



---

# Flow Monitoring Feature Guide for CSE2000



Modified: 2017-02-03

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
www.juniper.net

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

*Flow Monitoring Feature Guide for CSE2000*  
Copyright © 2017, Juniper Networks, Inc.  
All rights reserved.

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 the Documentation . . . . .	ix
	Documentation and Release Notes . . . . .	ix
	Supported Platforms . . . . .	ix
	Using the Examples in This Manual . . . . .	ix
	Merging a Full Example . . . . .	x
	Merging a Snippet . . . . .	x
	Documentation Conventions . . . . .	xi
	Documentation Feedback . . . . .	xiii
	Requesting Technical Support . . . . .	xiii
	Self-Help Online Tools and Resources . . . . .	xiii
	Opening a Case with JTAC . . . . .	xiv
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Active Flow Monitoring Version 9 Using CSE2000 . . . . .</b>	<b>3</b>
	Flow Monitoring Using CSE2000 Overview . . . . .	3
	Active Flow Monitoring Version 9 Formats and Fields . . . . .	6
	Aggregated Tethered Services Interfaces Overview . . . . .	13
	Properties of ATS Interfaces . . . . .	14
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 2</b>	<b>Active Flow Monitoring Version 9 Using CSE2000 . . . . .</b>	<b>19</b>
	Configuring Member Interfaces and Interface Family for Aggregated Tethered Services Interfaces . . . . .	19
	Configuring Active Flow Monitoring Version 9 Templates . . . . .	20
	Configuring a Firewall Filter for Active Flow Monitoring Version 9 . . . . .	22
	Configuring Traffic Sampling . . . . .	23
	Configuring Flow Server to Collect Active Flow Monitoring Version 9 Records . . . . .	23
	Example: Configuring Active Flow Monitoring Version 9 for IPv4 . . . . .	24
	Example: Configuring Active Flow Monitoring Version 9 for IPv6 . . . . .	38
	Example: Configuring Active Flow Monitoring Version 9 for MPLS . . . . .	52
	Example: Configuring Active Flow Monitoring Version 9 for MPLS and IPv4 . . . . .	67
	Example: Configuring Active Flow Monitoring Version 9 for Simultaneous IPv4, MPLS, and IPv6 Sampling . . . . .	82
	Example: Configuring Active Flow Monitoring Version 9 on PTX3000 and PTX5000 When Both Are Tethered to a CSE2000 . . . . .	102
<b>Chapter 3</b>	<b>Active Flow Monitoring Version 9 Configuration Statements . . . . .</b>	<b>137</b>
	disable (Forwarding Options) . . . . .	138
	export-port . . . . .	139
	family (Sampling) . . . . .	140

filter (Configuring) . . . . .	141
flow-active-timeout . . . . .	142
flow-inactive-timeout . . . . .	143
flow-server . . . . .	144
flow-monitoring . . . . .	145
input (Sampling) . . . . .	146
instance (Sampling) . . . . .	147
interface (Monitoring) . . . . .	148
ipv4-template . . . . .	149
ipv6-template . . . . .	149
label-position . . . . .	150
maximum-packet-length . . . . .	150
mpls-ipv4-template . . . . .	151
mpls-template . . . . .	151
option-refresh-rate . . . . .	152
template-refresh-rate . . . . .	153
output (Sampling) . . . . .	154
port . . . . .	155
rate (Forwarding Options) . . . . .	155
run-length . . . . .	156
sampling (Forwarding Options) . . . . .	157
source-address (Forwarding Options) . . . . .	158
template (Forwarding Options) . . . . .	158
version9 (Forwarding Options) . . . . .	159

## Part 3

## Administration

### Chapter 4

<b>Active Flow Monitoring Version 9 Operational Commands . . . . .</b>	<b>163</b>
show interfaces . . . . .	164
show services accounting errors . . . . .	169
show services accounting flow . . . . .	171
show services accounting status . . . . .	173
show system processes esc-node . . . . .	175

# List of Figures

<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Active Flow Monitoring Version 9 Using CSE2000</b>	<b>3</b>
	Figure 1: Active Flow Monitoring Version 9 by Tethering CSE2000 to PTX Series Router	5
	Figure 2: Version 9 Flow Header Format	8
	Figure 3: Version 9 Template FlowSet Format	9
	Figure 4: Version 9 Data FlowSet Format	11
	Figure 5: Version 9 Options Template Format	12
	Figure 6: Active Flow Monitoring Version 9 Options Data Record Format	13
	Figure 7: ATS Interfaces Between PTX Series Router and CSE2000	14
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 2</b>	<b>Active Flow Monitoring Version 9 Using CSE2000</b>	<b>19</b>
	Figure 8: Active Flow Monitoring Version 9 for IPv4 Topology	26
	Figure 9: Active Flow Monitoring Version 9 for IPv6 Topology	40
	Figure 10: Active Flow Monitoring Version 9 for MPLS Topology	54
	Figure 11: Active Flow Monitoring Version 9 for MPLS and IPv4 Topology	68
	Figure 12: Active Flow Monitoring Version 9 for Simultaneous IPv4, IPv6 and MPLS Topology	84
	Figure 13: Active Flow Monitoring Version 9 on PTX3000 and PTX5000 Connected to CSE2000	103



# List of Tables

	<b>About the Documentation</b> . . . . .	<b>ix</b>
	Table 1: Notice Icons . . . . .	xi
	Table 2: Text and Syntax Conventions . . . . .	xii
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Active Flow Monitoring Version 9 Using CSE2000</b> . . . . .	<b>3</b>
	Table 3: Flow Monitoring Version 9 Template Formats . . . . .	7
	Table 4: Version 9 Flow Header Fields . . . . .	8
	Table 5: Version 9 Template FlowSet Fields . . . . .	9
	Table 6: Field Type Definitions Supported in Junos OS . . . . .	10
	Table 7: Version 9 Data FlowSet Format . . . . .	11
	Table 8: Version 9 Options Template Format . . . . .	12
	Table 9: Active Flow Monitoring Version 9 Options Data Record Format . . . . .	13
<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 4</b>	<b>Active Flow Monitoring Version 9 Operational Commands</b> . . . . .	<b>163</b>
	Table 10: show interfaces Output Fields . . . . .	165
	Table 11: show services accounting errors Output Fields . . . . .	169
	Table 12: show services accounting flow Output Fields . . . . .	171
	Table 13: show services accounting status Output Fields . . . . .	173
	Table 14: show system processes esc-node Output Fields . . . . .	175



# About the Documentation

- Documentation and Release Notes on page ix
- Supported Platforms on page ix
- Using the Examples in This Manual on page ix
- Documentation Conventions on page xi
- Documentation Feedback on page xiii
- Requesting Technical Support on page xiii

## Documentation and Release Notes

---

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

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

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

## Supported Platforms

---

For the features described in this document, the following platforms are supported:

- PTX5000
- PTX3000
- CSE2000

## Using the Examples in This Manual

---

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

## Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

## Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see [CLI Explorer](#).

## Documentation Conventions

Table 1 on page xi defines notice icons used in this guide.

Table 1: Notice Icons

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

Table 2 on page xii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> <b>show chassis alarms</b>  No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces or emphasizes important new terms.</li> <li>Identifies guide names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS CLI User Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name:  [edit] root@# <b>set system domain-name</b> <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the [edit protocols ospf area area-id] hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul>
< > (angle brackets)	Encloses optional keywords or variables.	<b>stub &lt;default-metric metric&gt;;</b>
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	<b>broadcast   multicast</b>  <b>(string1   string2   string3)</b>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	<b>community name members [ community-ids ]</b>
Indentation and braces ( { } )	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	}

---

## GUI Conventions

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

Convention	Description	Examples
<b>Bold text like this</b>	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> <li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li> <li>To cancel the configuration, click <b>Cancel</b>.</li> </ul>
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.
- E-mail—Send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net). Include the document or topic name, URL or page number, and software version (if applicable).

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

## Self-Help Online Tools and Resources

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

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

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

## Opening a Case with JTAC

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

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

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

## PART 1

# Overview

- [Active Flow Monitoring Version 9 Using CSE2000 on page 3](#)



## CHAPTER 1

# Active Flow Monitoring Version 9 Using CSE2000

- [Flow Monitoring Using CSE2000 Overview on page 3](#)
- [Active Flow Monitoring Version 9 Formats and Fields on page 6](#)
- [Aggregated Tethered Services Interfaces Overview on page 13](#)

## Flow Monitoring Using CSE2000 Overview

---

**Supported Platforms** [CSE2000, PTX3000, PTX5000](#)

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. Further, 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 a 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 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:

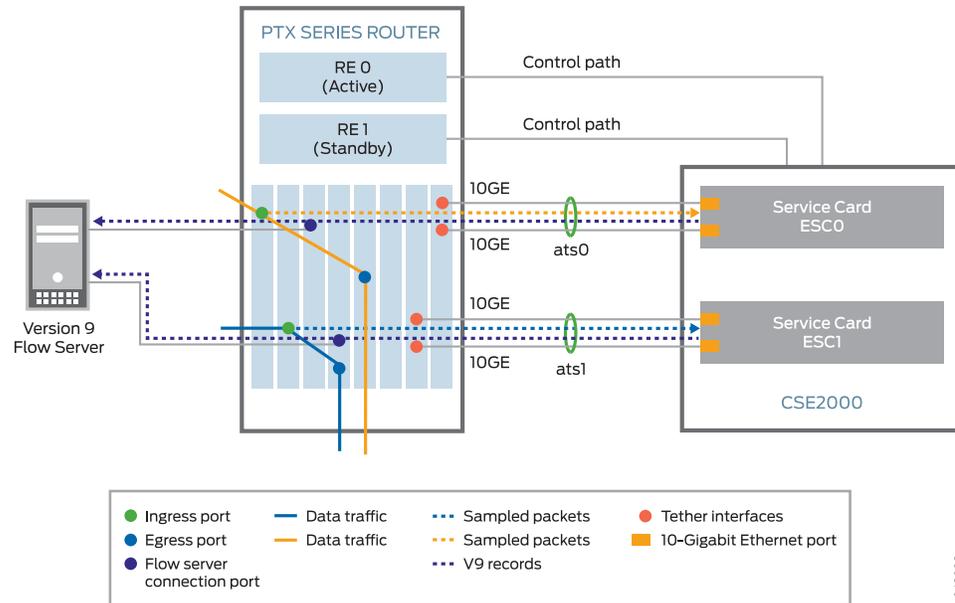
- Connect CSE2000 to a PTX5000 router.
- Connect CSE2000 to a PTX3000 router.
- Connect CSE2000 to two PTX3000 routers.
- Connect CSE2000 to two PTX5000 routers.
- Connect CSE2000 to a PTX5000 router and a PTX3000 router.

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 MPLS, IPv4, and IPv6 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 5](#).

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 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 Link Aggregation Control Protocol (LACP).

As shown in [Figure 1 on page 5](#), 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 for IPv4 on page 24](#)
- [Example: Configuring Active Flow Monitoring Version 9 for IPv6 on page 38](#)
- [Example: Configuring Active Flow Monitoring Version 9 for MPLS on page 52](#)
- [Example: Configuring Active Flow Monitoring Version 9 for MPLS and IPv4 on page 67](#)
- [Example: Configuring Active Flow Monitoring Version 9 for Simultaneous IPv4, MPLS, and IPv6 Sampling on page 82](#)
- [Example: Configuring Active Flow Monitoring Version 9 on PTX3000 and PTX5000 When Both Are Tethered to a CSE2000 on page 102](#)

## Active Flow Monitoring Version 9 Formats and Fields

---

**Supported Platforms** [CSE2000, PTX3000, PTX5000](#)

A detailed explanation of active flow monitoring version 9 packet formats and fields is shown as follows:

- [Table 3 on page 7](#)
- [Figure 2 on page 8](#)
- [Table 4 on page 8](#)
- [Figure 4 on page 11](#)
- [Table 4 on page 8](#)
- [Figure 5 on page 12](#)
- [Table 8 on page 12](#)
- [Figure 6 on page 13](#)
- [Table 9 on page 13](#)

Junos OS supports the following version 9 template formats:

Table 3: Flow Monitoring Version 9 Template Formats

Template	Fields
IPv4	<p>Flow selectors:</p> <ul style="list-style-type: none"> <li>• Source and destination IP address</li> <li>• Source and destination address prefix mask lengths</li> <li>• Source and destination port numbers</li> <li>• IP protocol and IP type of service</li> <li>• ICMP type</li> </ul> <p>Flow nonselectors:</p> <ul style="list-style-type: none"> <li>• TCP flags</li> <li>• Input and output SNMP</li> <li>• Input bytes</li> <li>• Input packets</li> <li>• Start time</li> <li>• End time</li> </ul>
MPLS	<p>Flow selectors:</p> <ul style="list-style-type: none"> <li>• MPLS label 1</li> <li>• MPLS label 2</li> <li>• MPLS label 3</li> </ul> <p>Flow nonselectors:</p> <ul style="list-style-type: none"> <li>• Input and output SNMP</li> <li>• Input bytes</li> <li>• Input packets</li> <li>• Start time</li> <li>• End time</li> </ul>
MPLS_IPv4	<p>Flow selectors:</p> <ul style="list-style-type: none"> <li>• MPLS label 1</li> <li>• MPLS label 2</li> <li>• MPLS label 3</li> <li>• MPLS top-level FEC address</li> </ul> <p>Flow nonselectors:</p> <ul style="list-style-type: none"> <li>• Input and output SNMP</li> <li>• Input bytes</li> <li>• Input packets</li> <li>• Start time</li> <li>• End time</li> </ul>

**Table 3: Flow Monitoring Version 9 Template Formats (continued)**

Template	Fields
IPv6	<p>Flow selectors:</p> <ul style="list-style-type: none"> <li>• IP protocol and IP type of service</li> <li>• Source and destination port numbers</li> <li>• Input SNMP</li> <li>• Source and destination IPv6 address</li> <li>• ICMP type</li> </ul> <p>Flow nonselectors:</p> <ul style="list-style-type: none"> <li>• Input bytes</li> <li>• Input packets</li> <li>• TCP flags</li> <li>• Output SNMP</li> <li>• Source and destination autonomous system</li> <li>• Last and first switched</li> <li>• IPv6 source and destination mask</li> <li>• IP protocol version</li> <li>• IPv6 next hop</li> </ul>



**NOTE:** Peer AS billing traffic is not supported for active flow monitoring version 9 configuration on a PTX Series router tethered to a CSE2000.

**Figure 2: Version 9 Flow Header Format**

Byte 3	Byte 2	Byte 1	Byte 0
Version		Count	
sysUptime			
UNIX seconds			
Flow Sequence Number			
Source ID			

g016785

**Table 4: Version 9 Flow Header Fields**

Field	Description
Version	9
Count	Total number of records in the protocol data unit (PDU) or packet. This number includes all the options–FlowSet records, template FlowSet records, and data FlowSet records.
sysUptime	Current time elapsed, in milliseconds, since the router started.

Table 4: Version 9 Flow Header Fields (*continued*)

Field	Description
UNIX seconds	Current seconds since 0000 UTC 1970.
Flow sequence number	Sequence counter of total flows received.
Source ID	32-bit value that identifies the data exporter. Version 9 uses the integrated field diagnostics (IFD) SNMP index of the PIC or device that is exporting the data flow. This field is equivalent to <b>engine type</b> and <b>engine ID</b> fields found in versions 5 and 8.

Figure 3: Version 9 Template FlowSet Format

Byte 3	Byte 2	Byte 1	Byte 0
Flowset ID = 0	Length		
Template ID 256	Field Count		
Field Type 1	Field Length 1		
Field Type 2	Field Length 2		
...	...		
Field Type N	Field Type N		
Template ID 257	Field Count		
Field Type 1	Field Length 1		

9016786

Table 5: Version 9 Template FlowSet Fields

Field	Description
FlowSet ID	FlowSet type. FlowSet ID 0 is reserved for the Template FlowSet.
Length	FlowSet length. Individual template FlowSets might contain multiple template records, which means that the length of template FlowSets varies.
Template ID	Unique template ID assigned to each newly generated template. Templates numbered 256 and higher define data formats. Templates numbered 0 through 255 define FlowSet IDs.
Field Count	Fields in the template record. This field allows the collector to determine the end of the current template record and the start of the next.
Field Type	Field type. These are defined in <a href="#">Table 6 on page 10</a> .
Field Length	Length, in bytes, of the corresponding field type.

