

Flow Monitoring



Published: 2013-08-29

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

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

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.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Flow Monitoring
Copyright © 2013, 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	xi
	Documentation and Release Notes	xi
	Supported Platforms	xi
	Using the Examples in This Manual	xi
	Merging a Full Example	xii
	Merging a Snippet	xii
	Documentation Conventions	xiii
	Documentation Feedback	xiv
	Requesting Technical Support	xv
	Self-Help Online Tools and Resources	xv
	Opening a Case with JTAC	xvi
Part 1	Overview	
Chapter 1	Flow Monitoring	3
	Active Flow Monitoring Overview	3
	Understanding Inline Sampling	6
	Inline Sampling	6
	Inline Sampling Limitations and Restrictions	7
	IPFIX and Version 9 Templates	7
	Fields Included in the IPFIX IPv4 Template	7
	Fields Included in the IPFIX IPv6 Template	8
	Fields Included in the Version 9 IPv4 Template	9
Part 2	Configuration	
Chapter 2	Configuration Tasks	13
	Configuring Flow Monitoring	13
	Configuring Flow-Monitoring Interfaces	13
	Configuring Flow-Monitoring Properties	14
	Directing Traffic to Flow-Monitoring Interfaces	15
	Exporting Flows	16
	Configuring Time Periods when Flow Monitoring is Active and Inactive	16
	Example: Configuring Flow Monitoring	17
	Configuring Inline Sampling	18
	Configuring Inline Sampling on MX80 Routers	22
	Directing Replicated Flows to Multiple Flow Servers	23
	Directing Replicated Routing Engine–Based Sampling Flows to Multiple Servers	24
	Directing Replicated Version 9 Flow Aggregates to Multiple Servers	25

	Logging cflowd Flows Before Export	26
	Configuring Services Interface Redundancy with Flow Monitoring	27
	Example: Configuring Active Monitoring on Logical Systems	29
Chapter 3	Configuration Statements	33
	[edit interfaces] Hierarchy Level	33
	[edit forwarding-options] Hierarchy Level	34
	address (Interfaces)	38
	cflowd (Discard Accounting)	39
	core-dump	40
	destination (Interfaces)	41
	engine-id (Forwarding Options)	42
	engine-type	43
	export-format	44
	family (Monitoring)	45
	filter	46
	flow-active-timeout	47
	flow-export-destination	48
	flow-inactive-timeout	49
	flow-table-size	49
	input-interface-index	50
	interface (Accounting or Sampling)	50
	ipv4-flow-table-size	51
	ipv6-flow-table-size	51
	monitoring	52
	multiservice-options	53
	output-interface-index	53
	output (Monitoring)	54
	port	55
	sampling (Interfaces)	55
	source-address (Forwarding Options)	56
	syslog	56
	unit	57
Part 3	Administration	
Chapter 4	Flow Monitoring Operational Mode Commands	61
	show services accounting aggregation	62
	show services accounting aggregation template	66
	show services accounting errors	67
	show services accounting flow	71
	show services accounting flow-detail	76
	show services accounting memory	81
	show services accounting packet-size-distribution	83
	show services accounting status	85
	show services accounting usage	88
Chapter 5	Flow Monitoring Interface Operational Mode Commands	91
	show interfaces (Flow Monitoring)	92

Part 4**Index**

Index	99
-------------	----

List of Figures

Part 1	Overview	
Chapter 1	Flow Monitoring	3
	Figure 1: Active Monitoring Configuration Topology	5

List of Tables

	About the Documentation	xi
	Table 1: Notice Icons	xiii
	Table 2: Text and Syntax Conventions	xiii
Part 3	Administration	
Chapter 4	Flow Monitoring Operational Mode Commands	61
	Table 3: show services accounting aggregation Output Fields	63
	Table 4: show services accounting aggregation template Output Fields	66
	Table 5: show services accounting errors Output Fields	67
	Table 6: show services accounting flow Output Fields	71
	Table 7: show services accounting flow-detail Output Fields	77
	Table 8: show services accounting memory Output Fields	81
	Table 9: show services accounting packet-size-distribution Output Fields	83
	Table 10: show services accounting status Output Fields	85
	Table 11: show services accounting usage Output Fields	88
Chapter 5	Flow Monitoring Interface Operational Mode Commands	91
	Table 12: Flow Monitoring show interfaces Output Fields	92

About the Documentation

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

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:

- M Series
- T Series

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 the *CLI User Guide*.

Documentation Conventions

Table 1 on page xiii 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.

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>

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

Convention	Description	Examples
<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@# set system domain-name <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"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	stub <default-metric <i>metric</i> >;
(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.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identify 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		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at

<https://www.juniper.net/cgi-bin/docbugreport/> . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release 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 JNASC 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: <https://www.juniper.net/alerts/>
- 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

- [Flow Monitoring on page 3](#)

CHAPTER 1

Flow Monitoring

- [Active Flow Monitoring Overview on page 3](#)
- [Understanding Inline Sampling on page 6](#)

Active Flow Monitoring Overview

Using a Juniper Networks M Series Multiservice Edge or T Series Core Router, a selection of PICs (including the Monitoring Services PIC, Adaptive Services [AS] PIC, Multiservices PIC, or Multiservices DPC) and other networking hardware, you can monitor traffic flow and export the monitored traffic. Monitoring traffic allows you to do the following:

- Gather and export detailed information about IP version 4 (IPv4) traffic flows between source and destination nodes in your network.
- Sample all incoming IPv4 traffic on the monitoring interface and present the data in cflowd record format.
- Perform discard accounting on an incoming traffic flow.
- Encrypt or tunnel outgoing cflowd records, intercepted IPv4 traffic, or both.
- Direct filtered traffic to different packet analyzers and present the data in its original format (port mirror).



NOTE: Monitoring Services PICs, AS PICs, and Multiservices PICs must be mounted on an Enhanced Flexible PIC Concentrator (FPC) in an M Series or T Series router.

Multiservices DPCs installed in Juniper Networks MX Series 3D Universal Edge Routers support the same functionality, with the exception of the passive monitoring and flow-tap features.

Although the Monitoring Services PIC was designed initially for use as an offline passive flow monitoring tool, it can also be used in an active flow monitoring topology. In contrast, the AS or Multiservices PIC is designed exclusively for active flow monitoring. To use either the Monitoring Services PIC, AS PIC, or Multiservices PIC for active flow monitoring, you must install the PIC in an M Series or T Series router. The router participates in both the monitoring application and in the normal routing functionality of the network.

Starting with Junos OS Release 11.4, support for active monitoring is extended to logical systems running on T Series and MX Series routers. A logical system is a partition created from a physical router that performs independent routing tasks. Several logical systems in a single router with their own interfaces, policies, instances, and routing tables can perform functions handled by several different routers. A shared services PIC handles flows from all the logical systems. Only version 9 flows, IPv4, and MPLS templates are supported. See [“Example: Configuring Active Monitoring on Logical Systems” on page 29](#) for a sample configuration that enables active monitoring on a logical system.

Specified packets can be filtered and sent to the monitoring interface. For the Monitoring Services PIC, the interface name contains the **mo-** prefix. For the AS or Multiservices PIC, the interface name contains the **sp-** prefix.



NOTE: If you upgrade from the Monitoring Services PIC to the Adaptive Services or Multiservices PIC for active flow monitoring, you must change the name of your monitoring interface from **mo-fpc/pic/port** to **sp-fpc/pic/port**.

