
    Xcvr 10      REV 01   740-031980   ANF08QE           SFP+-10G-SR
    Xcvr 11      REV 01   740-031980   AMB0WKG           SFP+-10G-SR
    Xcvr 12      REV 01   740-031980   B11J04031         SFP+-10G-SR
    Xcvr 13      REV 01   740-031980   AMB0TD9           SFP+-10G-SR
  PIC 1          REV 21   750-031913   BBAW4241          24x 10GE(LAN) SFP+
FPC 3            REV 03   711-035673   EF4357            Vaudville FPC P1
  CPU            REV 06   711-030686   EF3468            SNG PMB
  PIC 0          REV 21   750-031913   BBBA1821          24x 10GE(LAN) SFP+
    Xcvr 10      REV 01   740-031980   1Y3363A02069      SFP+-10G-SR
    Xcvr 11      REV 01   740-031980   063363A00044      SFP+-10G-SR
  PIC 1          REV 18   750-031916   BBBA2677          2x 100GE CFP
ESC 1            REV 00   650-049328   CJ2313AL0050      CSE2000-32G-S
  Backplane      REV 00   650-049327   CH2313AL0050      CSE2000 Chassis
SPMB 0           REV 13   711-030686   BBAW9018          SNG PMB
SPMB 1           REV 13   711-030686   BBAW2165          SNG PMB
SIB 0            REV 12   750-030631   BBAW9889          SIB-I-8S
SIB 1            REV 12   750-030631   BBAW4352          SIB-I-8S
SIB 2            REV 12   750-030631   BBAW4363          SIB-I-8S
SIB 3            REV 12   750-030631   BBAW9919          SIB-I-8S
SIB 4            REV 12   750-030631   BBAW4404          SIB-I-8S
SIB 5            REV 12   750-030631   BBAX0348          SIB-I-8S
SIB 6            REV 12   750-030631   BBAW9861          SIB-I-8S
SIB 7            REV 12   750-030631   BBAW9852          SIB-I-8S
SIB 8            REV 12   750-030631   BBAW4308          SIB-I-8S
Fan Tray 0       REV 10   760-032784   BBAW8152          Vertical Fan Tray
Fan Tray 1       REV 13   760-030642   BBAV8820          Horizontal Fan Tray
Fan Tray 2       REV 13   760-030642   BBAV3612          Horizontal Fan Tray
```

Meaning The output **ESC 0** and **ESC 1** shows that CSE2000 service cards have completed booting and are operational. If the service card is operational but flow monitoring is not working, verify that sampling is enabled on the media interface on which traffic flow is expected and that the sampling filter direction is correct.

Verifying That Sampling Is Enabled and the Filter Direction Is Correct for Active Flow Monitoring

Purpose Verify that sampling is enabled on the media interface on which traffic flow is expected and that the sampling filter direction is correct.

Action To verify that sampling is enabled on the media interface on which traffic flow is expected and that the sampling filter direction is correct, use the **show interfaces *interface-name* extensive | grep filters** command on the PTX5000 and PTX3000 routers.

```
user@ptx5000> show interfaces et-1/0/0 extensive | grep filters
    CAM destination filters: 3, CAM source filters: 0
      Input Filters: ipv4_sample_filter
      Input Filters: ipv6_sample_filter
      Input Filters: mpls_sample_filter
```

```
user@ptx3000> show interfaces et-2/0/0 extensive | grep filters
    CAM destination filters: 3, CAM source filters: 0
      Input Filters: ipv4_sample_filter
      Input Filters: ipv6_sample_filter
```

```
Input Filters: mpls_sample_filter
```

Meaning The command output shows that the sample filter is applied to the media interface on which traffic flow is expected (**et-1/0/0** and **et-2/0/0**) and that the sampling filter direction is **Input**. If the CSE2000 service card is operational and the filters are correct, but flow monitoring is not working, verify that the sampling instance is applied to the FPC where the media interface resides.

TIP: If a firewall filter is used to enable sampling, add a counter as an action in the firewall filter. Then, check whether the counter is incrementing. An incrementing counter confirms that the traffic is present and that the filter direction is correct.

Verifying That the Sampling Instance Is Applied to the Correct FPC for Active Flow Monitoring

Purpose Verify that the sampling instance is applied to the FPC where the media interface resides.

Action To verify that the sampling instance Is applied to the correct FPC, use the **show configuration chassis** command on the PTX5000 and PTX3000 routers.