Table 6: Field Type Definitions Supported in Junos OS

Field Type	Description
1	IN_BYTES: The number of bytes associated with an IP flow. By default, the length is 4 bytes.
2	IN_PKTS: The number of packets associated with an IP flow. By default, the length is 4 packets.
4	PROTOCOL: The IP protocol byte.
5	TOS: The type-of-service byte setting of an incoming packet.
6	TCP_FLAGS: The cumulative TCP flags associated with a flow.
7	L4_SRC_PORT: The TCP/UDP source port.
8	IPv4_SRC_ADDR: The IPv4 source address.
9	SRC_MASK: The number of contiguous bits in the source subnet mask.
10	INPUT_SNMP: The IFD SNMP input interface index. By default, the length is 2.
11	L4_DST_PORT: The TCP/UDP destination port number.
12	IPv4_DST_ADDR: The IPv4 destination address.
13	DST_MASK: The number of contiguous bits in the destination subnet mask.
14	OUTPUT_SNMP: The IFD SNMP output interface index. By default, the length is 2.
16	SRC_AS: The source autonomous system number. This is always set to zero.
17	DST_AS: The destination autonomous system number. This is always set to zero.
18	BGP_IPV4_NEXT_HOP: The BGP IPv4 next-hop address.
21	LAST_SWITCHED: The uptime of the device (in milliseconds) at which the last packet of the flow was switched.
22	FIRST_SWITCHED: The uptime of the device (in milliseconds) at which the first packet of the flow was switched.
29	IPv6_SRC_MASK: The length of the IPv6 source mask, in contiguous bits.
30	IPv6_DST_MASK: The length of the IPv6 destination mask, in contiguous bits.
32	ICMP_TYPE: The ICMP type.

Table 6: Field Type Definitions Supported in Junos OS (*continued*)

Field Type	Description
34	SAMPLING_INTERVAL: The rate at which packets are sampled. As an example, a rate of 100 means that one packet is sampled for every 100 packets in the data flow.
35	SAMPLING_ALGORITHM: The type of algorithm being used. 0x01 indicates deterministic sampling and 0x02 indicates random sampling.
47	MPLS_TOP_LABEL_IP_ADDRESS: The MPLS top- label address.
60	IP_PROTOCOL_VERSION: The IP protocol version being used.
62	IPV6_NEXT_HOP: The IPv6 address of the next-hop router.
70	MPLS_LABEL_1: The first MPLS label in the stack.
71	MPLS_LABEL_2: The second MPLS label in the stack.
72	MPLS_LABEL_3: The third MPLS label in the stack.
128	DST_PEER_AS: The destination of the BGP peer AS.

Figure 4: Version 9 Data FlowSet Format

Byte 3	Byte 2	Byte 1	Byte 0
Flowset ID = Template ID		Length	
Record 1 - Field Value 1		Record 1 - Field Value 2	
Record 1 - Field Value 3		...	
Record 2 - Field Value 1		Record 2 - Field Value 2	
Record 2 - Field Value 3		Record 2 - Field Value 2	
Record 3 - Field Value 1		...	
...		Padding	

129106

Table 7: Version 9 Data FlowSet Format

Field	Description
<b>FlowSet ID = Template ID</b>	Data FlowSet that is associated with a FlowSet ID. The FlowSet ID maps to a previously generated template ID. The flow server must use the FlowSet ID to find the corresponding template record and decode the flow records from the FlowSet.
<b>Length</b>	FlowSet length. Data FlowSets are fixed in length.

**Table 7: Version 9 Data FlowSet Format (continued)**

Field	Description
<b>Record Number - Field Value Number</b>	Flow data records, each containing a set of field values. The template record identified by the FlowSet ID dictates the type and length of the field values.
<b>Padding</b>	Bytes (in zeros) that the exporter inserts so that the subsequent FlowSet starts at a 4-byte aligned boundary.

**Figure 5: Version 9 Options Template Format**

Byte 3	Byte 2	Byte 1	Byte 0
Flowset ID = 1		Length	
Template ID		Option Scope Length	
Option Length		Scope 1 Field Type	
Scope 1 Field Length		...	
Scope N Field Length		Option 1 Field Type	
Option 1 Field Length		...	
Option M Field Length		Padding	

9016780

**Table 8: Version 9 Options Template Format**

Field	Description
<b>FlowSet ID</b>	FlowSet type. FlowSet ID 1 is reserved for the options template.
<b>Length</b>	FlowSet length. Option template FlowSets are fixed in length.
<b>Template ID</b>	Template ID of the options template. Options template values are greater than 255.
<b>Option Scope Length</b>	Length, in bytes, of any scope field definition that is part of the options template record.
<b>Scope 1 Field Type</b>	Relevant process. The Junos OS supports the system process (1).
<b>Scope 1 Field Length</b>	Length, in bytes, of the option field.
<b>Padding</b>	Bytes the exporter inserts so that the subsequent FlowSet starts at a 4-byte aligned boundary.

**Figure 6: Active Flow Monitoring Version 9 Options Data Record Format**

Byte 3	Byte 2	Byte 1	Byte 0
Flowset ID = Template ID		Length	
Record 1 - Scope 1 Value		Record 1 - Option Field 1 Value	
Record 1 - Option Field 2 Value		...	
Record 2 - Option Field 2 Value		...	
Record 3 - Scope 1 Value		Record 3 - Option Field 1 Value	
...		Padding	

90162926

**Table 9: Active Flow Monitoring Version 9 Options Data Record Format**

Field	Description
<b>FlowSet ID = Template ID</b>	ID that precedes each options data flow record. The FlowSet ID maps to a previously generated template ID. The collector must use the FlowSet ID to find the corresponding template record and decode the options data flow records from the FlowSet.
<b>Length</b>	FlowSet length. Option FlowSets are fixed in length.
<b>Number of Flow Data Records</b>	Remainder of the options data FlowSet is a collection of flow data records, each containing a set of field values. The template record identified by the FlowSet ID dictates the type and length of the field values.
<b>Padding</b>	Bytes (in zeros) the exporter inserts so that the subsequent FlowSet starts at a 4-byte aligned boundary.

**Related Documentation**

- [Flow Monitoring Using CSE2000 Overview on page 3](#)
- [Configuring Active Flow Monitoring Version 9 Templates on page 20](#)

## Aggregated Tethered Services Interfaces Overview

**Supported Platforms** CSE2000, PTX3000, PTX5000

Aggregated tethered services (ATS) interfaces are similar to aggregated Ethernet interfaces; however, ATS interfaces do not support Link Aggregation Control Protocol (LACP). ATS interfaces enable load balancing across links pointing to the same service card on the CSE2000. In other words, even when one of the tethered links between the PTX5000 or PTX3000 and the CSE2000 service card is down, sampled traffic from PTX Series router to the CSE2000 and the v9 records from the CSE2000 to the PTX Series router continues to flow through the other link, which is up.

When you connect a PTX Series router to a CSE2000, two ATS interfaces (ats0 and ats1) are created. The interfaces of the PTX Series router that connect to a CSE2000 are configured as the member interfaces of the ATS interfaces. Doing so associates the

physical links of the router with the logical bundle of the ATS interfaces. You must also specify the constituent physical links by including the **802.3ad** statement. All the configurations are performed on the PTX Series router.

**Figure 7: ATS Interfaces Between PTX Series Router and CSE2000**

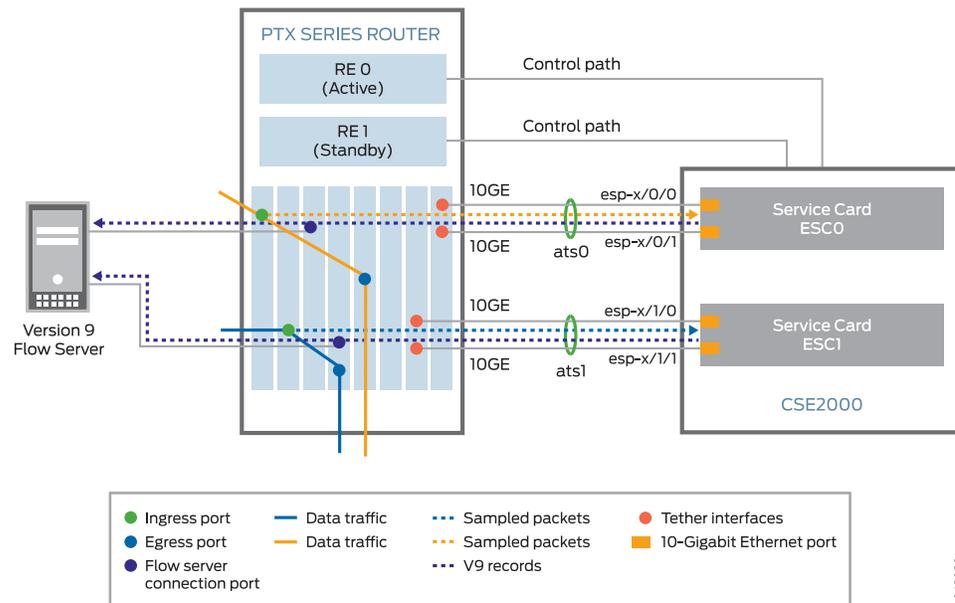


Figure 7 on page 14 shows the ATS interfaces between a PTX Series router and a CSE2000. The CSE2000 has two service cards (ESC0 and ESC1). For the data plane, the interfaces associated with these cards are represented by a logical interface *atsinterface-number* (where *interface-number* = 0 or 1). If the service card ESC0 is connected to the PTX Series router, then you use the interface *ats0* to represent the service card, whereas if the service card ESC1 is connected, then you use the interface *ats1*.

The CSE2000 service card logically occupies the last slot on the router chassis. In the PTX5000 chassis with eight slots, numbered 0 through 7, the CSE2000 service card occupies slot 8. If the *ats0* interface is configured and connected, the external service ports (ESPs) on the CSE2000 are represented as *esp-8/0/0* and *esp-8/0/1*. If the *ats1* interface is configured, the ESPs are represented as *esp-8/1/0* and *esp-8/1/1*. Similarly, the 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*.

## Properties of ATS Interfaces

An ATS interface has the following properties:

- An ATS interface is a point-to-point Interface.
- On the ATS interface, you can configure families **inet**, **inet6** and **mpls**.

- The maximum transmission unit (MTU) size supported for an ATS interface is 9192 bytes.
- The local MAC address of the ATS interface is assigned from the global MAC pool similar to those assigned for aggregated interfaces.
- A maximum of two 10-Gbps Ethernet member interfaces can be configured. These two interfaces must be present on the same FPC in the router that is tethered to the CSE2000.
- LACP is not supported on the ATS interface.
- At least one active member interface is needed for ATS to be active.
- Destination MAC (DMAC) filtering and source MAC (SMAC) filtering are not supported on the ATS interface.
- The ats0 interface represents the service card ESC0, whereas the ats1 interface represents the service card ESC1.
- Member interfaces inherit the properties of the ATS interface similar to the way member interfaces inherit the properties of aggregated Ethernet interfaces.
- If an interface is added as part of the ATS interface, then it cannot be configured separately.
- You must not configure any protocol on the ATS interface.

**Related  
Documentation**

- [Configuring Member Interfaces and Interface Family for Aggregated Tethered Services Interfaces on page 19](#)



## PART 2

# Configuration

- [Active Flow Monitoring Version 9 Using CSE2000 on page 19](#)
- [Active Flow Monitoring Version 9 Configuration Statements on page 137](#)



## CHAPTER 2

# Active Flow Monitoring Version 9 Using CSE2000

- [Configuring Member Interfaces and Interface Family for Aggregated Tethered Services Interfaces on page 19](#)
- [Configuring Active Flow Monitoring Version 9 Templates on page 20](#)
- [Configuring a Firewall Filter for Active Flow Monitoring Version 9 on page 22](#)
- [Configuring Traffic Sampling on page 23](#)
- [Configuring Flow Server to Collect Active Flow Monitoring Version 9 Records on page 23](#)
- [Example: Configuring Active Flow Monitoring Version 9 for IPv4 on page 24](#)
- [Example: Configuring Active Flow Monitoring Version 9 for IPv6 on page 38](#)
- [Example: Configuring Active Flow Monitoring Version 9 for MPLS on page 52](#)
- [Example: Configuring Active Flow Monitoring Version 9 for MPLS and IPv4 on page 67](#)
- [Example: Configuring Active Flow Monitoring Version 9 for Simultaneous IPv4, MPLS, and IPv6 Sampling on page 82](#)
- [Example: Configuring Active Flow Monitoring Version 9 on PTX3000 and PTX5000 When Both Are Tethered to a CSE2000 on page 102](#)

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

---

**Supported Platforms** CSE2000, PTX3000, PTX5000

ATS interfaces are similar to aggregated Ethernet interfaces; however, ATS interfaces do not support Link Aggregation Control Protocol (LACP). ATS interfaces enable load balancing across links pointing to the same service card on the CSE2000.

When you connect a PTX5000 or a PTX3000 router to a CSE2000, two ATS interfaces (ats0 and ats1) are created. The interfaces of a PTX Series router that connect to a CSE2000 are configured as the member interfaces of the ATS interfaces. Doing so associates the physical links of the router with the logical bundle of the ATS interfaces. You must also specify the constituent physical links by including the **802.3ad** statement. All the configurations are performed on the PTX Series router.

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

1. Configure the member interfaces of the ATS interface bundle.

[edit interfaces]

```
user@host# set interface-name gigether-options 802.3ad atsx
```

---



**NOTE:** The CSE2000 has two service card slots that can accommodate one service card each (ESC0 or ESC1). For both the data plane, the interfaces associated with these cards are represented by a logical interface atsX (where X = 0 or 1). If the service card ESC0 is connected to the PTX Series router, then you use the interface ats0 to represent the service card, whereas if the service card ESC1 is connected, then you use the interface ats1.

---

2. Configure an interface family for the ATS interface bundle.

[edit interfaces]

```
user@host# set atsx unit number family (inet | inet6 | mpls)
```

**Related  
Documentation**

- [Aggregated Tethered Services Interfaces Overview on page 13](#)

---

## Configuring Active Flow Monitoring Version 9 Templates

---

**Supported Platforms**    CSE2000, PTX3000, PTX5000

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.

To activate templates in flow monitoring, you must configure a template and include that template in the version 9 flow monitoring configuration. On PTX5000 or PTX3000 routers with CSE2000, Junos OS supports template configuration for IPv4, IPv6, MPLS, and MPLS-IPv4 traffic.

To configure active flow monitoring version 9:

1. To configure a version 9 template, assign each template a unique name by including the **template *template-name*** statement at the **[edit services flow-monitoring version9]** hierarchy level.

```
[edit services flow-monitoring version9]
user@host# set template template-name
```

2. Configure the active timeout and the inactive timeout values for the flows by including the **flow-active-timeout** and **flow-inactive-timeout** statements at the **[edit services flow-monitoring version9 template *template-name*]** hierarchy level.