The major active flow monitoring actions you can configure at the **[edit forwarding-options]** hierarchy level are as follows:

- Sampling, with the **[edit forwarding-options sampling]** hierarchy. This option sends a copy of the traffic stream to an AS or Monitoring Services PIC, which extracts limited information (such as the source and destination IP address) from some of the packets in a flow. The original packets are forwarded to the intended destination as usual.
- Discard accounting, with the **[edit forwarding-options accounting]** hierarchy. This option quarantines unwanted packets, creates cflowd records that describe the packets, and discards the packets instead of forwarding them.
- Port mirroring, with the **[edit forwarding-options port-mirroring]** hierarchy. This option makes one full copy of all packets in a flow and delivers the copy to a single destination. The original packets are forwarded to the intended destination.
- Multiple port mirroring, with the **[edit forwarding-options next-hop-group]** hierarchy. This option allows multiple copies of selected traffic to be delivered to multiple destinations. (Multiple port mirroring requires a Tunnel Services PIC.)

Unlike passive flow monitoring, you do not need to configure a monitoring group. Instead, you can send filtered packets to a monitoring services or adaptive services interface (**mo-** or **sp-**) by using sampling or discard accounting. Optionally, you can configure port mirroring or multiple port mirroring to direct packets to additional interfaces.

These active flow monitoring options provide a wide variety of actions that can be performed on network traffic flows. However, the following restrictions apply:

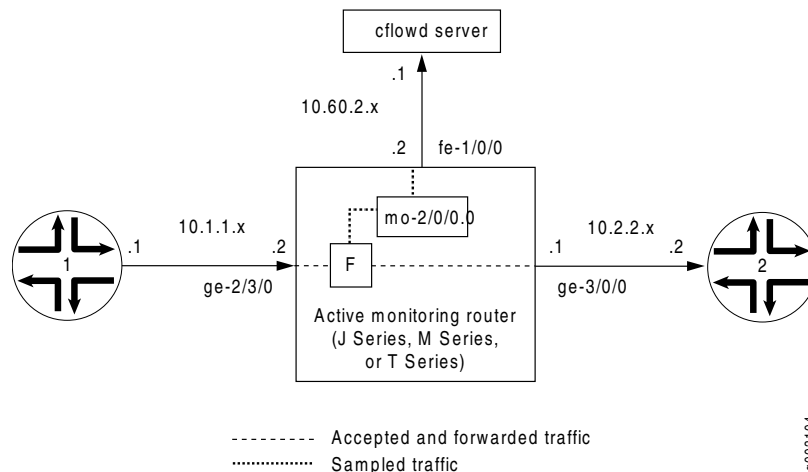
- The router can perform sampling *or* port mirroring at any one time.
- The router can perform forwarding *or* discard accounting at any one time.

Because the Monitoring Services, AS, and Multiservices PICs allow only one action to be performed at any one time, the following configuration options are available:

- Sampling and forwarding
- Sampling and discard accounting
- Port mirroring and forwarding
- Port mirroring and discard accounting
- Sampling and port mirroring on different sets of traffic

Figure 1 on page 5 shows a sample topology.

Figure 1: Active Monitoring Configuration Topology



In Figure 1 on page 5, traffic from Router 1 arrives on the monitoring router's Gigabit Ethernet **ge-2/3/0** interface. The exit interface on the monitoring router leading to destination Router 2 is **ge-3/0/0**, but this could be any interface type (such as SONET, Gigabit Ethernet, and so on). The export interface leading to the cflowd server is **fe-1/0/0**.

To enable active monitoring, configure a firewall filter on the interface **ge-2/3/0** with the following match conditions:

- Traffic matching certain firewall conditions is sent to the Monitoring Services PIC using filter-based forwarding. This traffic is quarantined and not forwarded to other routers.
- All other traffic is port-mirrored to the Monitoring Services PIC. Port mirroring copies each packet and sends the copies to the port-mirroring next hop (in this case, a Monitoring Services PIC). The original packets are forwarded out of the router as usual.

Related Documentation

- [Configuring Flow Monitoring on page 13](#)
- [Directing Replicated Flows to Multiple Flow Servers on page 23](#)
- [Configuring Services Interface Redundancy with Flow Monitoring on page 27](#)
- [Example: Configuring Active Monitoring on Logical Systems on page 29](#)

Understanding Inline Sampling

This topic provides an overview of the inline sampling feature and IPFIX and Version 9 flow collection templates used for inline sampling.

This topic contains the following sections:

- [Inline Sampling on page 6](#)
- [Inline Sampling Limitations and Restrictions on page 7](#)
- [IPFIX and Version 9 Templates on page 7](#)

Inline Sampling

The inline sampling feature on MX Series routers enables you to configure active sampling without making use of a services Dense Port Concentrator (DPC). The inline sampling is implemented on the Packet Forwarding Engine, and is carried out when the traffic enters the Packet Forwarding Engine.

Inline sampling provides for higher scalability and performance as the scaling and performance are not dependent on the capacity of the services interface. It is also cost effective in more than one way as there is no need to invest in additional hardware or to dedicate a PIC slot for the services PIC. You can make full use of the available slots for handling traffic on the device.

Junos OS Release 13.2 extends inline sampling support to VPLS flows. Now, you can configure inline sampling for IPv4, IPv6, and VPLS traffic.

The inline sampling configuration can be broadly classified into four categories:

1. Configurations at the **[edit services flow-monitoring]** hierarchy level—At this level, you configure the template properties for inline flow monitoring.
2. Configurations at the **[edit forwarding-options]** hierarchy level—At this level, you configure a sampling instance and associate the template (configured at the **[edit services flow-monitoring]** hierarchy level) with the sampling instance. At this level, you also configure the flow-server IP address and port number as well as the flow export rate.
3. Configurations at the **[edit chassis]** hierarchy level—At this level, you associate the sampling instance with the FPC on which the media interface is present. If you are configuring sampling of IPv6 flows, you must also specify the flow hash table size.
4. Configurations at the **[edit firewall]** hierarchy level—At this level you configure a firewall filter for the family of traffic to be sampled. You must attach this filter to the interface on which you want to sample the traffic.

Inline sampling supports version 9 and IPFIX flow collection templates. Support for version 9 template was introduced in Junos OS Release 13.2, and is limited to IPv4 flows. IPFIX template is supported for IPv4, IPv6, and VPLS flows. IPFIX template uses UDP as the transport protocol, whereas version 9 is transport protocol-independent.

Before you configure inline sampling, you should ensure that you have adequately-sized hash tables for IPv4 and IPv6 flow sampling. These tables can use one to fifteen 256k areas, and each table is assigned a default value of one such area. When anticipated traffic volume requires larger tables, allocate larger tables.

Inline Sampling Limitations and Restrictions

The following limitations and restrictions apply to the inline sampling feature in Junos OS:

- You can configure inline sampling only on MX Series routers that have Trio-based line cards.
- You can apply Version 9 flow template only to IPv4 traffic.
- You can configure only one sampling instance on an Flexible PIC Concentrator (FPC).
- You can configure only one type of sampling—either PIC-based sampling or inline sampling—per family in a sampling instance. However, you can configure PIC-based and inline sampling for different families in a sampling instance.
- You can configure only one collector for inline sampling.
- The following considerations apply to the inline flow-monitoring instance configuration:
 - Sampling run-length and clip-size are not supported.
 - For inline configurations, each family can support only one collector.
- Inline sampling instances can handle only up to 65536 AS paths. If the total number of AS paths exceed the maximum limit, the AS paths that have AS index greater than 65536 are discarded and counted as error. Flow records associated with such AS paths show the AS value as `0xFFFFFFFF`. However, this limitation does not impact normal forwarding operations.
- On routers with Multiservices PICs or Multiservices DPCs, all fragments of a fragmented IPv4 packet other than the first fragment of the packet are processed accurately by the flow monitoring application running on MS-PIC or MS-DPC. The flow monitoring mechanism handles such fragments accurately by setting the layer 4 related fields in the associated flows to zero.