```
user@ptx5000> show configuration chassis

  fpc 1 {
    sampling-instance ins1;
  }
user@ptx3000> show configuration chassis

  fpc 1 {
    sampling-instance ins1;
  }
```

Meaning The output shows that the sampling instance is applied to the correct FPC. If the CSE2000 service card is operational, the filters are correct, and the sampling instance is applied to the correct FPC, but flow monitoring is not working, verify that the route record set of data is being created.

Verifying That the Route Record Is Being Created for Active Flow Monitoring

Purpose Verify that the route record set of data is being created.

Action To verify that the route record set of data is being created, use the **show services accounting status** command on the PTX5000 and PTX3000 routers.

```
user@ptx5000> show services accounting status
Service Accounting interface: ats0
  Export format: 9, Route record count: 40
  IFL to SNMP index count: 11, AS count: 1
```

```
  Configuration set: Yes, Route record set: Yes, IFL SNMP map set: Yes


user@ptx3000> show services accounting status
Service Accounting interface: ats1
  Export format: 9, Route record count: 40
  IFL to SNMP index count: 11, AS count: 1
  Configuration set: Yes, Route record set: Yes, IFL SNMP map set: Yes
```

Meaning The output shows that the **Route record set** field is set to **Yes**. This confirms that the route record set is created.

TIP: If the route record set field is set to no, the record might not have been downloaded yet. Wait for 60–100 seconds and check again. If the route record is still not created, verify that the sampling process is running, that the connection between the CSE2000 service card and the process is operational, and that the CSE2000 service card memory is not overloaded.

Verifying That the Sampling Process Is Running for Active Flow Monitoring

Purpose Verify that the sampling process is running.

Action To verify that the sampling process is running, use the **show system processes extensive | grep sampled** command on the PTX5000 and PTX3000 routers.

```
user@ptx5000> show system processes extensive | grep sampled
PID USERNAME  THR PRI NICE   SIZE    RES   STATE    TIME   WCPU   COMMAND
1581 root     1   1   111    5660K  5108K select   0:00  0.00%   sampled

user@ptx3000> show system processes extensive | grep sampled
PID USERNAME  THR PRI NICE   SIZE    RES   STATE    TIME   WCPU   COMMAND
1581 root     1   1   111    5660K  5108K select   0:00  0.00%   sampled
```

Meaning The output shows that **sampled** is listed as a running system process. In addition to verifying that the process is running, verify that the TCP connection between the sampled process and the CSE2000 service card is operational.

Verifying That the TCP Connection Is Operational for Active Flow Monitoring

Purpose Verify that the TCP connection between the sampled process and the CSE2000 service card is operational.

Action To verify that the TCP connection is operational, use the **show system connections inet | grep 6153** command on the PTX5000 and PTX3000 routers.

```
user@ptx5000> show system connections inet | grep 6153
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
~
~
```

```
~
tcp        0      0  128.0.0.1.6153       128.0.2.17.11265    ESTABLISHED
tcp4       0      0  *.6153                 *.*                    LISTEN

user@ptx3000> show system connections inet | grep 6153
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
~
~
~
tcp        0      0  128.0.0.1.6153       128.0.2.17.11265    ESTABLISHED
tcp4       0      0  *.6153                 *.*                    LISTEN
```

Meaning The output shows that the TCP connection between the sampled process socket (**6153**) and the CSE2000 service card (**128.0.0.1**) is **ESTABLISHED**.

TIP: If the TCP connection between the sampled process and the CSE2000 service card is not established, restart the sampled process by using the **restart sampling** command.

Related Documentation

- Active Flow Monitoring on PTX Series Routers with CSE2000 Overview on page 1
- Example: Configuring Active Flow Monitoring Version 9 on a PTX Series Router Tethered to a CSE2000 on page 3