- 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.

```
[edit services flow-monitoring version9 template template-name]
user@host# set flow-active-timeout seconds
user@host# set flow-inactive-timeout seconds
```

3. To export the flow records in a template to the flow server, specify each template for the appropriate type of traffic by including the **ipv4-template**, **ipv6-template**, **mpls-template**, or **mpls-ipv4-template** statement at the **[edit services flow-monitoring version9 template *template-name*]** hierarchy level. If the template is used for MPLS traffic, you can also specify label positions for the MPLS header label data by including the **label-position** statement.

```
[edit services flow-monitoring version9 template template-name]
user@host# set ipv4-template
user@host# set ipv6-template
user@host# set mpls-template label-position [ 1 2 ]
user@host# set mpls-ipv4-template label-position [ 1 2 ]
```

4. Configure the rate at which the router sends template definitions and options to the flow server for IPv4, IPv6, or 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 flow server.

```
[edit services flow-monitoring version9 template template-name]
user@host# set template-refresh-rate (packets packets | seconds seconds)
user@host# set option-refresh-rate (packets packets | seconds seconds)
```

- Related Documentation**
- [Example: Configuring Active Flow Monitoring Version 9 for IPv4 on page 24](#)
  - [Example: Configuring Active Flow Monitoring Version 9 for IPv6 on page 38](#)
  - [Example: Configuring Active Flow Monitoring Version 9 for MPLS on page 52](#)
  - [Example: Configuring Active Flow Monitoring Version 9 for MPLS and IPv4 on page 67](#)
  - [Example: Configuring Active Flow Monitoring Version 9 for Simultaneous IPv4, MPLS, and IPv6 Sampling on page 82](#)
  - [Example: Configuring Active Flow Monitoring Version 9 on PTX3000 and PTX5000 When Both Are Tethered to a CSE2000 on page 102](#)

## Configuring a Firewall Filter for Active Flow Monitoring Version 9

---

**Supported Platforms** CSE2000, PTX3000, PTX5000

A firewall filter identifies the traffic flows that need to be sampled and processed by the CSE2000. The first step in active flow monitoring is to configure the match conditions for acceptable traffic. Common match actions for active flow monitoring include **sample** and **accept**. To configure the firewall filter, include the desired action statements and a counter as part of the **then** statement in a firewall filter and apply the filter to an interface.

During sampling, the router reviews a portion of the traffic and sends reports about this sample to the flow monitoring server. Accepted traffic is forwarded to the intended destination.

To configure the firewall filter:

1. Include the **filter** statement and specify the name of the filter at the **[edit firewall]** hierarchy level.

```
[edit firewall]
user@host# set family (inet | inet6 | mpls) filter filter-name
```

2. Configure the match conditions by using the **term** statement and specifying the name of the match condition at the **[edit firewall family (inet | inet6 | mpls) filter *filter-name*]** hierarchy level.

```
[edit firewall family (inet | inet6 | mpls) filter filter-name]
user@host# set term term-name from match-conditions then action
```

3. Apply the firewall filter to the set of media interfaces where traffic flow needs to be sampled at the **[edit interfaces *interface-name*]** hierarchy level.

```
[edit interfaces interface-name]
user@host# set family (inet | inet6 | mpls) filter input filter-name
```

- Related Documentation**
- [family on page 140](#)
  - [filter on page 141](#)

## Configuring Traffic Sampling

**Supported Platforms** CSE2000, PTX3000, PTX5000

Traffic sampling enables you to copy traffic to the CSE2000, which performs flow monitoring 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 on the PTX5000 or the PTX3000 router.

Before configuring the traffic sampling, you must configure member Interfaces and interface family for aggregated tethered services (ATS) interfaces. For more details, see “[Configuring Member Interfaces and Interface Family for Aggregated Tethered Services Interfaces](#)” on page 19.

To configure the sampling instance:

1. Configure the sampling instance at the **[edit forwarding-options]** hierarchy level and specify the sampling rate, the run length, and the maximum packet length.

The sampling rate determines the ratio of the number of packets to be sampled. For example, if you specify a rate of 10, 1 out of every 10 packets is sampled.

The run length sets the number of samples to be taken following the initial trigger event. This enables you to sample packets following those already being sampled.

The maximum packet length sets the maximum length (in bytes) of the packet used for traffic sampling. Packets with length greater than the specified maximum are truncated.

```
[edit forwarding-options]
user@host# set sampling instance instance-name input rate number
user@host# set sampling instance instance-name input run-length number
user@host# set sampling instance instance-name input maximum-packet-length
bytes
```

2. Apply the sampling instance to an FPC.

The FPC number must match the FPC portion of the interface name for the interface on which sampling is enabled. To apply the sampling instance, include the **sampling-instance** statement at the **[edit chassis]** hierarchy level.

```
[edit chassis]
user@host# set fpc slot sampling instance instance-name
```

- Related Documentation**
- [filter on page 141](#)
  - [family on page 140](#)
  - [sampling on page 157](#)

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

**Supported Platforms** CSE2000, PTX3000, PTX5000

Flow records generated from active flow monitoring version 9 are exported to the flow server. To configure the flow server:

1. Include the **flow-server** statement and specify the IPv4 address of the host system at the **[edit forwarding-options sampling instance *instance-name*]** hierarchy level. Also include the **port** statement and specify the UDP port for the flow server.

```
[edit forwarding-options sampling instance instance-name]
user@host# set family (inet | inet6| mpls) output flow-server address port port-number
```

2. Configure the flow server to receive records in version 9 template format.

To configure the flow server to receive records in version 9 template format, include the **version9** statement and specify the template name at the **[edit forwarding-options sampling instance *instance-name* family (inet | inet6| mpls) output flow-server address]** hierarchy level.

```
[edit forwarding-options sampling instance instance-name family (inet | inet6| mpls)
output flow-server address]
user@host# set version9 template template-name
```

3. Configure the interface connected to the flow server by specifying the source address for generating the monitored packets at the **[edit forwarding-options sampling instance *instance-name* family (inet | inet6| mpls) output]** hierarchy level.

```
[edit forwarding-options sampling instance instance-name family (inet | inet6| mpls)
output]
user@host# set interfaces atsx source-address address
```



NOTE:

- The steps to configure the flow server remain the same irrespective of whether the flow server is connected to the PTX Series router through a cloud network or through any other router.
- You can configure a maximum of eight flow servers.

Related Documentation

- [Active Flow Monitoring Version 9 Formats and Fields on page 6](#)
- [flow-active-timeout on page 142](#)
- [flow-inactive-timeout on page 143](#)
- [flow-server on page 144](#)

## Example: Configuring Active Flow Monitoring Version 9 for IPv4

**Supported Platforms** CSE2000, PTX3000, PTX5000

This example shows the configuration of active flow monitoring version 9 for IPv4 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.



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

The example is organized in the following sections:

- [Requirements on page 25](#)
- [Overview and Topology on page 25](#)
- [Configuration on page 27](#)
- [Verification on page 32](#)

## Requirements

This example requires the following hardware and software components:

- One PTX5000 router running Junos OS Release 13.3R4, 14.1R3, 14.2R1, or later
- One CSE2000 running CSE Series Release 13.3R4, 14.1R3, 14.2R1, or later
- Version 9 flow server (to collect sampled flows using the version 9 format)

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

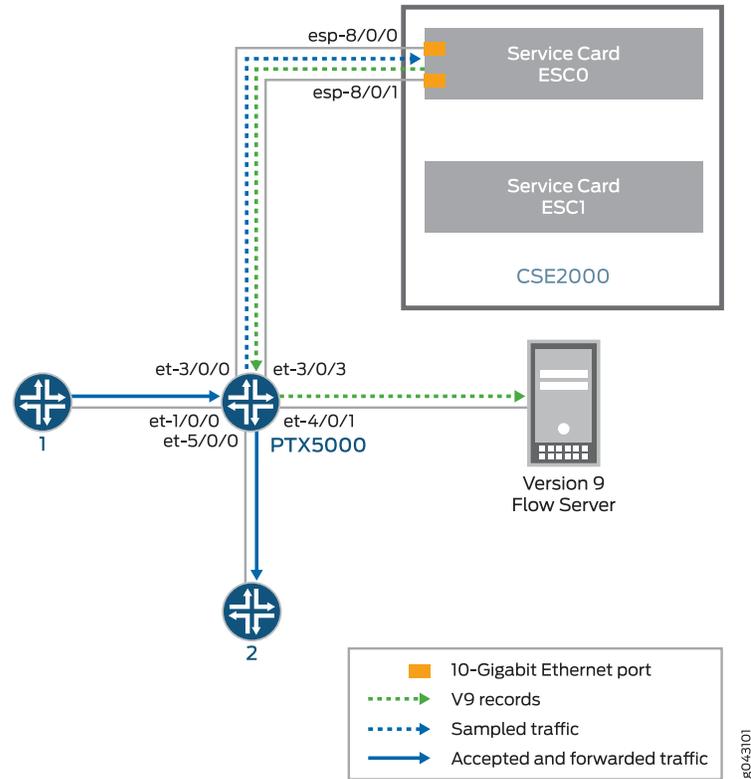
## Overview and Topology

This example shows the configuration of active flow monitoring version 9 for IPv4 on a PTX5000 router that is tethered to a 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 the active flow monitoring version 9 needs to be enabled (see [Figure 8 on page 26](#)). 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 8 on page 26](#).

Figure 8: Active Flow Monitoring Version 9 for IPv4 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 the 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 or esp-16/0/1) to export the active flow monitoring version 9 records to the version 9 flow server.

## Configuration

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

- [Configuring Member Interfaces and Interface Family for Aggregated Tethered Services Interface on page 28](#)
- [Configuring Active Flow Monitoring Version 9 Template for IPv4 Flows on page 28](#)
- [Configuring Firewall Filter on page 29](#)
- [Configuring Traffic Sampling on page 30](#)
- [Configuring Flow Server to Collect the Active Flow Monitoring Version 9 Records on page 30](#)
- [Results on page 31](#)

### 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, and paste the commands into the CLI at the **[edit]** hierarchy level.

```
[edit]
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 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 ipv4-template
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 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 interfaces et-1/0/0 unit 0 family inet filter input ipv4_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 inet output flow-server 192.0.2.2
  version9 template v4_template
set forwarding-options sampling instance ins1 family inet output interface ats0
  source-address 192.0.2.1

```

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

#### 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. Doing so 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 member 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 gigheter-options 802.3ad ats0
user@ptx5000# set et-3/0/3 gigheter-options 802.3ad ats0

```

2. Configure the ats0 interface to process IPv4 addresses by including the **family** statement and specifying the **inet** option at the **[edit interfaces]** hierarchy level.

```

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

```

### Configuring Active Flow Monitoring Version 9 Template for IPv4 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 flows:

1. Create a version 9 template 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. 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]** hierarchy level.
  - 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
```

3. 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
```

4. Configure the rate at which the router sends IPv4 template definitions and options to the flow server. 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 flow server. In this example, the template definitions and options are refreshed every 480 packets.

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

### Configuring 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 a firewall filter:

1. Include the **filter** statement and specify **ipv4\_sample\_filter** as the name of the filter at the **[edit firewall]** 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]** hierarchy level.

```
[edit firewall]
user@ptx5000# set family inet filter ipv4_sample_filter term 1 then count c1
user@ptx5000# set family inet filter ipv4_sample_filter term 1 then sample
user@ptx5000# set family inet filter ipv4_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, 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]** hierarchy level.

```
[edit interfaces et-1/0/0 unit 0]
user@ptx5000# set family inet filter input ipv4_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 Flow Server to Collect the Active Flow Monitoring Version 9 Records

**Step-by-Step Procedure** Active flow monitoring version 9 records generated by the CSE2000 are exported to the flow server.

1. To configure the flow server, 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]` hierarchy level. Also include the `port` statement and specify UDP port 2055 for the flow server.

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

2. Configure the flow server to receive records in version 9 template format.

To configure the flow server to receive records in version 9 template format, include the `version9` statement and specify `v4_template` as the template name 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
```

3. 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 interface ats0 source-address 192.0.2.1
```

## 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;
      }
    }
  }
}
interfaces {
  et-1/0/0 {
    unit 0 {
      family inet {
        filter {
          input ipv4_sample_filter;
        }
      }
    }
  }
  et-3/0/0 {
    gigger-options {
      802.3ad ats0;
    }
  }
  et-3/0/3 {
    gigger-options {
      802.3ad ats0;
    }
  }
  ats0 {
    unit 0 {
      family inet;
    }
  }
}
```

```
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;
            }
          }
        }
      }
    }
  }
}
firewall {
  family inet {
    filter ipv4_sample_filter {
      term 1 {
        then {
          count c1;
          sample;
          accept;
        }
      }
    }
  }
}
```

## Verification

Confirm that the configuration is working properly.

- [Verifying That the Packet Are Received on the Router on page 33](#)
- [Verifying That the Packets Are Matched and Filtered According to the Configuration on page 33](#)
- [Verifying That the ATS Interface Is Forwarding Packets on page 34](#)
- [Verifying That Active Flow Monitoring Is Working on page 34](#)
- [Verifying That the CSE2000 Service Card Is Operational for Active Flow Monitoring on page 35](#)

- [Verifying That Sampling Is Enabled and the Filter Direction Is Correct for Active Flow Monitoring on page 36](#)
- [Verifying That the Sampling Instance Is Applied to the Correct FPC for Active Flow Monitoring on page 37](#)
- [Verifying That the Route Record Is Being Created for Active Flow Monitoring on page 37](#)
- [Verifying That the Sampling Process Is Running for Active Flow Monitoring on page 37](#)
- [Verifying That the TCP Connection Is Operational for Active Flow Monitoring on page 38](#)

### [Verifying That the Packet 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: 0
    Protocol inet, MTU: 1500
      Flags: Sendbcst-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 the interface et-1/0/0 is working fine.

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
```

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

The **Packets** field display 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
  Bundle:
    Input :           4           0           244           0
    Output:          108           0          13392           0
  Protocol inet, MTU: 9536
    Flags: Sendbroadcast-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 shows that the ats0 interface is forwarding the packets (**Output** field) to 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	AMBOWKG	SFP+-10G-SR
Xcvr 12	REV 01	740-031980	B11J04031	SFP+-10G-SR
Xcvr 13	REV 01	740-031980	AMBOTD9	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 shows that CSE2000 service card ESC 0 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: 2, CAM source filters: 0
Input Filters: ipv4_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 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**
- [Flow Monitoring Using CSE2000 Overview on page 3](#)
  - [Example: Configuring Active Flow Monitoring Version 9 for MPLS and IPv4 on page 67](#)
  - [Example: Configuring Active Flow Monitoring Version 9 for Simultaneous IPv4, MPLS, and IPv6 Sampling on page 82](#)
  - [Example: Configuring Active Flow Monitoring Version 9 on PTX3000 and PTX5000 When Both Are Tethered to a CSE2000 on page 102](#)

## Example: Configuring Active Flow Monitoring Version 9 for IPv6

**Supported Platforms** CSE2000, PTX3000, PTX5000

This example shows the configuration of active flow monitoring version 9 for IPv6 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.



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

The example is organized in the following sections:

- [Requirements on page 39](#)
- [Overview and Topology on page 39](#)
- [Configuration on page 41](#)
- [Verification on page 46](#)

## Requirements

This example requires the following hardware and software components:

- One PTX5000 router running Junos OS Release 13.3R4, 14.1R3, 14.2R1, or later
- One CSE2000 running CSE Series Release 13.3R4, 14.1R3, 14.2R1, or later
- Version 9 flow server (to collect sampled flows using the version 9 format)

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

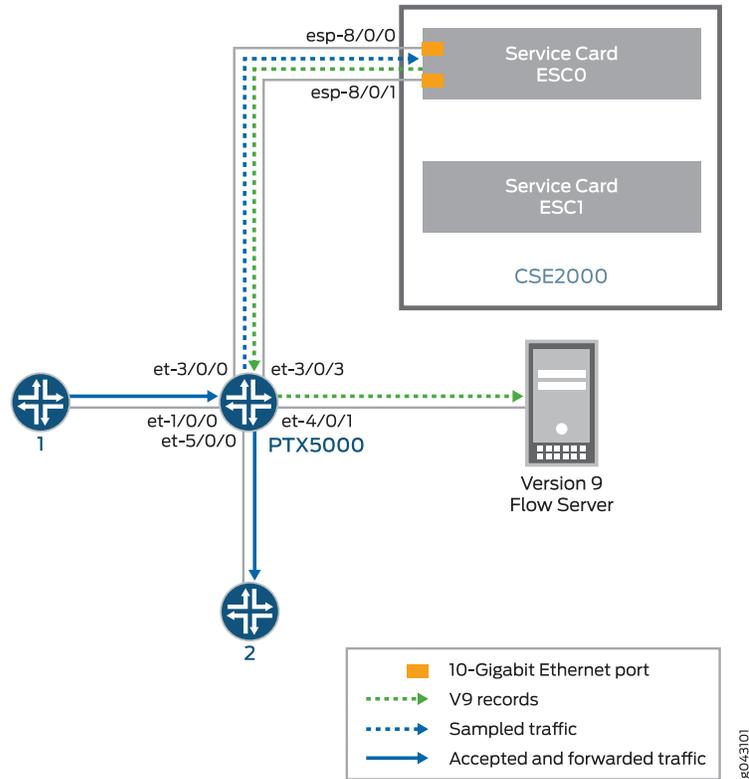
## Overview and Topology

This example shows the configuration of active flow monitoring version 9 for IPv6 on a PTX5000 router that is tethered to a 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 the active flow monitoring version 9 needs to be enabled (see [Figure 9 on page 40](#)). 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 9 on page 40](#).

Figure 9: Active Flow Monitoring Version 9 for IPv6 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 the 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 or esp-16/0/1) to export the active flow monitoring version 9 records.

## Configuration

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

- [Configuring Member Interfaces and Interface Family for Aggregated Tethered Services Interfaces on page 42](#)
- [Configuring Active Flow Monitoring Version 9 Template for IPv6 Flows on page 42](#)
- [Configuring Firewall Filter on page 43](#)
- [Configuring Traffic Sampling on page 44](#)
- [Configuring 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, and paste the commands into the CLI at the **[edit]** hierarchy level.