IPFIX and Version 9 Templates

The following sections list the fields included in IPFIX and Version 9 templates.

Fields Included in the IPFIX IPv4 Template

- IPv4 Source Address
- IPv4 Destination Address
- IPv4 TOS
- IPv4 Protocol
- L4 Source Port

- L4 Destination Port
- ICMP Type and Code
- Input Interface
- VLAN ID
- IPv4 Source Mask
- IPv4 Destination Mask
- Source AS
- Destination AS
- IPv4 Next Hop Address
- TCP Flags
- Output Interface
- Number of Flow Bytes
- Number of Flow Packets
- Minimum TTL (time to live)
- Maximum TTL (time to live)
- Flow Start Time
- Flow End Time
- Flow End Reason
- 802.1Q VLAN identifier (dot1qVlanId)
- 802.1Q Customer VLAN identifier (dot1qCustomerVlanId)

Fields Included in the IPFIX IPv6 Template

- IPv6 Source Address
- IPv6 Destination Address
- IPv6 TOS
- IPv6 Protocol
- L4 Source Port
- L4 Destination Port
- ICMP Type and Code
- Input Interface
- VLAN ID
- IPv6 Source Mask
- IPv6 Destination Mask
- Source AS

- Destination AS
- IPv6 Next Hop Address
- TCP Flags
- Output Interface
- Number of Flow Bytes
- Number of Flow Packets
- Minimum Hop Limits
- Maximum Hop Limits
- Flow Start Time
- Flow End Time
- Flow End Reason
- 802.1Q VLAN identifier (dot1qVlanId)
- 802.1Q Customer VLAN identifier (dot1qCustomerVlanId)

Fields Included in the Version 9 IPv4 Template

- IPv4 Source Address
- IPv4 Destination Address
- IPv4 TOS
- IPv4 Protocol
- L4 Source Port
- L4 Destination Port
- ICMP Type and Code
- Input Interface
- VLAN ID
- IPv4 Source Mask
- IPv4 Destination Mask
- Source AS
- Destination AS
- IPv4 Next Hop Address
- BGP IPv4 Next Hop Address
- TCP Flags
- Output Interface
- Number of Flow Bytes
- Number of Flow Packets

- Time when the first packet of the flow was switched.
- Time when the last packet of flow was switched.
- Internet Protocol Version

**Related
Documentation**

- *Configuring Inline Sampling*
- [Configuring Inline Sampling on MX80 Routers on page 22](#)

PART 2

Configuration

- [Configuration Tasks on page 13](#)
- [Configuration Statements on page 33](#)

CHAPTER 2

Configuration Tasks

- [Configuring Flow Monitoring on page 13](#)
- [Configuring Inline Sampling on page 18](#)
- [Configuring Inline Sampling on MX80 Routers on page 22](#)
- [Directing Replicated Flows to Multiple Flow Servers on page 23](#)
- [Logging cflowd Flows Before Export on page 26](#)
- [Configuring Services Interface Redundancy with Flow Monitoring on page 27](#)
- [Example: Configuring Active Monitoring on Logical Systems on page 29](#)

Configuring Flow Monitoring

The flow-monitoring application performs traffic flow monitoring and enables lawful interception of traffic between two routers. Traffic flows can either be passively monitored by an offline router or actively monitored by a router participating in the network.

To configure flow monitoring you need to do the following:

- [Configuring Flow-Monitoring Interfaces on page 13](#)
- [Configuring Flow-Monitoring Properties on page 14](#)
- [Example: Configuring Flow Monitoring on page 17](#)

Configuring Flow-Monitoring Interfaces

To enable flow monitoring on the Monitoring Services PIC, include the **mo-fpc/pic/port** statement at the **[edit interfaces]** hierarchy level:

```
mo-fpc/pic/port {
  unit logical-unit-number {
    family inet {
      address address {
        destination address;
      }
      filter {
        group filter-group-number;
        input filter-name;
        output filter-name;
      }
      sampling {
```

```
        [ input output ];
    }
}
}
multiservice-options {
    (core-dump | no-core-dump);
    (syslog | no-syslog);
    flow-control-options {
        down-on-flow-control;
        dump-on-flow-control;
        reset-on-flow-control;
    }
}
}
```

Specify the physical and logical location of the flow-monitoring interface. You cannot use **unit 0**, because it is already used by internal processes. Specify the source and destination addresses. The **filter** statement allows you to associate an input or output filter or a filter group that you have already configured for this purpose. The **sampling** statement specifies the traffic direction: **input**, **output**, or both.

The **multiservice-options** statement allows you to configure properties related to flow-monitoring interfaces:

- Include the **core-dump** statement to enable storage of core files in **/var/tmp**.
- Include the **syslog** statement to enable storage of system logging information in **/var/log**.



NOTE: Boot images for monitoring services interfaces are specified at the **[edit chassis images pic]** hierarchy level. You must include the following configuration to make the flow monitoring feature operable:

```
[edit system]
ntp {
    boot-server ntp.juniper.net;
    server 172.17.28.5;
}
processes {
    ntp enable;
}
```

For more information, see the *Junos OS Administration Library for Routing Devices*.

- Include the **flow-control-options** statement to configure flow control.

Configuring Flow-Monitoring Properties

To configure flow-monitoring properties, include the **monitoring** statement at the **[edit forwarding-options]** hierarchy level:

```
monitoring name {
```

```

family inet {
  output {
    cflowd hostname port port-number;
    export-format format;
    flow-active-timeout seconds;
    flow-export-destination {
      collector-pic;
    }
    flow-inactive-timeout seconds;
    interface interface-name {
      engine-id number;
      engine-type number;
      input-interface-index number;
      output-interface-index number;
      source-address address;
    }
  }
}

```

A monitoring instance is a named entity that specifies collector information under the **monitoring name** statement. The following sections describe the properties you can configure:

- [Directing Traffic to Flow-Monitoring Interfaces on page 15](#)
- [Exporting Flows on page 16](#)
- [Configuring Time Periods when Flow Monitoring is Active and Inactive on page 16](#)

Directing Traffic to Flow-Monitoring Interfaces

To direct traffic to a flow-monitoring interface, include the **interface** statement at the **[edit forwarding-options monitoring name output]** hierarchy level. By default, the Junos OS automatically assigns values for the **engine-id** and **engine-type** statements:

- **engine-id**—Monitoring interface location.
- **engine-type**—Platform-specific monitoring interface type.

The **source-address** statement specifies the traffic source for transmission of cflowd information; you must configure it manually. If you provide a different **source-address** statement for each monitoring services output interface, you can track which interface processes a particular cflowd record.

By default, the **input-interface-index** value is the SNMP index of the input interface. You can override the default by including a specific value. The **input-interface-index** and **output-interface-index** values are exported in fields present in the cflowd version 5 flow format.



NOTE: On J Series Services Routers, cflowd sampling in the input direction of an interface reports the output interface index as 0.

Exporting Flows

To direct traffic to a flow collection interface, include the **flow-export-destination** statement. For more information about flow collection, see *Flow Collection*.