```
[edit]
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 inet6
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 ipv6-template
set services flow-monitoring version9 template v46_template template-refresh-rate
  packets 480
set services flow-monitoring version9 template v6_template option-refresh-rate packets
  480
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 interfaces et-1/0/0 unit 0 family inet6 filter input ipv6_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 inet6 output flow-server 192.0.2.2
  port 2055
set forwarding-options sampling instance ins1 family inet6 output flow-server 192.0.2.2
  version9 template v4_template
set forwarding-options sampling instance ins1 family inet6 output interface ats0
  source-address 192.0.2.1

```

### Configuring 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. Doing so 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 member 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 gigheter-options 802.3ad ats0
user@ptx5000# set et-3/0/3 gigheter-options 802.3ad ats0

```

2. Configure the ats0 interface to process IPv6 addresses by including the **family** statement and specifying the **inet** option at the **[edit interfaces]** hierarchy level.

```

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

```

### Configuring Active Flow Monitoring Version 9 Template for IPv6 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 IPv6 flows:

1. Create a version 9 template 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

```

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 v6\_template]** hierarchy level.
  - 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 v6_template]
user@ptx5000# set flow-active-timeout 60
user@ptx5000# set flow-inactive-timeout 30
```

3. 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
```

4. Configure the rate at which the router sends IPv6 template definitions and options to the flow server for IPv6 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 flow server. In this example, the template definitions and options are refreshed for every 480 packets.

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

### Configuring 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 a firewall filter:

1. Include the `filter` statement and specify `ipv6_sample_filter` as the name of the filter at the `[edit firewall]` 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]` hierarchy level.

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

2. Apply the firewall filter to the set of media interfaces 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, 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]` hierarchy level.

```
[edit interfaces et-1/0/0 unit 0]
user@ptx5000# set family inet6 filter input ipv6_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 Flow Server to Collect the Active Flow Monitoring Version 9 Records

**Step-by-Step Procedure** Active flow monitoring version 9 records generated by the CSE2000 are exported to the flow server.

1. To configure the flow server, 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]` hierarchy level. Also include the port statement and specify UDP port 2055 for the flow server.

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

2. Configure the flow server to receive records in version 9 template format.

To configure the flow server to receive records in version 9 template format, include the `version9` statement and specify `v6_template` as the template name 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
```

3. 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 interface ats0 source-address 192.0.2.1
```

## Results

Display the results of the configuration.

```
user@ptx5000> show configuration
chassis {
  fpc 1 {
    sampling-instance ins1;
  }
}
services {
  flow-monitoring {
    version9 {
      template v6_template {
        flow-active-timeout 60;
        flow-inactive-timeout 30;
        template-refresh-rate {
          packets 480;
        }
        option-refresh-rate {
          packets 480;
        }
        ipv6-template;
      }
    }
  }
}
interfaces {
  et-1/0/0 {
    unit 0 {
      family inet6 {
        filter {
          input ipv6_sample_filter;
        }
      }
    }
  }
  et-3/0/0 {
    gige-ether-options {
      802.3ad ats0;
    }
  }
  et-3/0/3 {
    gige-ether-options {
      802.3ad ats0;
    }
  }
  ats0 {
    unit 0 {
      family inet6;
    }
  }
}
```

```
forwarding-options {
  sampling {
    instance {
      ins1 {
        input {
          rate 10;
          run-length 1;
          maximum-packet-length 128;;
        }
        family inet6 {
          output {
            flow-server 192.0.2.2 {
              port 2055;
              version9 {
                template {
                  v6_template;
                }
              }
            }
            interface ats0 {
              source-address 192.0.2.1;
            }
          }
        }
      }
    }
  }
}
firewall {
  family inet6 {
    filter ipv6_sample_filter {
      term 1 {
        then {
          count c1;
          sample;
          accept;
        }
      }
    }
  }
}
```

## Verification

Confirm that the configuration is working properly.

- [Verifying That the Packet Are Received on the Router on page 47](#)
- [Verifying That the Packets Are Matched and Filtered According to the Configuration on page 47](#)
- [Verifying That the ATS Interface Is Forwarding Packets on page 48](#)
- [Verifying That Active Flow Monitoring Is Working on page 48](#)
- [Verifying That the CSE2000 Service Card Is Operational for Active Flow Monitoring on page 49](#)

- [Verifying That Sampling Is Enabled and the Filter Direction Is Correct for Active Flow Monitoring on page 50](#)
- [Verifying That the Sampling Instance Is Applied to the Correct FPC for Active Flow Monitoring on page 51](#)
- [Verifying That the Route Record Is Being Created for Active Flow Monitoring on page 51](#)
- [Verifying That the Sampling Process Is Running for Active Flow Monitoring on page 51](#)
- [Verifying That the TCP Connection Is Operational for Active Flow Monitoring on page 52](#)

### [Verifying That the Packet 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: 0
    Protocol inet, MTU: 1500
      Flags: Sendbcst-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 the interface et-1/0/0 is working fine.

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: ipv6_sample_filter
Counters:
Name                Bytes          Packets
c1                  11880          108
```

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

The **Packets** field display 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
  Bundle:
    Input :           4           0           244           0
    Output:          108           0          13392           0
  Protocol inet, MTU: 9536
    Flags: Sendbcst-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 shows that the ats0 interface is forwarding the packets (**Output** field) to 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	AMBOWKG	SFP+-10G-SR
Xcvr 12	REV 01	740-031980	B11J04031	SFP+-10G-SR
Xcvr 13	REV 01	740-031980	AMBOTD9	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 shows that CSE2000 service card ESC 0 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: 2, CAM source filters: 0
Input Filters: ipv6_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 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**
- [Example: Configuring Active Flow Monitoring Version 9 for Simultaneous IPv4, MPLS, and IPv6 Sampling on page 82](#)
  - [Example: Configuring Active Flow Monitoring Version 9 for IPv4 on page 24](#)

## Example: Configuring Active Flow Monitoring Version 9 for MPLS

**Supported Platforms** `CSE2000, PTX3000, PTX5000`

This example shows the configuration of active flow monitoring version 9 for MPLS 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.



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

The example is organized in the following sections:

- [Requirements on page 53](#)
- [Overview and Topology on page 53](#)
- [Configuration on page 55](#)
- [Verification on page 60](#)

## Requirements

This example requires the following hardware and software components:

- One PTX5000 router running Junos OS Release 13.3R4, 14.1R3, 14.2R1, or later
- One CSE2000 running CSE Series Release 13.3R4, 14.1R3, 14.2R1, or later
- Version 9 flow server (to collect sampled flows using the version 9 format)

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

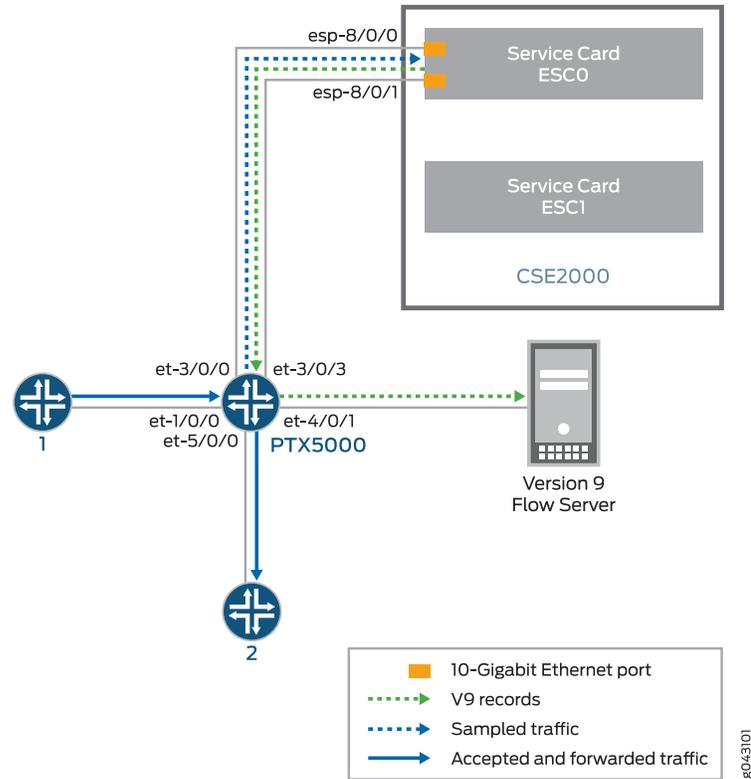
## Overview and Topology

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

The topology for this example consists of a PTX5000 router on which the active flow monitoring version 9 needs to be enabled (see [Figure 10 on page 54](#)). 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 10 on page 54](#).

Figure 10: Active Flow Monitoring Version 9 for 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 the 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 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 or esp-16/0/1) to export the active flow monitoring version 9 records.

## Configuration

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

- [Configuring Member Interfaces and Interface Family for Aggregated Tethered Services Interfaces on page 56](#)
- [Configuring Active Flow Monitoring Version 9 for MPLS Flows on page 56](#)
- [Configuring Firewall Filter on page 57](#)
- [Configuring Traffic Sampling on page 58](#)
- [Configuring Flow Server to Collect the Active Flow Monitoring Version 9 Records on page 58](#)
- [Results on page 59](#)

### 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, and paste the commands into the CLI at the **[edit]** hierarchy level.

```
[edit]
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 mpls
set services flow-monitoring version9 template mpls
set services flow-monitoring version9 template mpls mpls-template label-position [ 1 2
]
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 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 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 mpls output flow-server 192.0.2.2
  port 2055
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 mpls output interface ats0
  source-address 192.0.2.1

```

### Configuring 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. Doing so 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 gigheter-options 802.3ad ats0
user@ptx5000# set et-3/0/3 gigheter-options 802.3ad ats0

```

2. Configure the ats0 interface to process MPLS addresses by including the **family** statement and specifying the **mpls** option at the **[edit interfaces]** hierarchy level.

```

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

```

### Configuring Active Flow Monitoring Version 9 for MPLS Flows

#### Step-by-Step Procedure

1. Create a version 9 template 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. 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]** hierarchy level.

The **label-position** statement allows selection of up to three label positions in the label stack to be exported as part of the flow record. In this example, the label positions selected are 1 and 2.

```

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

```

3. 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 mpls]** hierarchy level.
  - 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 mpls]
user@ptx5000# set flow-active-timeout 60
user@ptx5000# set flow-inactive-timeout 30
```

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

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

### Configuring 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 a firewall filter:

1. Include the **filter** statement and specify `mpls_sample_filter` as the name of the filter at the **[edit firewall]** 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]** hierarchy level.

```
[edit firewall]
user@ptx5000# set family mpls filter mpls_sample_filter term 1 then count c1
user@ptx5000# set family mpls filter mpls_sample_filter term 1 then sample
user@ptx5000# set family mpls 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, 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]** hierarchy level.

```
[edit interfaces et-1/0/0 unit 0]
```

```
user@ptx5000# set family mpls filter 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 Flow Server to Collect the Active Flow Monitoring Version 9 Records

#### Step-by-Step Procedure

Active flow monitoring version 9 records generated by the CSE2000 are exported to the flow server.

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

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

2. Configure the flow server to receive records in version 9 template format.

To configure the flow server to receive records in version 9 template format, include the `version9` statement and specify `mpls` as the template name 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 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 interface ats0 source-address 192.0.2.1
```

## Results

Display the results of the configuration.

```
user@ptx5000> show configuration
chassis {
  fpc 1 {
    sampling-instance ins1;
  }
}
services {
  flow-monitoring {
    version9 {
      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 mpls {
        filter {
          input mpls_sample_filter;
        }
      }
    }
  }
  et-3/0/0 {
    gige-ether-options {
      802.3ad ats0;
    }
  }
  et-3/0/3 {
    gige-ether-options {
      802.3ad ats0;
    }
  }
  ats0 {
    unit 0 {
      family mpls;
    }
  }
}
```



- [Verifying That the CSE2000 Service Card Is Operational for Active Flow Monitoring on page 63](#)
- [Verifying That Sampling Is Enabled and the Filter Direction Is Correct for Active Flow Monitoring on page 65](#)
- [Verifying That the Sampling Instance Is Applied to the Correct FPC for Active Flow Monitoring on page 65](#)
- [Verifying That the Route Record Is Being Created for Active Flow Monitoring on page 66](#)
- [Verifying That the Sampling Process Is Running for Active Flow Monitoring on page 66](#)
- [Verifying That the TCP Connection Is Operational for Active Flow Monitoring on page 66](#)

### Verifying That the Packet 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: 0
    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 the interface et-1/0/0 is working fine.