To configure the cflowd version number, include the **export-format** statement at the **[edit forwarding-options monitoring name output]** hierarchy level. By default, version 5 is used. Version 8 enables the router software to aggregate the flow information using broader criteria and reduce cflowd traffic. Version 8 aggregation is performed periodically (every few seconds) on active flows and when flows are allowed to expire. Because the aggregation is performed periodically, active timeout events are ignored.

For more information on cflowd properties, see *Enabling Flow Aggregation*.

Configuring Time Periods when Flow Monitoring is Active and Inactive

To configure time periods for active flow monitoring and intervals of inactivity, include the **flow-active-timeout** and **flow-inactive-timeout** statements at the **[edit forwarding-options monitoring name output]** hierarchy level:

- The **flow-active-timeout** statement specifies the time interval between flow exports for active flows. 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.

This timer is needed to provide periodic updates when a flow has a long duration. The active timeout setting enables the router to retain the start time for the flow as a constant and send out periodic cflowd reports. This in turn allows the collector to register the start time and determine that a flow has survived for a duration longer than the configured active timeout.



NOTE: In active flow monitoring, the cflowd records are exported after a time period that is a multiple of 60 seconds and greater than or equal to the configured active timeout value. For example, if the active timeout value is 90 seconds, the cflowd records are exported at 120-second intervals. If the active timeout value is 150 seconds, the cflowd records are exported at 180-second intervals, and so forth.

- The **flow-inactive-timeout** statement specifies the interval of inactivity for a flow that triggers the flow export. 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.

If the flow stops transmitting for longer than the configured inactive timeout value, the router purges it from the flow table and exports the cflowd record. As a result, the flow is forgotten as far as the PIC is concerned and if the same 5-tuple appears again, it is assigned a new start time and considered a new flow.

Both timers are necessary. The active timeout setting is needed to provide information for flows that constantly transmit packets for a long duration. The inactive timeout setting

enables the router to purge flows that have become inactive and would waste tracking resources.



NOTE: The router must contain an Adaptive Services, Multiservices, or Monitoring Services PIC for the `flow-active-timeout` and `flow-inactive-timeout` statements to take effect.

Example: Configuring Flow Monitoring

The following is an example of flow-monitoring properties configured to support input SONET/SDH interfaces, output monitoring services interfaces, and export to cflowd for flow analysis. To complete the configuration, you also need to configure the interfaces and set up a virtual private network (VPN) routing and forwarding (VRF) instance. For a complete example, see the *Junos OS Feature Guides*. For information on cflowd, see *Enabling Flow Aggregation*.

```
[edit forwarding-options]
monitoring group1 {
  family inet {
    output {
      cflowd 192.168.245.2 port 2055;
      export-format cflowd-version-5;
      flow-active-timeout 60;
      flow-inactive-timeout 30;
      interface mo-4/0/0.1 {
        engine-id 1;
        engine-type 1;
        input-interface-index 44;
        output-interface-index 54;
        source-address 192.168.245.1;
      }
      interface mo-4/1/0.1 {
        engine-id 2;
        engine-type 1;
        input-interface-index 45;
        output-interface-index 55;
        source-address 192.168.245.1;
      }
      interface mo-4/2/0.1 {
        engine-id 3;
        engine-type 1;
        input-interface-index 46;
        output-interface-index 56;
        source-address 192.168.245.1;
      }
      interface mo-4/3/0.1 {
        engine-id 4;
        engine-type 1;
        input-interface-index 47;
        output-interface-index 57;
        source-address 192.168.245.1;
      }
    }
  }
}
```

```
    }  
  }  
}
```

**Related
Documentation**

- [Active Flow Monitoring Overview on page 3](#)
- [Directing Replicated Flows to Multiple Flow Servers on page 23](#)
- [Configuring Services Interface Redundancy with Flow Monitoring on page 27](#)
- [Example: Configuring Active Monitoring on Logical Systems on page 29](#)

Configuring Inline Sampling

On MX Series routers and EX Series switches, you can configure active sampling to be performed on an inline data path without the need for a services Dense Port Concentrator (DPC). To do this, you define a sampling instance with specific properties. One Flexible PIC Concentrator (FPC) can support only one instance; for each instance, either services PIC-based sampling or inline sampling is supported per family. As a result, a particular instance can define PIC-based sampling for one family and inline sampling for a different family. Both IPv4 and IPv6 are supported for inline sampling.

Inline sampling supports version 9 and IPFIX flow collection templates. Support for version 9 template was introduced in Junos OS Release 13.2, and is limited to IPv4 flows. IPFIX template is supported for IPv4, IPv6, and VPLS flows. IPFIX template uses UDP as the transport protocol, whereas version 9 is transport protocol-independent.

The following limitations exist for inline sampling:

- Flow records and templates cannot be exported if the flow collector is reachable through any management interface.
- The flow collector should be reachable through the default routing table (inet.0 or inet6.0). If the flow collector is reachable via a non-default VPN routing and forwarding table (VRF), flow records and templates cannot be exported.
- If the destination of the sampled flow is reachable through multiple paths, the IP_NEXT_HOP (Element ID 15) and OUTPUT_SNMP (Element ID 14) in the IPv4 flow record would be set to the Gateway Address and SNMP Index of the first path seen in the forwarding table.
- If the destination of the sampled flow is reachable through multiple paths, the IP_NEXT_HOP (Element ID 15) and OUTPUT_SNMP (Element ID 14) in the IPv6 flow records would be set to 0.
- The user-defined sampling instance gets precedence over the global instance. When a user-defined sampling instance is attached to the FPC, the global instance is removed from the FPC and the user-defined sampling instance is applied to the FPC.
- The Incoming Interface (IIF) and Outgoing Interface (OIF) should be part of the same VRF. If OIF is in a different VRF, DST_MASK (Element ID 13), DST_AS (Element ID 17),

IP_NEXT_HOP (Element ID 15), and OUTPUT_SNMP (Element ID 14) would be set to 0 in the flow records.

- Each Lookup Chip (LU) maintains and exports flows independent of other LUs. Traffic received on a media interface is distributed across all LUs in a multi-LU platform. It is likely that a single flow will be processed by multiple LUs. Therefore, each LU creates a unique flow and exports it to the flow collector. This can cause duplicate flows records to be seen on the flow collector. The flow collector should aggregate PKTS_COUNT and BYTES_COUNT for duplicate flow records to derive a single flow record.

Before you configure inline sampling, you should ensure that you have adequately-sized hash tables for IPv4 and IPv6 flow sampling. These tables can use one to fifteen 256k areas, and each table is assigned a default value of one such area. When anticipated traffic volume requires larger tables, allocate larger tables.



NOTE: For Junos OS releases earlier than Release 12.1, the following points are applicable for supporting backward compatibility when you configure the IPv4 and IPv6 flow table sizes for inline sampling:

- If you do not configure the `flow-table-size` statement at the `[edit chassis fpc slot-number inline-services]` hierarchy level, fifteen 256K entries are allocated by default for the IPv4 flow table and one 1K entry is allocated by default for the IPv6 flow table on the Packet Forwarding Engine.
- If you configure the `ipv4-flow-table-size size` statement at the `[edit chassis fpc slot-number inline-services flow-table-size]` hierarchy level and if you do not configure the `ipv6-flow-table-size size` statement at the `[edit chassis fpc slot-number inline-services flow-table-size]` hierarchy level, the number of units of 256K entries that you configure for the IPv4 flow table is allocated. For the IPv6 flow table, a default size of one 1K entry is allocated on the Packet Forwarding Engine.
- If you do not configure the `ipv4-flow-table-size size` statement at the `[edit chassis fpc slot-number inline-services flow-table-size]` hierarchy level and if you configure the `ipv6-flow-table-size size` statement at the `[edit chassis fpc slot-number inline-services flow-table-size]` hierarchy level, the number of units of 256K entries that you configure for the IPv6 flow table is allocated. For the IPv4 flow table, a default size of one 1K entry is allocated on the Packet Forwarding Engine.
- If you configure the sizes of both the IPv4 and IPv6 flow tables, the flow tables are created on the Packet Forwarding Engine based on the size that you specified.