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: mpls_sample_filter
Counters:
Name                               Bytes           Packets
c1                                  11880           108
```

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

The **Packets** field display 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 :      4      0      244      0
  Output:    108      0    13392      0
  Protocol inet, MTU: 9536
  Flags: Sendbcst-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 shows that the ats0 interface is forwarding the packets (**Output** field) to 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              REV 11   750-035893  JN11FF811AJA  PTX5000
Midplane             REV 12   760-030647  BBAX0093      Midplane-8S
FPM                  Rev 07   740-032019  1E002220031  Front Panel Display
PDU 0                Rev 06   740-032022  1E002280079  DC Power Dist Unit
  PSM 0               Rev 06   740-032022  1E002280070  DC 12V Power Supply
  PSM 1               Rev 06   740-032022  1E002280080  DC 12V Power Supply
  PSM 2               Rev 06   740-032022  1E002280069  DC 12V Power Supply
  PSM 3               Rev 07   740-032019  1E002220052  DC 12V Power Supply
PDU 1                Rev 06   740-032022  1E002280040  DC Power Dist Unit
  PSM 0               Rev 06   740-032022  1E002280071  DC 12V Power Supply
  PSM 2               Rev 10   740-026942  P737A-003458  DC 12V Power Supply
Routing Engine 0    REV 10   740-026942  P737A-003388  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  AMBOWKG       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 shows that CSE2000 service card ESC 0 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: 2, CAM source filters: 0
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 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

- [Example: Configuring Active Flow Monitoring Version 9 for MPLS and IPv4 on page 67](#)
- [Example: Configuring Active Flow Monitoring Version 9 for Simultaneous IPv4, MPLS, and IPv6 Sampling on page 82](#)

## Example: Configuring Active Flow Monitoring Version 9 for MPLS and IPv4

**Supported Platforms** CSE2000, PTX3000, PTX5000

This example shows the configuration of active flow monitoring version 9 for IPv4 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.



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

The example is organized in the following sections:

- [Requirements on page 67](#)
- [Overview and Topology on page 68](#)
- [Configuration on page 69](#)
- [Verification on page 76](#)

## Requirements

This example requires the following hardware and software components:

- One PTX5000 router running Junos OS Release 13.3R4, 14.1R3, 14.2R1, or later
- One CSE2000 running CSE Series Release 13.3R4, 14.1R3, 14.2R1, or later
- Version 9 flow server (to collect sampled flows using the version 9 format)

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

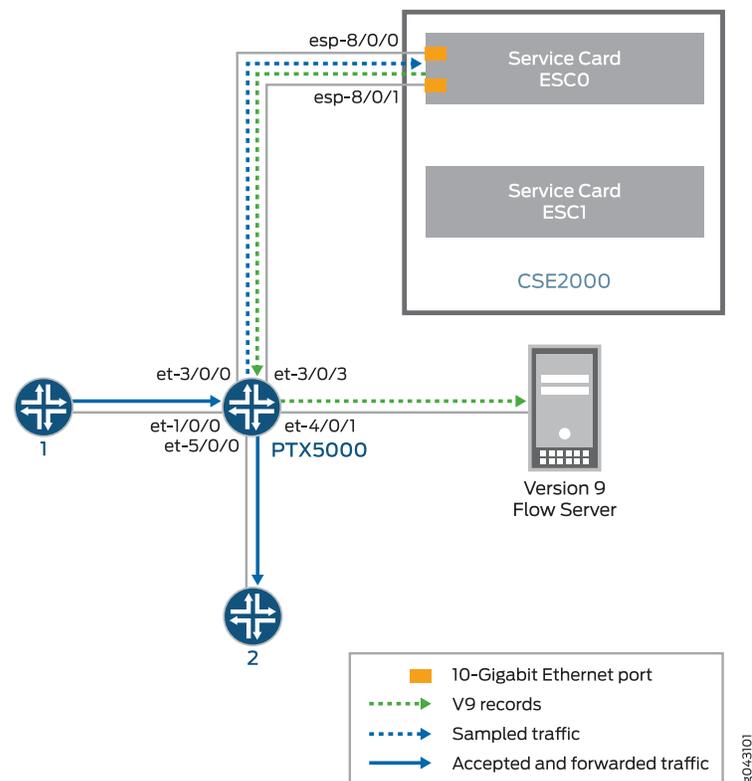
## Overview and Topology

This example shows the configuration of active flow monitoring version 9 for IPv4 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 the active flow monitoring version 9 needs to be enabled (see [Figure 11 on page 68](#)). 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 11 on page 68](#).

**Figure 11: Active Flow Monitoring Version 9 for MPLS and IPv4 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 the 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 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` or `esp-16/0/1`) to export the active flow monitoring version 9 records.

## Configuration

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

- [Configuring Member Interfaces and Interface Family for Aggregated Tethered Services Interfaces on page 70](#)
- [Configuring Active Flow Monitoring Version 9 Template for IPv4 and MPLS Flows on page 71](#)
- [Configuring Firewall Filter on page 72](#)
- [Configuring Traffic Sampling on page 73](#)
- [Configuring Flow Server to Collect the Active Flow Monitoring Version 9 Records on page 73](#)
- [Results on page 74](#)

### 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, and paste the commands into the CLI at the `[edit]` hierarchy level.

```
[edit]
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 mpls
set services flow-monitoring version9 template mpls-ipv4
set services flow-monitoring version9 template mpls-ipv4 mpls-ipv4-template
  label-position [ 1 2 ]
set services flow-monitoring version9 template mpls-ipv4 flow-active-timeout 60
set services flow-monitoring version9 template mpls-ipv4 flow-inactive-timeout 30
```

```

set services flow-monitoring version9 template mpls-ipv4 template-refresh-rate packets
  480
set services flow-monitoring version9 template mpls-ipv4 option-refresh-rate packets
  480
set firewall family mpls filter ipv4_sample_filter term 1 then count c1
set firewall family mpls filter ipv4_sample_filter term 1 then sample
set firewall family mpls filter ipv4_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 ipv4 filter input ipv4_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 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 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 mpls output interface ats0
  source-address 192.0.2.1

```

### Configuring 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. Doing so 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 gigger-options 802.3ad ats0
user@ptx5000# set et-3/0/3 gigger-options 802.3ad ats0

```

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

```

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

```

## Configuring Active Flow Monitoring Version 9 Template for IPv4 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 and MPLS flows:

1. Create a version 9 template by including the **flow-monitoring version9 template** statement and specifying `mpls-ipv4` as the name of the template at the **[edit services]** hierarchy level.

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

2. Enable the template for MPLS and IPv4 flows by including the **mpls-ipv4-template** statement at the **[edit services flow-monitoring version9 template mpls-ipv4]** hierarchy level. Also include the **label-position** statement and specify label positions 1 and 2 at the **[edit services flow-monitoring version9 template mpls-ipv4 mpls-ipv4-template]** hierarchy level.

The **label-position** statement allows selection of up to three label positions in the label stack to be exported as part of the flow record. In this example, the label positions selected are 1 and 2.

```
[edit services flow-monitoring version9 template mpls-ipv4]
user@ptx5000# set mpls-ipv4-template label-position [ 1 2 ]
```

3. 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 mpls-ipv4]** hierarchy level.
  - 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 mpls-ipv4]
user@ptx5000# set flow-active-timeout 60
user@ptx5000# set flow-inactive-timeout 30
```

4. Configure the rate at which the router sends IPv4 and MPLS template definitions and options to the flow server. 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 flow server. In this example, the template definitions and options are refreshed for every 480 packets.

```
[edit services flow-monitoring version9 template mpls-ipv4]
user@ptx5000# set template-refresh-rate packets 480
user@ptx5000# set option-refresh-rate packets 480
```

## Configuring 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:

- 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 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
```

- Apply the firewall filter to the set of media interfaces 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 `mpls_sample_filter` as the name of the filter at the **[edit interfaces et-1/0/0 unit 0]** hierarchy level.

```
[edit interfaces et-1/0/0 unit 0]
user@ptx5000# set family inet filter input ipv4_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]** hierarchy level.

```
[edit interfaces et-1/0/0 unit 0]
user@ptx5000# set family mpls filter 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 Flow Server to Collect the Active Flow Monitoring Version 9 Records

### Step-by-Step Procedure

Active flow monitoring version 9 records generated by the CSE2000 are exported to the flow server.

1. Configure the flow server for IPv4 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]
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 using version 9 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 by using the version 9 template format for IPv4 flows, include the `version9 template` statement and specify `inet` 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 by using the version 9 template format for MPLS flows, 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 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
```

## Results

Display the results of the configuration.

```
user@ptx5000> show configuration
chassis {
  fpc 1 {
    sampling-instance ins1;
  }
}
services {
  flow-monitoring {
    version9 {
      template mpls_ipv4 {
        flow-active-timeout 60;
        flow-inactive-timeout 30;
        mpls-ipv4-template {
          label-position [ 1 2 ];
        }
        template-refresh-rate {
          packets 480;
        }
      }
      option-refresh-rate {
        packets 480;
      }
    }
  }
}
```



```
        output {
            flow-server 192.0.2.2 {
                port 2055;
                version9 {
                    template mpls;
                }
            }
            interface ats0 {
                source-address 192.0.2.1;
            }
        }
    }
}
firewall {
    family inet {
        filter ipv4_sample_filter {
            term 1 {
                then {
                    count c1;
                    sample;
                    accept;
                }
            }
        }
    }
    family mpls {
        filter mpls_v4_sample_filter {
            term 1 {
                then {
                    count c1;
                    sample;
                    accept;
                }
            }
        }
    }
}
```

## Verification

Confirm that the configuration is working properly.

- [Verifying That the Packet Are Received on the Router on page 77](#)
- [Verifying That the Packets Are Matched and Filtered According to the Configuration on page 77](#)
- [Verifying That the ATS Interface Is Forwarding Packets on page 78](#)
- [Verifying That Active Flow Monitoring Is Working on page 79](#)
- [Verifying That the CSE2000 Service Card Is Operational for Active Flow Monitoring on page 79](#)

- [Verifying That Sampling Is Enabled and the Filter Direction Is Correct for Active Flow Monitoring on page 80](#)
- [Verifying That the Sampling Instance Is Applied to the Correct FPC for Active Flow Monitoring on page 81](#)
- [Verifying That the Route Record Is Being Created for Active Flow Monitoring on page 81](#)
- [Verifying That the Sampling Process Is Running for Active Flow Monitoring on page 82](#)
- [Verifying That the TCP Connection Is Operational for Active Flow Monitoring on page 82](#)

### [Verifying That the Packet 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: 0
    Protocol inet, MTU: 1500
      Flags: Sendbroadcast-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 the interface et-1/0/0 is working fine.

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: mpls_sample_filter
Counters:
Name                Bytes                Packets
c1                  11880                108

```

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

The **Packets** field display 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  :             4             0             244             0
  Output :            108             0            13392             0
Protocol inet, MTU: 9536
Flags: Sendbcst-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 shows that the ats0 interface is forwarding the packets (**Output** field) to 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  AMBOWKG       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 shows that CSE2000 service card ESC 0 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: 2, CAM source filters: 0
Input Filters: ipv4_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 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

- [Example: Configuring Active Flow Monitoring Version 9 for MPLS on page 52](#)
- [Example: Configuring Active Flow Monitoring Version 9 for Simultaneous IPv4, MPLS, and IPv6 Sampling on page 82](#)

## Example: Configuring Active Flow Monitoring Version 9 for Simultaneous IPv4, MPLS, and IPv6 Sampling

**Supported Platforms** CSE2000, PTX3000, PTX5000

This example shows the configuration of 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.



**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 is organized in the following sections:

- [Requirements on page 83](#)
- [Overview and Topology on page 83](#)
- [Configuration on page 85](#)
- [Verification on page 95](#)

## Requirements

This example requires the following hardware and software components:

- One PTX5000 router running Junos OS Release 13.3R4, 14.1R3, 14.2R1, or later
- One CSE2000 running CSE Series Release 13.3R4, 14.1R3, 14.2R1, or later
- Version 9 flow server (to collect sampled flows using the version 9 format)

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

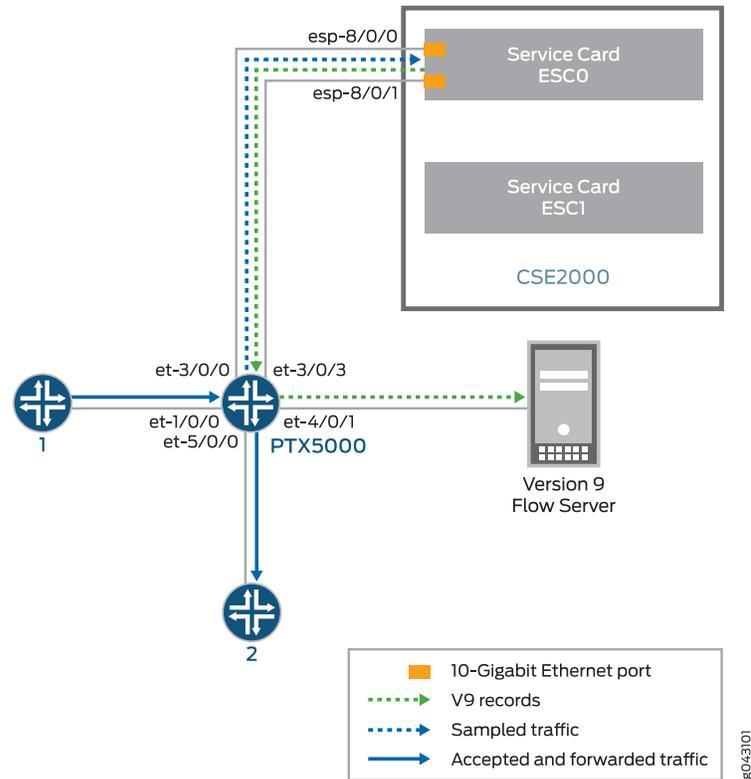
## Overview and Topology

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 the active flow monitoring version 9 needs to be enabled (see [Figure 12 on page 84](#)). 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 12 on page 84](#).

Figure 12: 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 the 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 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 or 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:

- [Configuring Member Interfaces and Interface Family for Aggregated Tethered Services Interfaces on page 87](#)
- [Configuring Active Flow Monitoring Version 9 Template for IPv4, MPLS, and IPv6 Flows on page 87](#)
- [Configuring Firewall Filter on page 89](#)
- [Configuring Traffic Sampling on page 90](#)
- [Configuring Flow Server to Collect the Active Flow Monitoring Version 9 Records on page 91](#)
- [Results on page 92](#)

### 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, and paste the commands into the CLI at the **[edit]** hierarchy level.

```
[edit]
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 firewall family mpls filter ipv4_sample_filter term 1 then count c1
set firewall family mpls filter ipv4_sample_filter term 1 then sample
set firewall family mpls filter ipv4_sample_filter term 1 then accept
set firewall family mpls filter ipv6_sample_filter term 1 then count c1
set firewall family mpls filter ipv6_sample_filter term 1 then sample
set firewall family mpls 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 inet6 output interface ats0
  source-address 192.0.2.1
set forwarding-options sampling instance ins1 family mpls output interface ats0
  source-address 192.0.2.1
```

### Configuring 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. Doing so 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 gigheter-options 802.3ad ats0
user@ptx5000# set et-3/0/3 gigheter-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 Active Flow Monitoring Version 9 Template for IPv4, MPLS, and IPv6 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 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 Flow Server to Collect the Active Flow Monitoring Version 9 Records

#### Step-by-Step Procedure

- 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
```
- 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
```

## 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;
    }
  }
}
```



```
    }
    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;
          }
        }
      }
    }
    family inet6 {
      output {
        flow-server 192.0.2.2 {
          port 2055;
          version9 {
            template {
              v6_template;
            }
          }
        }
      }
      interface ats0 {
        source-address 192.0.2.1;
      }
    }
  }
  family mpls {
    output {
      flow-server 192.0.2.2 {
        port 2055;
        version9 {
          template {
            mpls;
          }
        }
      }
    }
  }
}
```



- [Verifying That the ATS Interface Is Forwarding Packets on page 97](#)
- [Verifying That Active Flow Monitoring Is Working on page 98](#)
- [Verifying That the CSE2000 Service Card Is Operational for Active Flow Monitoring on page 98](#)
- [Verifying That Sampling Is Enabled and the Filter Direction Is Correct for Active Flow Monitoring on page 100](#)
- [Verifying That the Sampling Instance Is Applied to the Correct FPC for Active Flow Monitoring on page 100](#)
- [Verifying That the Route Record Is Being Created for Active Flow Monitoring on page 101](#)
- [Verifying That the Sampling Process Is Running for Active Flow Monitoring on page 101](#)
- [Verifying That the TCP Connection Is Operational for Active Flow Monitoring on page 101](#)

### Verifying That the Packet 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: 0
    Protocol inet, MTU: 1500
      Flags: Sendbcst-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 the interface et-1/0/0 is working fine.

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 display 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  :           4           0           244           0
    Output :          108           0          13392           0
  Protocol inet, MTU: 9536
  Flags: Sendbcst-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 shows that the ats0 interface is forwarding the packets (**Output** field) to 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              REV 11   750-035893  JN11FF811AJA  PTX5000
Midplane             REV 12   760-030647  BBAX0093      Front Panel Display
FPM                  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  BBAX8988      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  BBAX8899      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  AMBOWKG       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 shows that CSE2000 service card ESC 0 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 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

- [Example: Configuring Active Flow Monitoring Version 9 for IPv4 on page 24](#)
- [Example: Configuring Active Flow Monitoring Version 9 for IPv6 on page 38](#)
- [Example: Configuring Active Flow Monitoring Version 9 for MPLS on page 52](#)
- [Example: Configuring Active Flow Monitoring Version 9 for MPLS and IPv4 on page 67](#)
- [Example: Configuring Active Flow Monitoring Version 9 on PTX3000 and PTX5000 When Both Are Tethered to a CSE2000 on page 102](#)

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

**Supported Platforms** [CSE2000](#), [PTX3000](#), [PTX5000](#)

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.

This example is organized in the following sections:

- [Requirements on page 102](#)
- [Overview and Topology on page 103](#)
- [Configuring Active Flow Monitoring Version 9 on PTX5000 Router on page 104](#)
- [Configuring Active Flow Monitoring Version 9 on PTX3000 Router on page 115](#)
- [Verification on page 126](#)

### Requirements

This example requires the following hardware and software components:

- One PTX5000 router running Junos OS Release 13.3R4, 14.1R3, 14.2R1, or later
- One PTX3000 router running Junos OS Release 13.3R4, 14.1R3, 14.2R1, or later

- One CSE2000 running CSE Series Release 13.3R4, 14.1R3, 14.2R1, or later
- Version 9 flow server (to collect sampled flows using the version 9 format)

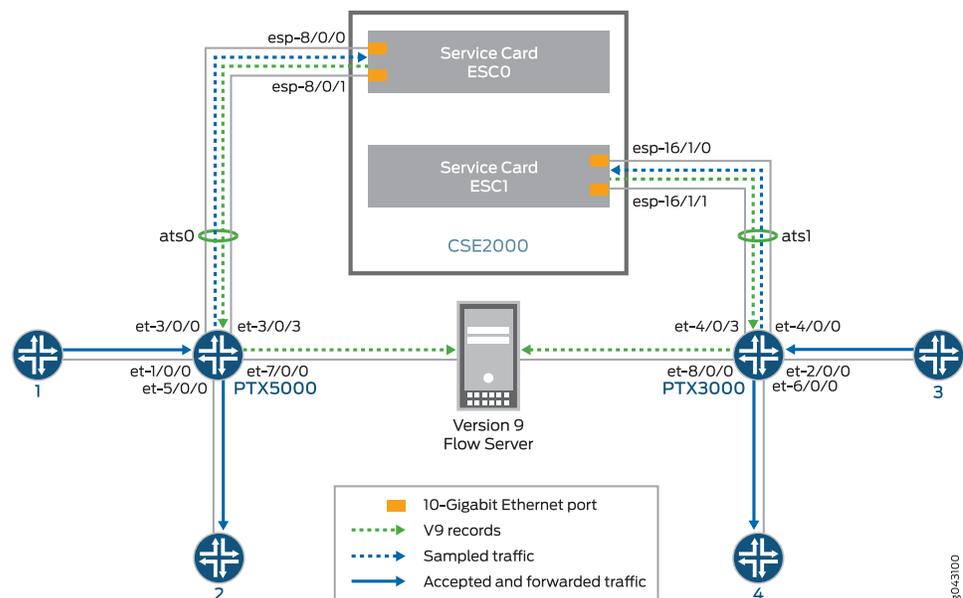
Before you configure the active flow monitoring version 9, connect the CSE2000 to the PTX5000 router and the PTX3000 router. For more information, see the *CSE2000 Hardware Installation Guide*.

## 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 router.

The topology for this example consists of a PTX5000 router and a PTX3000 router on which the active flow monitoring version 9 needs to be enabled (see [Figure 13 on page 103](#)). These routers are tethered to a CSE2000 device.

**Figure 13: 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 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 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 the 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 the 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 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 the 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 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 13 on page 103](#).

## Configuring Active Flow Monitoring Version 9 on 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:

- [Configuring Member Interfaces and Interface Family for Aggregated Tethered Services Interfaces on page 106](#)
- [Configuring Active Flow Monitoring Version 9 Template for IPv4, MPLS, and IPv6 Flows on page 107](#)
- [Configuring Firewall Filter on page 109](#)
- [Configuring Traffic Sampling on page 110](#)
- [Configuring Flow Server to Collect the Active Flow Monitoring Version 9 Records on page 110](#)
- [Results on page 112](#)

### 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, and paste the commands into the CLI at the **[edit]** hierarchy level.

```
[edit]
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 firewall family mpls filter ipv4_sample_filter term 1 then count c1
set firewall family mpls filter ipv4_sample_filter term 1 then sample
set firewall family mpls filter ipv4_sample_filter term 1 then accept
set firewall family mpls filter ipv6_sample_filter term 1 then count c1
set firewall family mpls filter ipv6_sample_filter term 1 then sample
set firewall family mpls 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 inet6 output interface ats0
  source-address 192.0.2.1

```

```
set forwarding-options sampling instance ins1 family mpls output interface ats0
source-address 192.0.2.1
```

### Configuring 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. Doing so 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 gigeother-options 802.3ad ats0
user@ptx5000# set et-3/0/3 gigeother-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 Active Flow Monitoring Version 9 Template for IPv4, MPLS, and IPv6 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.

- 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
```

```
[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
```
- 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 Firewall Filter

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

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 Flow Server to Collect the Active Flow Monitoring Version 9 Records

### Step-by-Step Procedure

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
```

- 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
```

- 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
```

## 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 {
  gigeother-options {
    802.3ad ats0;
  }
}
et-3/0/3 {
  gigeother-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 {
```



```

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 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 Member Interfaces and Interface Family for Aggregated Tethered Services Interfaces on page 117](#)
- [Configuring Active Flow Monitoring Version 9 Template for IPv4, MPLS, and IPv6 Flows on page 118](#)
- [Configuring Firewall Filter on page 120](#)
- [Configuring Traffic Sampling on page 121](#)
- [Configuring Flow Server to Collect the Active Flow Monitoring Version 9 Records on page 121](#)
- [Results on page 123](#)

### 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, and paste the commands into the CLI at the **[edit]** hierarchy level.

```

[edit]
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 mpls mpls-template label-position [ 1 2
  ]
set firewall family mpls filter ipv4_sample_filter term 1 then count c1
set firewall family mpls filter ipv4_sample_filter term 1 then sample
set firewall family mpls filter ipv4_sample_filter term 1 then accept
set firewall family mpls filter ipv6_sample_filter term 1 then count c1
set firewall family mpls filter ipv6_sample_filter term 1 then sample
set firewall family mpls 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 inet6 output interface ats1
  source-address 192.0.2.1
set forwarding-options sampling instance ins1 family mpls output interface ats1
  source-address 192.0.2.1
```

## Configuring 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. Doing so 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 Active Flow Monitoring Version 9 Template for IPv4, MPLS, and IPv6 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.

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 Firewall Filter

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

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 Flow Server to Collect the Active Flow Monitoring Version 9 Records

#### Step-by-Step Procedure

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
```

## 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 {
  gigeother-options {
    802.3ad ats1;
  }
}
et-4/0/3 {
  gigeother-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 {
```



```
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 on page 126](#)
- [Verifying That the Packets Are Matched and Filtered According to the Configuration on page 128](#)
- [Verifying That the ATS Interface Is Forwarding Packets on page 129](#)
- [Verifying That Active Flow Monitoring Is Working on page 131](#)
- [Verifying That the CSE2000 Service Cards Are Operational on page 131](#)
- [Verifying That Sampling Is Enabled and the Filter Direction Is Correct for Active Flow Monitoring on page 133](#)
- [Verifying That the Sampling Instance Is Applied to the Correct FPC for Active Flow Monitoring on page 134](#)
- [Verifying That the Route Record Is Being Created for Active Flow Monitoring on page 134](#)
- [Verifying That the Sampling Process Is Running for Active Flow Monitoring on page 135](#)
- [Verifying That the TCP Connection Is Operational for Active Flow Monitoring on page 135](#)

### Verifying That the Packets Are Received on the Routers

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

**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: 0
    Protocol inet, MTU: 1500
      Flags: Sendbroadcast-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 : 0
  Active alarms  : None
  Active defects : None
  PCS statistics
    Bit errors          Seconds
    Errored blocks     3
  Interface transmit statistics: Disabled

```

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

- 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 the PTX3000 router indicates that the interfaces on the routers are receiving packets.

- Input packets : 108
- Input packets : 130

### 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  :             4             0           244            0
    Output :            108             0          13392            0
  Protocol inet, MTU: 9536
    Flags: Sendbcst-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  :             4             0           244            0
    Output :            108             0          13392            0
  Protocol inet, MTU: 9536
    Flags: Sendbcst-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 interface 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 the 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 on 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 the PTX3000 routers.

```
user@ptx5000> show chassis hardware
Item                Version  Part number  Serial number  Description
Chassis              REV 11   750-035893  JN11FF811AJA  PTX5000
Midplane             REV 12   760-030647  ACW6233       Midplane-8S
FPM                  REV 07   740-032019  BBAX0093      Front Panel Display
PDU 0                Rev 06   740-032022  1E002280031   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	AMBOWKG	SFP+-10G-SR
Xcvr 12	REV 01	740-031980	B11J04031	SFP+-10G-SR
Xcvr 13	REV 01	740-031980	AMBOTD9	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&gt; 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	AMBOWKG	SFP+-10G-SR
Xcvr 12	REV 01	740-031980	B11J04031	SFP+-10G-SR
Xcvr 13	REV 01	740-031980	AMBOTD9	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 shows that CSE2000 service cards ESC 0 and ESC1 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 the 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 the 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 the 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 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 the 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**

- [Example: Configuring Active Flow Monitoring Version 9 for IPv4 on page 24](#)
- [Example: Configuring Active Flow Monitoring Version 9 for IPv6 on page 38](#)
- [Example: Configuring Active Flow Monitoring Version 9 for MPLS on page 52](#)
- [Example: Configuring Active Flow Monitoring Version 9 for MPLS and IPv4 on page 67](#)

## CHAPTER 3

# Active Flow Monitoring Version 9 Configuration Statements

- `disable` (Forwarding Options) on page 138
- `export-port` on page 139
- `family` (Sampling) on page 140
- `filter` (Configuring) on page 141
- `flow-active-timeout` on page 142
- `flow-inactive-timeout` on page 143
- `flow-server` on page 144
- `flow-monitoring` on page 145
- `input` (Sampling) on page 146
- `instance` (Sampling) on page 147
- `interface` (Monitoring) on page 148
- `ipv4-template` on page 149
- `ipv6-template` on page 149
- `label-position` on page 150
- `maximum-packet-length` on page 150
- `mpls-ipv4-template` on page 151
- `mpls-template` on page 151
- `option-refresh-rate` on page 152
- `template-refresh-rate` on page 153
- `output` (Sampling) on page 154
- `port` on page 155
- `rate` (Forwarding Options) on page 155
- `run-length` on page 156
- `sampling` (Forwarding Options) on page 157
- `source-address` (Forwarding Options) on page 158

- [template \(Forwarding Options\)](#) on page 158
- [version9 \(Forwarding Options\)](#) on page 159

## disable (Forwarding Options)

---

**Supported Platforms** [CSE2000, PTX Series](#)

**Syntax** disable;

**Hierarchy Level** [edit forwarding-options sampling]

**Release Information** Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000.  
Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.

**Description** Disable traffic sampling.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Traffic Sampling on page 23](#)

## export-port

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	export-port <address <i>address</i>   gateway <i>address</i> >;
<b>Hierarchy Level</b>	[edit forwarding-options sampling instance <i>instance-name</i> family (inet   inet6   mpls) output interface <i>interface-name</i> ]
<b>Release Information</b>	This statement is deprecated starting in Junos OS release 13.3R7, 14.1R6, 14.2R4, 15.1R2, 15.2R1 and later. Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Specify the export port information for the CSE2000 interface connected to the flow server.



**NOTE:** If you configure the export-port <address *address*> <gateway *gateway-address*> statement at the [edit forwarding-options sampling instance *instance-name* family (inet | inet6 | mpls) output interface *interface-name*] hierarchy level, the configuration does not have any effect; instead, a warning is displayed about the deprecated configuration.

The deprecation of export port configuration is intended to match the configuration similar to MS-PIC.

<b>Options</b>	<b>address <i>address</i></b> —(Optional) Address to use for the export port connected to the flow server. <b>gateway <i>address</i></b> —(Optional) Gateway address for the v9 records to reach the flow server.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Flow Server to Collect Active Flow Monitoring Version 9 Records on page 23</a></li> </ul>

## family (Sampling)

**Supported Platforms** [PTX3000, PTX5000, T Series](#)

**Syntax**

```
family (inet | inet6 | mpls) {
  disable;
  output {
    flow-active-timeout seconds;
    flow-inactive-timeout seconds;
    flow-server hostname {
      port port-number;
      source-address address;
      version9 {
        template template-name;
      }
    }
  }
}
```

**Hierarchy Level** [edit forwarding-options sampling],  
[edit forwarding-options sampling instance *instance-name*]

**Release Information** Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000.  
Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.

**Description** Configure the protocol family to be sampled. IPv4 (**inet**) is supported for most purposes, but you can configure **family mpls** to collect and export MPLS label information or **family inet6** to collect and export IPv6 traffic by using flow monitoring version 9.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Traffic Sampling on page 23](#)

## filter (Configuring)

---

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	<pre>filter <i>filter-name</i> {   term <i>term-name</i> {     ... term configuration ...   } }</pre>
<b>Hierarchy Level</b>	[edit firewall family (inet   inet6   mpls)]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Configure firewall filters.
<b>Options</b>	<p><b><i>filter-name</i></b>—Name that identifies the filter. This must be a nonreserved string of not more than 64 characters. You cannot use special characters within the name of a firewall filter. Firewall filter names are restricted from having the form <code>_.*_</code> (beginning and ending with underscores) or <code>_.*</code> (beginning with an underscore).</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>firewall—To view this statement in the configuration.</p> <p>firewall-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring a Firewall Filter for Active Flow Monitoring Version 9 on page 22</a></li> </ul>

## flow-active-timeout

---

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	flow-active-timeout <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit services flow-monitoring version9 template <i>template-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	<p>Set the interval after which an active flow is exported.</p> <p>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.</p>
<b>Options</b>	<p><i>seconds</i>—Duration of the timeout period.</p> <p><b>Range:</b> 10 through 600 seconds</p> <p><b>Default:</b> 60 seconds</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Active Flow Monitoring Version 9 Templates on page 20</a></li></ul>

## flow-inactive-timeout

---

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	flow-inactive-timeout <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit services flow-monitoring version9 template <i>template-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	<p>Set the interval of inactivity that marks a flow inactive.</p> <p>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.</p>
<b>Options</b>	<p><i>seconds</i>—Duration of the timeout period.</p> <p><b>Range:</b> 10 through 600 seconds</p> <p><b>Default:</b> 60 seconds</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Active Flow Monitoring Version 9 Templates on page 20</a></li></ul>

## flow-server

---

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	<pre>flow-server hostname {   port port-number;   version9 {     template template-name;   } }</pre>
<b>Hierarchy Level</b>	[edit forwarding-options sampling instance <i>instance-name</i> family (inet   inet6   mpls) output]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Specify a flow server to collect v9 records.
<b>Options</b>	<p><i>hostname</i>—The IP address or identifier of the host system (the workstation collecting the traffic flows using version 9).</p> <p>You can configure only one host system for version 9.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Active Flow Monitoring Version 9 Formats and Fields on page 6</a></li><li>• <a href="#">Configuring Flow Server to Collect Active Flow Monitoring Version 9 Records on page 23</a></li></ul>

## flow-monitoring

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	<pre> flow-monitoring {   version9{     template <i>template-name</i> {       flow-active-timeout <i>seconds</i>;       flow-inactive-timeout <i>seconds</i>;       ipv4-template;       ipv6-template;       mpls-template {         label-position [ <i>positions</i> ];       }       mpls-ipv4-template {         label-position [ <i>positions</i> ];       }       option-refresh-rate <i>packets packets seconds seconds</i>;       template-refresh-rate <i>packets packets seconds seconds</i>;     }   } } </pre>
<b>Hierarchy Level</b>	[edit services]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Specify the active monitoring properties for flow aggregation version 9.  The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring Active Flow Monitoring Version 9 for IPv4 on page 24</a></li> <li>• <a href="#">Example: Configuring Active Flow Monitoring Version 9 for IPv6 on page 38</a></li> <li>• <a href="#">Example: Configuring Active Flow Monitoring Version 9 for MPLS on page 52</a></li> <li>• <a href="#">Example: Configuring Active Flow Monitoring Version 9 for MPLS and IPv4 on page 67</a></li> <li>• <a href="#">Example: Configuring Active Flow Monitoring Version 9 for Simultaneous IPv4, MPLS, and IPv6 Sampling on page 82</a></li> </ul>

## input (Sampling)

---

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	<pre>input {   rate <i>number</i>;   run-length <i>number</i>;   maximum-packet-length <i>bytes</i>; }</pre>
<b>Hierarchy Level</b>	[edit forwarding-options sampling instance <i>instance-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	<p>Configure traffic sampling input, such as the sampling rate, the run length, and the maximum packet length.</p> <p>The statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Traffic Sampling on page 23</a></li></ul>

## instance (Sampling)

**Supported Platforms** CSE2000, PTX3000, PTX5000

**Syntax**

```
instance instance-name {
  disable;
  input {
    rate number;
    run-length number;
    maximum-packet-length bytes;
  }
  family (inet | inet6 | mpls) {
    disable;
    output {
      flow-active-timeout seconds;
      flow-inactive-timeout seconds;
      flow-server hostname {
        port port-number;
        version9 {
          template template-name;
        }
      }
    }
  }
}
```

**Hierarchy Level** [edit forwarding-options sampling]

**Release Information** Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000.  
Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.