To allocate IPv4 and IPv6 flow hash tables:

1. Go to the `flow-table-size` hierarchy level for inline services on the FPC that processes the monitored flows.

```
[edit]
user@host# edit chassis fpc 0 inline-services flow-table-size
```

2. Specify the required sizes for the sampling hash tables.

```
[edit chassis fpc 0 inline-services flow-table-size]
user@host# set ipv4-flow-table-size 5
user@host# set ipv6-flow-table-size 5
```



NOTE: When you set the flow hash table sizes, remember:

- Any change in the configured size of flow hash table sizes initiates an automatic reboot of the FPC.
- The total number of units used for both IPv4 and IPv6 cannot exceed 15.

The configuration for inline sampling on MX80 routers is slightly different.

To configure inline sampling on all other MX Series routers and EX Series switches:

1. Enable inline sampling and specify the source address for the traffic.

```
[edit forwarding-options sampling instance instance-name family inet output]
user@host# set inline-jflow source address address
```

2. Specify the IP_FIX output format.

```
[edit forwarding-options sampling instance instance-name family inet output flow-server
address]
user@host# set version-ipfix template ipv4
```

3. Specify the output properties.

```
[edit services flow-monitoring]
user@host# set version-ipfix
```

The output format properties are common to other output formats and are described in “*Configuring Flow Aggregation to Use IPFIX Flow Templates*”.

The following is an example of the sampling configuration for an instance that supports inline sampling on **family inet** and PIC-based sampling on **family inet6**:

```
[edit forwarding-options]
sampling {
  instance {
    sample-ins1 {
      input {
        rate 1;
      }
      family inet {
        output {
          flow-server 2.2.2.2 {
            port 2055;
            version-ipfix {
              template {
                ipv4;
              }
            }
          }
        }
      }
    }
  }
}
```

```

        inline-jflow {
            source-address 10.11.12.13;
        }
    }
}
family inet6 {
    output {
        flow-server 2.2.2.2 {
            port 2055;
            version-ipfix {
                template {
                    ipv6;
                }
            }
        }
    }
    interface sp-0/1/0 {
        source-address 10.11.12.13;
    }
}
}
}
}
}

```

The following example shows the output format configuration:

```

services {
    flow-monitoring {
        version-ipfix {
            template ipv4 {
                flow-active-timeout 60;
                flow-inactive-timeout 60;
                ipv4-template;
                template-refresh-rate {
                    packets 1000;
                    seconds 10;
                }
                option-refresh-rate {
                    packets 1000;
                    seconds 10;
                }
            }
        }
    }
}
}
}
}

```

The following considerations apply to the inline flow-monitoring instance configuration:

- Sampling run-length and clip-size are not supported.
- For inline configurations, each family can support only one collector.



NOTE: Inline sampling instances can handle only up to 65536 AS paths. If the total number of AS paths exceed the maximum limit, the AS paths that have AS index greater than 65536 are discarded and counted as error. Flow records associated with such AS paths show the AS value as `0xFFFFFFFF`. However, this limitation does not impact normal forwarding operations.



NOTE: On routers with Multiservices PICs or Multiservices DPCs, all fragments of a fragmented IPv4 packet other than the first fragment of the packet are processed accurately by the flow monitoring application running on MS-PIC or MS-DPC. The flow monitoring mechanism handles such fragments accurately by setting the layer 4 related fields in the associated flows to zero.

**Related
Documentation**

- [Configuring Inline Sampling on MX80 Routers on page 22](#)
- [inline-jflow](#)

Configuring Inline Sampling on MX80 Routers

To configure inline sampling on MX80 routers:

1. Associate a sampling instance with the Forwarding Engine Processor.

[edit]

```
user@host# set chassis tfeb slot sampling-instance sampling-instance
```

The Forwarding Engine Processor slot is always **0** because MX80 routers have only one Packet Forwarding Engine. In this configuration, the sampling instance is **sample-ins1**.

[edit]

```
user@host# set chassis tfeb 0 sampling-instance sample-ins1
```



NOTE: MX80 routers support only one sampling instance.

2. Configure the rate at the **[edit forwarding-options sampling instance instance-name input]** hierarchy level to apply specific values for the sampling instance **sample-ins1**.

[edit forwarding-options sampling instance sample-ins1 input]

```
user@host# set rate number
```

In this configuration, the rate is **1000**.

[edit forwarding-options sampling instance sample-ins1 input]

```
user@host# set rate 1000
```

3. Enable inline sampling and specify the source address for the traffic.

[edit forwarding-options sampling instance sample-ins1 family inet output]

```
user@host# set inline-jflow source-address address
```

In this configuration, the source address is 10.11.12.13.

```
[edit forwarding-options sampling instance sample-ins1 family inet output]
user@host# set inline-jflow source-address 10.11.12.13
```

4. Specify the output properties.

```
[edit services flow-monitoring]
user@host# set version-ipfix
```

The output format properties are common to other output formats and are described in “*Configuring Flow Aggregation to Use IPFIX Flow Templates*”.

The following is an example of the sampling configuration for an instance that supports inline sampling on MX80 routers:

```
[edit forwarding-options]
sampling {
  instance {
    sample-ins1 {
      input {
        rate 1000;
      }
      family inet {
        output {
          inline-jflow {
            source-address 10.11.12.13;
          }
        }
      }
    }
  }
}
```



NOTE: You need not configure a Flexible PIC Concentrator (FPC) slot because MX80 routers have only one Packet Forwarding Engine.

The following considerations apply to the inline flow-monitoring instance configuration:

- This configuration does not support MPLS-IPv6.
- Clip-size is not supported.

Related Documentation

- [Configuring Flow Aggregation to Use IPFIX Flow Templates](#)
- [Configuring Inline Sampling on page 18](#)
- *inline-jflow*

Directing Replicated Flows to Multiple Flow Servers

You can configure replication of the sampled flow records for use by multiple flow servers. You can use either sampling based on the Routing Engine, using cflowd version 5 or

version 8, or sampling based on the services PIC, using flow aggregation version 9, as described in the following sections:

- [Directing Replicated Routing Engine–Based Sampling Flows to Multiple Servers on page 24](#)
- [Directing Replicated Version 9 Flow Aggregates to Multiple Servers on page 25](#)

Directing Replicated Routing Engine–Based Sampling Flows to Multiple Servers

Routing Engine–based sampling supports up to eight flow servers for both cflowd version 5 and version 8 configurations. The total number of servers is limited to eight regardless of how many are configured for cflowd v5 or v8.

When you configure cflowd-based sampling, the export packets are replicated to all flow servers configured to receive them. If two servers are configured to receive v5 records, both the servers will receive records for a specified flow.