**Description** Configure a sampling instance to collect the sampling data.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Traffic Sampling on page 23](#)

## interface (Monitoring)

---

**Supported Platforms** CSE2000, PTX3000, PTX5000

**Syntax** interface *interface-name* {  
     export-port *address*;  
     gateway *address*;  
 }

**Hierarchy Level** [edit forwarding-options sampling instance ins] family inet output]

**Release Information** export-port *address* and gateway *address* options are deprecated in Junos OS release 13.3R7, 14.1R6, 14.2R4, 15.1R2, 15.2R1 and later.  
 Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000.  
 Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.

**Description** Specify the output interface for monitored traffic.



**NOTE:** If you configure the export-port <address *address*> <gateway *gateway-address*> statement at the [edit forwarding-options sampling instance *instance-name* family (inet | inet6 | mpls) output interface *interface-name*] hierarchy level, the configuration does not have any effect; instead, a warning is displayed about the deprecated configuration.

The deprecation of export port configuration is intended to match the configuration similar to MS-PIC.

**Options** *interface-name*—Name of the interface.

*export-port address*—Address of the export port connected to the flow server.

*gateway address*—Gateway address to reach the flow server.

**Required Privilege Level** interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

- Related Documentation**
- [Configuring Flow Server to Collect Active Flow Monitoring Version 9 Records on page 23](#)
  - [Configuring Active Flow Monitoring Version 9 Templates on page 20](#)

## ipv4-template

---

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	ipv4-template;
<b>Hierarchy Level</b>	[edit services <a href="#">flow-monitoring version9 template</a> <i>template-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Specify that the flow aggregation version 9 template is used only for IPv4 records.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring Active Flow Monitoring Version 9 for IPv4 on page 24</a></li> </ul>

## ipv6-template

---

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	ipv6-template;
<b>Hierarchy Level</b>	[edit services <a href="#">flow-monitoring version9 template</a> <i>template-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Specify that the flow aggregation version 9 template is used only for IPv6 records.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring Active Flow Monitoring Version 9 for IPv6 on page 38</a></li> </ul>

## label-position

---

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	label-position [ <i>positions</i> ];
<b>Hierarchy Level</b>	[edit services flow-monitoring version9 template <i>template-name</i> mpls-ipv4-template], [edit services flow-monitoring version9 template <i>template-name</i> mpls-template]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Specify positions for up to three labels in the active flow monitoring version 9 template.
<b>Default</b>	[1 2 3]
<b>Options</b>	<i>positions</i> —Numbered positions for the labels.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Active Flow Monitoring Version 9 Templates on page 20</a></li><li>• <a href="#">Example: Configuring Active Flow Monitoring Version 9 for MPLS and IPv4 on page 67</a></li><li>• <a href="#">Example: Configuring Active Flow Monitoring Version 9 for MPLS on page 52</a></li></ul>

## maximum-packet-length

---

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	maximum-packet-length <i>bytes</i> ;
<b>Hierarchy Level</b>	[edit forwarding-options sampling instance <i>instance-name</i> input]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Set the maximum length of the packet used for traffic sampling. Packets with lengths greater than the specified maximum length are truncated.
<b>Options</b>	<i>bytes</i> —Maximum length (in bytes) of the sampled packet. <b>Range:</b> 0 through 9216 <b>Default:</b> 0
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Traffic Sampling on page 23</a></li></ul>

## mpls-ipv4-template

---

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	<pre>mpls-ipv4-template {   label-position [ <i>positions</i> ]; }</pre>
<b>Hierarchy Level</b>	[edit services <a href="#">flow-monitoring version9 template <i>template-name</i></a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Specify the flow aggregation version 9 properties for templates that combine IPv4 and MPLS records. The remaining statement is explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring Active Flow Monitoring Version 9 for MPLS and IPv4 on page 67</a></li> </ul>

## mpls-template

---

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	<pre>mpls-template {   label-position [ <i>positions</i> ]; }</pre>
<b>Hierarchy Level</b>	[edit services <a href="#">flow-monitoring version9 template <i>template-name</i></a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Specify the flow aggregation version 9 properties for templates used only for MPLS records. The remaining statement is explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring Active Flow Monitoring Version 9 for MPLS on page 52</a></li> </ul>

## option-refresh-rate

---

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	option-refresh-rate packets <i>packets</i> seconds <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit services <a href="#">flow-monitoring version9 template</a> <i>template-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Specify the refresh rate, in either packets or seconds.
<b>Options</b>	<p><i>packets</i>—Refresh rate, in number of packets. <b>Range:</b> 1 through 480,000 <b>Default:</b> 4800</p> <p><i>seconds</i>—Refresh rate, in number of seconds. <b>Range:</b> 10 through 600 <b>Default:</b> 60</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Active Flow Monitoring Version 9 Templates on page 20</a></li></ul>

---

## template-refresh-rate

---

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	template-refresh-rate packets <i>packets</i> seconds <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit services <a href="#">flow-monitoring version9 template</a> <i>template-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Specify the refresh rate, in either packets or seconds.
<b>Options</b>	<p><i>packets</i>—Refresh rate, in number of packets. <b>Range:</b> 1 through 480,000 <b>Default:</b> 4800</p> <p><i>seconds</i>—Refresh rate, in number of seconds. <b>Range:</b> 10 through 600 <b>Default:</b> 60</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Active Flow Monitoring Version 9 Templates on page 20</a></li></ul>

## output (Sampling)

---

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	<pre>output {   flow-active-timeout <i>seconds</i>;   flow-inactive-timeout <i>seconds</i>;   flow-server <i>hostname</i> {     port <i>port-number</i>;     source-address <i>address</i>;     version9 {       template <i>template-name</i>;     }   } }</pre>
<b>Hierarchy Level</b>	[edit forwarding-options sampling instance <i>instance-name</i> family (inet  inet6  mpls)], [edit forwarding-options sampling family (inet  inet6  mpls)]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Configure traffic sampling output.  The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Traffic Sampling on page 23</a></li></ul>

## port

---

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	port <i>port-number</i> ;
<b>Hierarchy Level</b>	[edit forwarding-options sampling instance <i>instance-name</i> family (inet   inet6   mpls) output flow-server <i>hostname</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Specify the UDP port number on the flow server.
<b>Options</b>	<i>port-number</i> —Any valid UDP port number on the flow server.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">flow-server on page 144</a></li> </ul>

## rate (Forwarding Options)

---

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	rate <i>number</i> ;
<b>Hierarchy Level</b>	[edit forwarding-options sampling instance <i>instance-name</i> input]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Set a ratio of the number of packets to be sampled. For example, if you specify a rate of 10, every tenth packet (1 packet out of 10) is sampled.
<b>Options</b>	<i>number</i> —Denominator of the ratio. <b>Range:</b> 1 through 65,535
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Traffic Sampling on page 23</a></li> </ul>

## run-length

---

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	run-length <i>number</i> ;
<b>Hierarchy Level</b>	[edit forwarding-options sampling instance <i>instance-name</i> input]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Set the number of samples following the initial trigger event. The configuration enables you to sample packets following those already being sampled.
<b>Options</b>	<i>number</i> —Number of samples. <b>Range:</b> 0 through 20 <b>Default:</b> 0
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">instance on page 147</a></li><li>• <a href="#">Configuring Traffic Sampling on page 23</a></li></ul>

## sampling (Forwarding Options)

**Supported Platforms** CSE2000, PTX3000, PTX5000

**Syntax**

```
sampling {
  disable;
  family (inet | inet6 | mpls) {
    disable;
  }
  input {
    maximum-packet-length bytes;
    rate number;
    run-length number;
  }
  instance instance-name {
    disable;
    family (inet | inet6 | mpls) {
      disable;
      output {
        flow-active-timeout seconds;
        flow-inactive-timeout seconds;
        flow-server hostname {
          port port-number;
          source-address address;
          version9 {
            template template-name;
          }
        }
      }
    }
  }
}
```

**Hierarchy Level** [edit forwarding-options]

**Release Information** Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.

**Description** Configure traffic sampling.

The statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Traffic Sampling on page 23](#)

## source-address (Forwarding Options)

---

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	source-address <i>address</i> ;
<b>Hierarchy Level</b>	[edit forwarding-options sampling family (inet  inet6  mpls) output interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Specify the source address for monitored packets.
<b>Options</b>	<i>address</i> —Interface source address.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Active Flow Monitoring Version 9 Templates on page 20</a></li><li>• <a href="#">Configuring Traffic Sampling on page 23</a></li></ul>

## template (Forwarding Options)

---

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	template <i>template-name</i> ;
<b>Hierarchy Level</b>	[edit forwarding-options sampling family (inet  inet6  mpls) output flow-server <i>hostname</i> version9]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Specify the flow monitoring version 9 template to be used to generate the output of sampling records.
<b>Options</b>	<i>template-name</i> —Name of the version 9 template.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Active Flow Monitoring Version 9 Templates on page 20</a></li></ul>

## version9 (Forwarding Options)

---

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	<pre>version9 {   template <i>template-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit forwarding-options sampling instance <i>instance-name</i> family (inet  inet6  mpls) output flow-server <i>hostname</i> ], [edit forwarding-options sampling family (inet  inet6  mpls) output flow-server <i>hostname</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Statement introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Specify flow monitoring version 9 properties to apply to output sampling records. The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Active Flow Monitoring Version 9 Templates on page 20</a></li></ul>



## PART 3

# Administration

- [Active Flow Monitoring Version 9 Operational Commands on page 163](#)



## CHAPTER 4

# Active Flow Monitoring Version 9 Operational Commands

- show interfaces
- show services accounting errors
- show services accounting flow
- show services accounting status
- show system processes esc-node

## show interfaces

---

**Supported Platforms** CSE2000, PTX3000, PTX5000

**Syntax** `show interfaces <esp max-router-fpcs/slot-id/port > |<ats interface-number>`  
`<brief | detail | extensive | terse>`  
`<descriptions>`  
`<media>`  
`<snmp-index snmp-index>`  
`<statistics>`

**Release Information** Command introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000.  
 Command introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.

**Description** Display status information about the specified Ethernet interface.

**Options** `none`—Display information about physical and logical interfaces.

`esp max-router-fpcs/slot-id/port`—(Optional) Display standard information about the specified export service port.

`ats interface-number`—(Optional) Display standard information about the specified aggregated tethered services (ATS) interface.

`brief | detail | extensive | terse`—(Optional) Display the specified level of output.

`descriptions`—(Optional) Display interface description strings.

`media` —(Optional) Display media-specific information about network interfaces.

`snmp-index snmp-index`—(Optional) Display information for the specified SNMP index of the interface.

`statistics`—(Optional) Display static interface statistics.

**Required Privilege Level** view

**List of Sample Output** [show interfaces esp \(Export Service Port\) on page 167](#)  
[show interfaces ats \(Aggregated Tethered Services\) on page 168](#)

**Output Fields** See [Table 10 on page 165](#) for the output fields for the `show interfaces` command.

Table 10: show interfaces Output Fields

Field Name	Field Description	Level of Output
<b>Physical Interface</b>		
<b>Physical interface</b>	Name of the physical interface.	All levels
<b>Enabled</b>	State of the interface. Possible values are described in the “Enabled Field” section under <i>Common Output Fields Description</i> .	All levels
<b>Interface index</b>	Index number of the physical interface, which reflects its initialization sequence.	<b>detail extensive none</b>
<b>SNMP ifIndex</b>	SNMP index number for the physical interface.	<b>detail extensive none</b>
<b>Generation</b>	Unique number for use by Juniper Networks technical support only.	<b>detail extensive</b>
<b>Link-level type</b>	Encapsulation being used on the physical interface.	All levels
<b>MTU</b>	Maximum transmission unit size on the physical interface.	All levels
<b>Speed</b>	Speed at which the interface is running.	All levels
<b>Device flags</b>	Information about the physical device. Possible values are described in the “Device Flags” section under <i>Common Output Fields Description</i> .	All levels
<b>Interface flags</b>	Information about the interface. Possible values are described in the “Interface Flags” section under <i>Common Output Fields Description</i> .	All levels
<b>Link flags</b>	Information about the link. Possible values are described in the “Links Flags” section under <i>Common Output Fields Description</i> .	All levels
<b>Hold-times</b>	Current interface hold-time up and hold-time down, in milliseconds.	<b>detail extensive</b>
<b>Current address</b>	Configured MAC address.	<b>detail extensive none</b>
<b>Hardware address</b>	Hardware MAC address.	<b>detail extensive none</b>
<b>Last flapped</b>	Date, time, and how long ago the interface went from down to up. The format is <b>Last flapped: year-month-day hour:minute:second:timezone (hour:minute:second ago)</b> . For example, <b>Last flapped: 2013-11-28 16:24:06 IST (21:23:45 ago)</b> .	<b>detail extensive none</b>
<b>Statistics last cleared</b>	Time when the statistics for the interface were last set to zero.	<b>detail extensive</b>
<b>Traffic statistics</b>	Number and rate of bytes and packets received and transmitted on the physical interface. <ul style="list-style-type: none"> <li>• <b>Input bytes</b>—Number of bytes received on the interface.</li> <li>• <b>Output bytes</b>—Number of bytes transmitted on the interface.</li> <li>• <b>Input packets</b>—Number of packets received on the interface.</li> <li>• <b>Output packets</b>—Number of packets transmitted on the interface.</li> </ul>	<b>detail extensive</b>

Table 10: show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>Input errors</b>	<p>Input errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</p> <ul style="list-style-type: none"> <li>• <b>Errors</b>—Sum of the incoming frame aborts and FCS errors.</li> <li>• <b>Drops</b>—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism.</li> <li>• <b>Framing errors</b>—Number of packets received with an invalid frame checksum (FCS).</li> <li>• <b>Runts</b>—Number of frames received that are smaller than the runt threshold.</li> <li>• <b>Policed discards</b>—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle.</li> <li>• <b>Resource errors</b>—Sum of transmit drops.</li> </ul>	<b>extensive</b>
<b>Output errors</b>	<p>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</p> <ul style="list-style-type: none"> <li>• <b>Carrier transitions</b>—Number of times the interface has gone from <b>down</b> to <b>up</b>. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC or PIM is malfunctioning.</li> <li>• <b>Errors</b>—Sum of the outgoing frame aborts and FCS errors.</li> <li>• <b>Drops</b>—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism.</li> <li>• <b>Collisions</b>—Number of Ethernet collisions. The Gigabit Ethernet PIC supports only full-duplex operation, so for Gigabit Ethernet PICs, this number should always remain 0. If it is nonzero, there is a software bug.</li> <li>• <b>MTU errors</b>—Number of packets whose size exceeded the MTU of the interface.</li> <li>• <b>Resource errors</b>—Sum of transmit drops.</li> </ul>	<b>extensive</b>
<b>Logical Interface</b>		
<b>Logical interface</b>	Name of the logical interface.	All levels
<b>Index</b>	Index number of the logical interface, which reflects its initialization sequence.	<b>detail extensive none</b>
<b>SNMP ifIndex</b>	SNMP interface index number for the logical interface.	<b>detail extensive none</b>
<b>Generation</b>	Unique number for use by Juniper Networks technical support only.	<b>detail extensive</b>
<b>Flags</b>	Information about the logical interface. Possible values are described in the "Logical Interface Flags" section under <i>Common Output Fields Description</i> .	All levels
<b>Encapsulation</b>	Encapsulation on the logical interface.	All levels