NOTE: With Routing Engine–based sampling, if multiple flow servers are configured with version 8 export format, all of them must use the same aggregation type. For example, all servers receiving version 8 export could be configured for source-destination aggregation type.

The following configuration example allows replication of export packets to two flow servers.

```
forwarding-options {
  sampling {
    instance inst1 {
      input {
        rate 1;
      }
      family inet;
      output {
        flow-server 10.10.3.2 {
          port 2055;
          version 5;
          source-address 192.168.164.119;
        }
        flow-server 172.17.20.62 {
          port 2055;
          version 5;
          source-address 192.168.164.119;
        }
      }
    }
  }
}
```


Directing Replicated Version 9 Flow Aggregates to Multiple Servers

The export packets generated for a template are replicated to all the flow servers that are configured to receive information for that template. The maximum number of servers supported is eight.

This also implies that periodic updates required by version 9 (RFC 3954) are sent to each configured collector. The following updates are sent periodically as part of this requirement:

- Options data
- Template definition

The refresh period for options data and template definition is configured on a per-template basis at the **[edit services flow-monitoring]** hierarchy level.

The following configuration example allows replication of version 9 export packets to two flow servers.

```
forwarding-options {
  sampling {
    instance inst1 {
      input {
        rate 1;
      }
      family inet;
      output {
        flow-server 10.10.3.2 {
          port 2055;
          version9 {
            template {
              ipv4;
            }
          }
        }
        flow-server 172.17.20.62 {
          port 2055;
          version9 {
            template {
              ipv4;
            }
          }
        }
      }
    }
    flow-inactive-timeout 30;
    flow-active-timeout 60;
    interface sp-4/0/0 {
      source-address 10.10.3.4;
    }
  }
}
```

**Related
Documentation**

- [Active Flow Monitoring Overview on page 3](#)
- [Configuring Flow Monitoring on page 13](#)
- [Configuring Services Interface Redundancy with Flow Monitoring on page 27](#)
- [Example: Configuring Active Monitoring on Logical Systems on page 29](#)

Logging cflowd Flows Before Export

To collect the cflowd flows in a log file before they are exported, include the **local-dump** statement at the **[edit forwarding-options sampling output flow-server *hostname*]** hierarchy level:

```
[edit forwarding-options sampling output flow-server hostname]  
local-dump;
```

By default, the flows are collected in **/var/log/sampled**; to change the filename, include the **filename** statement at the **[edit forwarding-options sampling traceoptions]** hierarchy level. For more information about changing the filename, see *Configuring Traffic Sampling Output*.



NOTE: Because the **local-dump** statement adds extra overhead, you should use it only while debugging cflowd problems, not during normal operation.

The following is an example of the flow information. The AS number exported is the origin AS number. All flows that belong under a cflowd header are dumped, followed by the header itself:

```
Jun 27 18:35:43 v5 flow entry  
Jun 27 18:35:43   Src addr: 192.53.127.1  
Jun 27 18:35:43   Dst addr: 192.6.255.15  
Jun 27 18:35:43   Nhop addr: 192.6.255.240  
Jun 27 18:35:43   Input interface: 5  
Jun 27 18:35:43   Output interface: 3  
Jun 27 18:35:43   Pkts in flow: 15  
Jun 27 18:35:43   Bytes in flow: 600  
Jun 27 18:35:43   Start time of flow: 7230  
Jun 27 18:35:43   End time of flow: 7271  
Jun 27 18:35:43   Src port: 26629  
Jun 27 18:35:43   Dst port: 179  
Jun 27 18:35:43   TCP flags: 0x10  
Jun 27 18:35:43   IP proto num: 6  
Jun 27 18:35:43   TOS: 0xc0  
Jun 27 18:35:43   Src AS: 7018  
Jun 27 18:35:43   Dst AS: 11111  
Jun 27 18:35:43   Src netmask len: 16  
Jun 27 18:35:43   Dst netmask len: 0
```

[... 41 more version 5 flow entries; then the following header:]

```
Jun 27 18:35:43 cflowd header:  
Jun 27 18:35:43   Num-records: 42  
Jun 27 18:35:43   Version: 5  
Jun 27 18:35:43   low seq num: 118
```

Jun 27 18:35:43 Engine id: 0
 Jun 27 18:35:43 Engine type: 3

**Related
Documentation**

- [Active Flow Monitoring Overview on page 3](#)
- [Configuring Flow Monitoring on page 13](#)
- [Directing Replicated Flows to Multiple Flow Servers on page 23](#)
- [Configuring Services Interface Redundancy with Flow Monitoring on page 27](#)
- [Example: Configuring Active Monitoring on Logical Systems on page 29](#)

Configuring Services Interface Redundancy with Flow Monitoring

Active monitoring services configurations on AS, Multiservices PICs, and Multiservices DPCs support redundancy. To configure redundancy, you specify a redundancy services PIC (**rsp**) interface in which the primary AS or Multiservices PIC is active and a secondary PIC is on standby. If the primary PIC fails, the secondary PIC becomes active, and all service processing is transferred to it. If the primary PIC is restored, it remains on standby and does not preempt the secondary PIC; you need to manually restore the services to the primary PIC. To determine which PIC is currently active, issue the **show interfaces redundancy** command.



NOTE: On flow-monitoring configurations, the only service option supported is *warm standby*, in which one backup PIC supports multiple working PICs. Recovery times are not guaranteed, because the configuration must be completely restored on the backup PIC after a failure is detected. However, configuration is preserved and available on the new active PIC.

As with the other services that support warm standby, you can issue the **request interfaces (revert | switchover)** command to switch manually between the primary and secondary flow monitoring interfaces.

For more information, see *Configuring AS or Multiservices PIC Redundancy*. For information on operational mode commands, see the *Junos OS Operational Mode Commands*.

A sample configuration follows.

```
interface {
  rsp0 {
    redundancy-options {
      primary sp-0/0/0;
      secondary sp-1/3/0;
    }
    unit 0 {
      family inet;
    }
  }
}
interface {
```

```
ge-0/2/0 {
  unit 0 {
    family inet {
      filter {
        input as_sample;
      }
    }
    address 10.58.255.49/28;
  }
}
forwarding-options {
  sampling {
    instance instance1 { # named instances of sampling parameters
      input {
        rate 1;
        run-length 0;
        max-packets-per-second 65535;
      }
      family inet {
        output {
          flow-server 10.10.10.2 {
            port 5000;
            version 5;
          }
          flow-active-timeout 60;
          interface rsp0 {
            source-address 10.10.10.1;
          }
        }
      }
    }
  }
}
firewall {
  filter as_sample {
    term t1 {
      then {
        sample;
        accept;
      }
    }
  }
}
```

**Related
Documentation**

- [Active Flow Monitoring Overview on page 3](#)
- [Configuring Flow Monitoring on page 13](#)
- [Directing Replicated Flows to Multiple Flow Servers on page 23](#)
- [Example: Configuring Active Monitoring on Logical Systems on page 29](#)

Example: Configuring Active Monitoring on Logical Systems

This example shows a sample configuration that allows you to configure active monitoring on a logical system. The following section shows the configuration on the master router:

```
[edit forwarding-options]
sampling {
  instance inst1 {
    input {
      rate 1;
    }
    family inet;
    output {
      flow-server 2.2.2.2 {
        port 2055;
        version9 {
          template {
            ipv4;
          }
        }
      }
    }
    interface sp-0/1/0 {
      source-address 10.11.12.13;
    }
  }
}
family mpls;
output {
  flow-server 2.2.2.2 {
    port 2055;
    version9 {
      template {
        mpls;
      }
    }
  }
}
interface sp-0/1/0 {
  source-address 10.11.12.13;
}
}
services {
  flow-monitoring {
    version9 {
      template ipv4 {
        flow-active-timeout 60;
        flow-inactive-timeout 60;
        ipv4-template;
        template-refresh-rate {
          packets 1000;
          seconds 10;
        }
      }
    }
  }
}
```

```
        option-refresh-rate {
            packets 1000;
            seconds 10;
        }
    }
    template mpls {
        mpls-template;
    }
}
}
```

The configuration for the logical router uses the input parameters and the output interface for sampling from the master router. Each logical router should have separate template definitions for the flow-server configuration. The following section shows the configuration on the logical router:

```
logical-systems {
    ls-1 {
        firewall {
            family inet {
                filter test-sample {
                    term term-1 {
                        then {
                            sample;
                            accept;
                        }
                    }
                }
            }
        }
        interfaces {
            ge-0/0/1 {
                unit 0 {
                    family inet {
                        filter {
                            input test-sample;
                            output test-sample;
                        }
                    }
                }
            }
        }
        forwarding-options {
            sampling {
                instance sample-inst1 {
                    family inet;
                    output {
                        flow-server 2.2.2.2 {
                            port 2055;
                            version 9 {
                                template {
                                    ipv4-ls1;
                                }
                            }
                        }
                    }
                }
            }
        }
    }
}
```


CHAPTER 3

Configuration Statements

- [\[edit interfaces\] Hierarchy Level on page 33](#)
- [\[edit forwarding-options\] Hierarchy Level on page 34](#)

[\[edit interfaces\] Hierarchy Level](#)

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

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

```
}
so-fpc/pic/port {
  unit logical-unit-number {
    passive-monitor-mode;
  }
}
```

- Related Documentation**
- [\[edit forwarding-options\] Hierarchy Level on page 34](#)
 - [\[edit services flow-monitoring\] Hierarchy Level](#)

[edit forwarding-options] Hierarchy Level

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

```
[edit forwarding-options]
accounting name {
  output {
    aggregate-export-interval seconds;
    cflowd hostname {
      aggregation {
        autonomous-system;
        destination-prefix;
        protocol-port;
        source-destination-prefix {
          caida-compliant;
        }
        source-prefix;
      }
      autonomous-system-type (origin | peer);
      port port-number;
      version format;
    }
    flow-active-timeout seconds;
    flow-inactive-timeout seconds;
    interface interface-name {
      engine-id number;
      engine-type number;
      source-address address;
    }
  }
}
monitoring name {
  family family {
    output {
      cflowd hostname port port-number;
      export-format format;
      flow-active-timeout seconds;
      flow-export-destination {
        collector-pic;
      }
      flow-inactive-timeout seconds;
      interface interface-name {
        engine-id number;
      }
    }
  }
}
```

```

        engine-type number;
        input-interface-index number;
        output-interface-index number;
        source-address address;
    }
}
next-hop-group group-names {
    interface interface-name {
        next-hop address;
    }
}
port-mirroring {
    input {
        rate rate;
        run-length number;
        maximum-packet-length bytes
    }
    family (inet | inet6) {
        output {
            interface interface-name {
                next-hop address;
            }
            no-filter-check;
        }
    }
    traceoptions {
        file filename {
            files number;
            size bytes;
            (world-readable | no-world-readable);
        }
    }
}
sampling {
    disable;
    sample-once;
    input {
        rate number;
        run-length number;
        max-packets-per-second number;
        maximum-packet-length bytes;
    }
    traceoptions {
        no-remote-trace;
        file filename <files number> <size bytes> <match expression> <world-readable |
            no-world-readable>;
    }
    family (inet | inet6 | mpls) {
        disable;
        output {
            aggregate-export-interval seconds;
            flow-active-timeout seconds;
            flow-inactive-timeout seconds;
            extension-service service-name;
            flow-server hostname {

```

```
aggregation {
    autonomous-system;
    destination-prefix;
    protocol-port;
    source-destination-prefix {
        caida-compliant;
    }
    source-prefix;
}
autonomous-system-type (origin | peer);
(local-dump | no-local-dump);
port port-number;
source-address address;
version format;
version9 {
    template template-name;
}
}
interface interface-name {
    engine-id number;
    engine-type number;
    source-address address;
}
file {
    disable;
    filename filename;
    files number;
    size bytes;
    (stamp | no-stamp);
    (world-readable | no-world-readable);
}
}
instance instance-name {
    disable;
    input {
        rate number;
        run-length number;
        max-packets-per-second number;
        maximum-packet-length bytes;
    }
    family (inet | inet6 | mpls) {
        disable;
        output {
            aggregate-export-interval seconds;
            flow-active-timeout seconds;
            flow-inactive-timeout seconds;
            extension-service service-name;
            flow-server hostname {
                aggregation {
                    autonomous-system;
                    destination-prefix;
                    protocol-port;
                    source-destination-prefix {
                        caida-compliant;
                    }
                }
            }
        }
    }
}
```

```

        source-prefix;
    }
    autonomous-system-type (origin | peer);
    (local-dump | no-local-dump);
    port port-number;
    source-address address;
    version format;
    version9 {
        template template-name;
    }
}
interface interface-name {
    engine-id number;
    engine-type number;
    source-address address;
}
inline-jflow {
    source-address address;
    flow-export-rate rate;
}
}
}
}
}

```



NOTE: For the complete [edit forwarding-options] hierarchy, see the *Routing Policy Feature Guide for Routing Devices*. This section documents only the statements used in flow monitoring and accounting services.

**Related
Documentation**

- [\[edit interfaces\] Hierarchy Level on page 33](#)
- [\[edit services flow-monitoring\] Hierarchy Level](#)


address (Interfaces)

Syntax	<pre>address address { destination address; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the interface address.
Options	<p>address—Address of the interface.</p> <p>The remaining statement is explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• <i>Junos OS Network Interfaces Library for Routing Devices</i> for other options not associated with flow monitoring.• Configuring Flow Monitoring on page 13• <i>Configuring Traffic Sampling</i>

cflowd (Discard Accounting)

Syntax	<pre> cflowd <i>hostname</i> { aggregation { autonomous-system; destination-prefix; protocol-port; source-destination-prefix { caida-compliant; } source-prefix; } autonomous-system-type (origin peer); label-position { template <i>template-name</i>; } (local-dump no-local-dump); port <i>port-number</i>; source-address (Forwarding Options) <i>address</i>; version <i>format</i>; } </pre>
Hierarchy Level	[edit forwarding-options accounting <i>name</i> output],
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Collect an aggregate of sampled flows and send the aggregate to a specified host system that runs the collection utility cfdcollect.</p> <p>You can configure up to one version 5 and one version 8 flow format at the [edit forwarding-options accounting <i>name</i> output] hierarchy level.</p>
Options	<p>hostname—The IP address or identifier of the host system (the workstation running the cflowd utility).</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Enabling Flow Aggregation

core-dump

Syntax	(core-dump no-core-dump);
Hierarchy Level	[edit interfaces mo- <i>fpc/pic/port</i> multiservice-options]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>A useful tool for isolating the cause of a problem. Core dumping is enabled by default. The directory /var/tmp contains core files. The Junos OS saves the current core file (0) and the four previous core files, which are numbered from 1 through 4 (from newest to oldest):</p> <div><p>NOTE: By default, all members of a configured user group (with read-only permissions) can access the core dump files and attach them to cases associated with JTAC.</p></div>
	<ul style="list-style-type: none">• core-dump—Enable the core dumping operation.• no-core-dump—Disable the core dumping operation.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Flow Monitoring on page 13


destination (Interfaces)