Table 10: show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>Protocol</b>	Protocol family. Possible values are described in the "Protocol Field" section under <i>Common Output Fields Description</i> .	<b>detail extensive none</b>
<b>MTU</b>	Maximum transmission unit size on the logical interface.	<b>detail extensive none</b>
<b>Maximum labels</b>	Maximum number of MPLS labels configured for the MPLS protocol family on the logical interface.	<b>detail extensive none</b>
<b>statistics</b>	<p>Number of bytes and packets received and transmitted on the specified ATS bundle.</p> <ul style="list-style-type: none"> <li>• <b>Input bytes, Output bytes</b>—Number of bytes received and transmitted on the ATS interface bundle.</li> <li>• <b>Input pps, Output pps</b>—Number of packets per second received and transmitted on the ATS interface bundle.</li> <li>• <b>Input packets, Output packets</b>—Number of packets received and transmitted on the ATS interface bundle.</li> <li>• <b>Input bps, Output bps</b>—Number of bytes per second received and transmitted on the ATS interface bundle.</li> </ul>	<b>detail extensive</b>
<b>Links</b>	<p>Number and rate of bytes and packets received and transmitted on the specified member interface links of the ATS interface bundle.</p> <ul style="list-style-type: none"> <li>• <b>Input bytes, Output bytes</b>—Number of bytes received and transmitted on the member interface link.</li> <li>• <b>Input pps, Output pps</b>—Number of packets per second received and transmitted on the member interface link.</li> <li>• <b>Input packets, Output packets</b>—Number of packets received and transmitted on the member interface link.</li> <li>• <b>Input bps, Output bps</b>—Number of bytes per second received and transmitted on the member interface link.</li> </ul>	<b>detail</b>
<b>Generation</b>	Unique number for use by Juniper Networks technical support only.	<b>detail extensive</b>
<b>Route Table</b>	Route table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.	<b>detail extensive none</b>

## Sample Output

### show interfaces esp (Export Service Port)

```

user@host> show interfaces esp-8/0/1
Physical interface: esp-8/0/1, Enabled, Physical link is Down
  Interface index: 131, SNMP ifIndex: 605
  Type: Ethernet, Link-level type: Ethernet, MTU: 9536, Speed: 10Gbps
  Device flags   : Present Running
  Interface flags: Hardware-Down
  Link type      : Full-Duplex
  Link flags     : None
  Last flapped   : Never
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)

```

**show interfaces ats (Aggregated Tethered Services)**

```

user@host> show interfaces ats0
Physical interface: ats0, Enabled, Physical link is Up
  Interface index: 195, SNMP ifIndex: 503, Generation: 1268
  Type: Ethernet, Link-level type: Ethernet, MTU: 9536, Clocking: Unspecified,
Speed: 10Gbps
Device flags      : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Link type        : Full-Duplex
Link flags       : None
Physical info    : Unspecified
Hold-times      : Up 0 ms, Down 0 ms
Current address: 08:81:f4:d0:40:10, Hardware address: 08:81:f4:d0:40:10
Alternate link address: Unspecified
Last flapped    : 2013-11-28 16:24:06 IST (22:15:57 ago)
Statistics last cleared: Never
Traffic statistics:
Input bytes      :           7532           0 bps
Output bytes    :             0           0 bps
Input packets   :            122           0 pps
Output packets  :             0           0 pps
IPv6 transit statistics:
Input bytes     :             0
Output bytes    :             0
Input packets   :             0
Output packets  :             0

Logical interface ats0.0 (Index 66) (SNMP ifIndex 504) (Generation 425)
Flags: Up Point-To-Point SNMP-Traps 0x4000 Encapsulation: Tether-Enet-Svcs
Statistics
Bundle:
  Input :           122           0           7532           0
  Output:            0           0             0           0
Link:
et-0/0/12.0
  Input :            0           0             0           0
  Output:            0           0             0           0
et-0/0/13.0
  Input :           122           0           7532           0
  Output:            0           0           7423           0
Protocol inet, MTU: 9536, Generation: 979, Route table: 0
Flags: Sendbcst-pkt-to-re
Protocol inet6, MTU: 9536, Generation: 980, Route table: 0
Flags: Is-Primary

```

## show services accounting errors

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	show services accounting errors <name (*   all   <i>service-name</i> )>
<b>Release Information</b>	Command introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Command introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Display active flow error statistics.
<b>Options</b>	<b>none</b> —Display error statistics for all services accounting instances. <b>name (*   all   <i>service-name</i>)</b> —(Optional) Display active flow error statistics. Use a wildcard character, specify all services, or provide a specific service name.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">show services accounting status on page 173</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show services accounting errors on page 170</a>
<b>Output Fields</b>	<a href="#">Table 11 on page 169</a> lists the output fields for the <b>show services accounting errors</b> command. Output fields are listed in the approximate order in which they appear.

Table 11: show services accounting errors Output Fields

Field	Field Description
Service Accounting interface	Name of the service accounting interface.
Service sets dropped	The number of service sets dropped.
Active timeout failures	The number of active timeout failures. For more details on active timeout, see <a href="#">flow-active-timeout</a> .
Export Packet Failures	Number of times packet export failed.
Flow Creation Failures	<p>Number of times flow creation failed.</p> <p>The flow creation can fail because of the following reasons:</p> <ul style="list-style-type: none"> <li>• The CSE2000 receives unsupported protocols or fragmented packets.</li> <li>• Two different processes try to add the same flow to the CSE2000.</li> <li>• The CSE2000 receives TCP segments with flags that do not match any existing flow entry.</li> <li>• The CSE2000 is running low on resources.</li> </ul>
Memory overload	Whether the memory has been overloaded. The response can be <b>Yes</b> or <b>No</b> .

## Sample Output

### show services accounting errors

```
user@host> show services accounting errors
  Service Accounting interface: ats0
  Service sets dropped: 0, Active timeout failures: 0
  Export packet failures: 0, Flow creation failures: 0
  Memory overload: No

  Service Accounting interface: ats1
  Service sets dropped: 0, Active timeout failures: 0
  Export packet failures: 0, Flow creation failures: 0
  Memory overload: No
```

## show services accounting flow

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	show services accounting flow < name (*   all   service-name) >
<b>Release Information</b>	Command introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Command introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Display active flow statistics.
<b>Options</b>	<b>none</b> —Display active flow statistics for all service instances. <b>name (*   all   service-name)</b> —(Optional) Display services accounting active flow statistics. Use a wildcard character, specify all services, or provide a specific service name.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">show services accounting status on page 173</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show services accounting flow on page 172</a>
<b>Output Fields</b>	<a href="#">Table 12 on page 171</a> lists the output fields for the <b>show services accounting flow</b> command. Output fields are listed in the approximate order in which they appear.

Table 12: show services accounting flow Output Fields

Output Field	Output Field Description
Service Accounting interface	Name of the service accounting interface.
Local interface index	Index counter of the local interface.
Flow packets	Number of packets received by an operational CSE2000 service card.
Flow bytes	Number of bytes received by an operational CSE2000 service card.
Flow packets 10-second rate	Number of packets per second handled by the CSE2000 service card and displayed as a 10-second average.
Flow bytes 10-second rate	Number of bytes per second handled by the CSE2000 service card and displayed as a 10-second average.
Active flows	Number of currently active flows tracked by the CSE2000 service card.
Total flows	Total number of flows received by an operational CSE2000 service card.
Flows exported	Total number of flows records generated by an operational CSE2000 service card.

Table 12: show services accounting flow Output Fields (*continued*)

Output Field	Output Field Description
Flows packets exported	Total number of flow monitoring packets exported by an operational CSE2000 service card to the flow server.
Flows inactive timed out	Total number of flows that are exported because of inactivity.
Flows active timed out	Total number of long-lived flows that are exported because of an active timeout.

## Sample Output

### show services accounting flow

```
user@host> show services accounting flow
Flow information
Service Accounting interface: ats1, Local interface index: 194
Flow packets: 261334529080, Flow bytes: 26553475212445
Flow packets 10-second rate: 14220447, Flow bytes 10-second rate: 1450485594

Active flows: 30000000, Total flows: 30000000
Flows exported: 6667726081, Flows packets exported: 281343003
Flows inactive timed out: 0, Flows active timed out: 6668264479
```

## show services accounting status

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	show services accounting status < name (*   all   <i>service-name</i> ) >
<b>Release Information</b>	Command introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Command introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Display available aggregated tethered services (ATS) interfaces for accounting services.
<b>Options</b>	<b>none</b> —Display available ATS interfaces for all accounting services. <b>name (*   all   <i>service-name</i>)</b> —(Optional) Use a wildcard character, specify all services, or provide a specific services name.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Aggregated Tethered Services Interfaces Overview on page 13</a></li> <li>• <a href="#">Configuring Member Interfaces and Interface Family for Aggregated Tethered Services Interfaces on page 19</a></li> <li>• <a href="#">show services accounting flow on page 171</a></li> <li>• <a href="#">show services accounting errors on page 169</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show services accounting status on page 174</a>
<b>Output Fields</b>	Table 13 on page 173 lists the output fields for the <b>show services accounting status</b> command. Output fields are listed in the approximate order in which they appear.

Table 13: show services accounting status Output Fields

Field	Field Description
Service Accounting interface	Name of the service accounting interface.
Export format	Configured export format.
Route Record Count	Number of routes recorded.
AS Record Count	Number of autonomous systems recorded.
Route Records Set	Status of route recording; whether routes are recorded or not.
Configuration Set	Status of monitoring configuration; whether monitoring configuration is set or not.
IFL to SNMP index count	Number of logical interfaces mapped to an SNMP index.

## Sample Output

### Sample Output

#### show services accounting status

```
user@host> show services accounting status
Service Accounting interface: ats0
Export format: 9, Route record count: 60
IFL to SNMP index count: 16, AS count: 1
Configuration set: Yes, Route record set: Yes, IFL SNMP map set: Yes

Service Accounting interface: ats1
Export format: 9, Route record count: 60
IFL to SNMP index count: 16, AS count: 1
Configuration set: Yes, Route record set: Yes, IFL SNMP map set: Yes
```

## show system processes esc-node

<b>Supported Platforms</b>	CSE2000, PTX3000, PTX5000
<b>Syntax</b>	show system processes esc-node
<b>Release Information</b>	Command introduced in Junos OS Release 13.3 for PTX5000 routers with CSE2000. Command introduced in Junos OS Release 13.3R4 for PTX3000 routers with CSE2000.
<b>Description</b>	Display information about software processes that are running on the CSE2000 service card.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>request chassis service-node</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show system processes esc-node on page 176</a>
<b>Output Fields</b>	<a href="#">Table 14 on page 175</a> lists the output fields for the <b>show system processes esc-node</b> command. Output fields are listed in the approximate order in which they appear.

Table 14: show system processes esc-node Output Fields

Field Name	Field Description
top	Shows the system information: <ul style="list-style-type: none"> <li>• The current time.</li> <li>• Duration of system up and running time.</li> <li>• Number of users logged in.</li> </ul>
load average	Load averages for the last 1 minute, 5 minutes, and 15 minutes.
Tasks	Total the number of processes and their current state.
Cpu(s)	CPU utilization in percentage.
Mem	Information about physical and virtual memory allocation.
Swap	Information about swap memory: <ul style="list-style-type: none"> <li>• <b>Total</b>—Total space on the swap device.</li> <li>• <b>Used</b>—Memory swapped to disk.</li> <li>• <b>Free</b>—Unused space available on the swap device.</li> </ul>
PID	Process identifier.
USER	User that is running the process.
PR	Current priority of the process. A lower number indicates a higher priority.

Table 14: show system processes esc-node Output Fields (*continued*)

Field Name	Field Description
NI	UNIX "niceness" value. A lower number indicates a higher priority.
VIRT	The total amount of virtual memory used.
RES	Current amount of resident memory.
SHR	Amount of shared memory used.
S	State of the task. The first letter indicates the run state of the task: <ul style="list-style-type: none"> <li>• S—Sleeping for less than 20 seconds</li> <li>• D—In disk or other short-term, uninterruptible wait</li> <li>• R—Running</li> <li>• Z—Dead (zombie)</li> <li>• T—Stopped</li> </ul>
%CPU	Percentage of CPU used.
%MEM	Percentage of memory used.
TIME+	Total CPU time used.
COMMAND	Command issued.

## Sample Output

### show system processes esc-node

```

user@host> show system processes esc-node
top - 16:20:20 up 15 min, 1 user, load average: 26.36, 24.85, 15.85
Tasks: 284 total, 29 running, 249 sleeping, 0 stopped, 6 zombie
Cpu(s): 75.9%us, 0.7%sy, 0.0%ni, 23.4%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 131878180k total, 28865040k used, 103013140k free, 9800k buffers
Swap: 134184956k total, 0k used, 134184956k free, 51340k cached

```

```

      PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM   TIME+  COMMAND
    2081 root       20   0 28.0g 15m 1284 R   100   0.0 14:08.41 Timer-1
    2084 root       20   0 28.0g 15m 1284 R   100   0.0 14:08.47 PktProc-4
    2085 root       20   0 28.0g 15m 1284 R   100   0.0 14:08.49 PktProc-5
    2086 root       20   0 28.0g 15m 1284 R   100   0.0 14:08.48 PktProc-6
    2087 root       20   0 28.0g 15m 1284 R   100   0.0 14:08.48 PktProc-7
    2088 root       20   0 28.0g 15m 1284 R   100   0.0 14:08.78 LoadBal-8
    2089 root       20   0 28.0g 15m 1284 R   100   0.0 14:08.79 LoadBal-9
    2091 root       20   0 28.0g 15m 1284 R   100   0.0 14:08.69 JFlow_Export-11
    2092 root       20   0 28.0g 15m 1284 R   100   0.0 14:08.66 PktProc-12
    2093 root       20   0 28.0g 15m 1284 R   100   0.0 14:08.74 PktProc-13
    2094 root       20   0 28.0g 15m 1284 R   100   0.0 14:08.53 PktProc-14
    2095 root       20   0 28.0g 15m 1284 R   100   0.0 14:08.54 PktProc-15
    2096 root       20   0 28.0g 15m 1284 R   100   0.0 14:08.41 PktProc-16
    2101 root       20   0 28.0g 15m 1284 R   100   0.0 14:08.50 PktProc-21
    2102 root       20   0 28.0g 15m 1284 R   100   0.0 14:08.49 PktProc-22

```

```

2103 root      20    0 28.0g 15m 1284 R 100 0.0 14:08.49 PktProc-23
2104 root      20    0 28.0g 15m 1284 R 100 0.0 14:08.52 PktProc-30
2105 root      20    0 28.0g 15m 1284 R 100 0.0 14:08.54 PktProc-31
2082 root      20    0 28.0g 15m 1284 R  98 0.0 14:08.41 Timer-2
2083 root      20    0 28.0g 15m 1284 R  98 0.0 14:08.46 PktProc-3
2090 root      20    0 28.0g 15m 1284 R  98 0.0 14:08.65 PktProc-10
2097 root      20    0 28.0g 15m 1284 R  98 0.0 14:08.45 PktProc-17
2098 root      20    0 28.0g 15m 1284 R  98 0.0 14:08.46 PktProc-18
2099 root      20    0 28.0g 15m 1284 R  98 0.0 14:08.47 PktProc-19
2100 root      20    0 28.0g 15m 1284 R  98 0.0 14:08.47 PktProc-20
1957 root      20    0 28.0g 15m 1284 R  94 0.0 14:06.66 jtapperd
1043 root      39   19    0    0    0 R  23 0.0  2:32.58 kipmi0
13368 juniper  20    0 17464 1400 916 R   4 0.0  0:00.03 top
   1 root      20    0 24480 2372 1356 S   0 0.0  0:04.88 init
   2 root      20    0    0    0    0 S   0 0.0  0:00.05 kthreadd
   3 root      20    0    0    0    0 S   0 0.0  0:00.06 ksoftirqd/0
   6 root      RT    0    0    0    0 S   0 0.0  0:00.00 migration/0
   7 root      RT    0    0    0    0 S   0 0.0  0:00.34 watchdog/0
   8 root      RT    0    0    0    0 S   0 0.0  0:00.00 migration/1
   9 root      20    0    0    0    0 S   0 0.0  0:00.00 kworker/1:0
  10 root      20    0    0    0    0 S   0 0.0  0:00.00 ksoftirqd/1
  11 root      20    0    0    0    0 S   0 0.0  0:00.83 kworker/0:1

```