Syntax	<code>destination address;</code>
Hierarchy Level	<pre>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> tunnel] [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet address <i>address</i>], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> tunnel] [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet address <i>address</i>]</pre>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>For CoS on ATM interfaces, specify the remote address of the connection.</p> <p>For point-to-point interfaces only, specify the address of the interface at the remote end of the connection.</p> <p>For tunnel and encryption interfaces, specify the remote address of the tunnel.</p>
Options	address —Address of the remote side of the connection.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Linear RED Profiles on ATM Interfaces</i> • <i>Multilink and Link Services Logical Interface Configuration Overview</i> • <i>Configuring Encryption Interfaces</i> • <i>Configuring Traffic Sampling</i> • Configuring Flow Monitoring on page 13 • <i>Configuring Unicast Tunnels</i>

engine-id (Forwarding Options)

Syntax	engine-id <i>number</i> ;
Hierarchy Level	[edit forwarding-options accounting <i>name</i> output interface <i>interface-name</i>], [edit forwarding-options monitoring <i>name</i> output interface <i>interface-name</i>], [edit forwarding-options sampling instance <i>instance-name</i> family (inet inet6 mpls) output interface <i>interface-name</i>], [edit forwarding-options sampling family (inet inet6 mpls) output interface <i>interface-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the engine ID number for flow monitoring and accounting services.
Options	<i>number</i> —Identity of accounting interface.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Traffic Sampling• Configuring Flow Monitoring on page 13• Configuring Discard Accounting

engine-type

Syntax	<code>engine-type <i>number</i>;</code>
Hierarchy Level	<p>[edit forwarding-options accounting <i>name</i> output interface <i>interface-name</i>],</p> <p>[edit forwarding-options monitoring <i>name</i> output interface <i>interface-name</i>],</p> <p>[edit forwarding-options sampling instance <i>instance-name</i> family (inet inet6 mpls) output interface <i>interface-name</i>],</p> <p>[edit forwarding-options sampling family (inet inet6 mpls) output interface <i>interface-name</i>]</p>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Specify the engine type number for flow monitoring and accounting services. The engine type attribute refers to the type of the flow switching engine, such as the route processor or a line module. The configured engine type is inserted in output cflowd packets. The Source ID, a 32-bit value to ensure uniqueness for all flows exported from a particular device, is the equivalent of the engine type and the engine ID fields.</p>
	<div>  <p>NOTE: You must configure a source address in the output interface statements. The interface-level statement of engine-type is added automatically but you may override this value with manually configured statements to track different flows with a single cflowd collector.</p> </div>
Options	<i>number</i> —Platform-specific accounting interface type.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Traffic Sampling • Configuring Flow Monitoring on page 13 • Configuring Discard Accounting

export-format

Syntax	export-format <i>format</i> ;
Hierarchy Level	[edit forwarding-options monitoring name output]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Flow monitoring export format.
Options	<i>format</i> —Format of the flows. Values: 5 or 8 Default: 5
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• version• Exporting Flows on page 16

family (Monitoring)

```
Syntax  family inet {
        output {
            flow-active-timeout seconds;
            flow-inactive-timeout seconds;
            export-format format;
            cflowd hostname {
                aggregation {
                    autonomous-system;
                    destination-prefix;
                    protocol-port;
                    source-destination-prefix {
                        caida-compliant;
                    }
                    source-prefix;
                }
            }
            port port-number;
        }
        interface interface-name {
            engine-id number;
            engine-type number;
            input-interface-index number;
            output-interface-index number;
            source-address address;
        }
    }
```

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify input and output interfaces and properties for flow monitoring. Only IPv4 (**inet**) is supported.

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 Flow Monitoring on page 13](#)

filter

Syntax	<pre>filter { input <i>filter-name</i>; output <i>filter-name</i>; group <i>filter-group-number</i>; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Apply a firewall filter to an interface. You can also use filters for encrypted traffic.
Options	<p>group <i>filter-group-number</i>—Define an interface to be part of a filter group. The default filter group number is 0.</p> <p>input <i>filter-name</i>—Name of one filter to evaluate when packets are received on the interface.</p> <p>output <i>filter-name</i>—Name of one filter to evaluate when packets are transmitted on the interface.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Routing Policy Feature Guide for Routing Devices</i> or the <i>Junos OS Administration Library for Routing Devices</i>• Configuring Flow Monitoring on page 13


flow-active-timeout

Syntax	flow-active-timeout <i>seconds</i> ;
Hierarchy Level	[edit forwarding-options accounting <i>name</i> output], [edit forwarding-options monitoring <i>name</i> output], [edit forwarding-options sampling instance <i>instance-name</i> family (inet inet6 mpls) output], [edit forwarding-options sampling family (inet inet6 mpls) output], [edit services flow-monitoring version9]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Interval after which an active flow is exported.
<div>  <p>NOTE: The router must include an Adaptive Services, Multiservices, or Monitoring Services PIC for this statement to take effect.</p> </div>	
Options	<p>seconds—Duration of the timeout period.</p> <p>Range: 60 through 1800 seconds (for forwarding-options configurations); 10 through 600 seconds (for services configurations)</p> <p>Default: 1800 seconds (for forwarding-options configurations); 60 seconds (for services configurations)</p>
<div>  <p>NOTE: In active flow monitoring, the cflowd records are exported after a time period that is a multiple of 60 seconds and greater than or equal to the configured active timeout value. For example, if the active timeout value is 90 seconds, the cflowd records are exported at 120-second intervals. If the active timeout value is 150 seconds, the cflowd records are exported at 180-second intervals, and so forth.</p> </div>	
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Time Periods when Flow Monitoring is Active and Inactive on page 16 • Configuring the Version 9 Template Properties

flow-export-destination

Syntax	<code>flow-export-destination { (cflowd-collector collector-pic); }</code>
Hierarchy Level	[edit forwarding-options monitoring <i>group-name</i> family inet output]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure flow collection.
Options	<code>cflowd-collector</code> —cflowd collector. <code>collector-pic</code> —Collector PIC.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Exporting Flows on page 16

flow-inactive-timeout

Syntax	flow-inactive-timeout <i>seconds</i> ;
Hierarchy Level	[edit forwarding-options accounting <i>name</i> output], [edit forwarding-options monitoring <i>name</i> output], [edit forwarding-options sampling instance <i>instance-name</i> family (inet inet6 mpls) output], [edit forwarding-options sampling family (inet inet6 mpls) output], [edit services flow-monitoring version9]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Interval of inactivity that marks a flow inactive.
<div>  <p>NOTE: The router must include an Adaptive Services, Multiservices, or Monitoring Services PIC for this statement to take effect.</p> </div>	
Options	<p>seconds—Duration of the timeout period.</p> <p>Range: 60 through 1800 seconds (for forwarding-options configurations); 10 through 600 seconds (for services configurations)</p> <p>Default: 1800 seconds (for forwarding-options configurations); 60 seconds (for services configurations)</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Time Periods when Flow Monitoring is Active and Inactive on page 16 • Configuring the Version 9 Template Properties

flow-table-size

Syntax	<pre>flow-table-size { ipv4-flow-table-size <i>units</i>; ipv6-flow-table-size <i>units</i>; }</pre>
Hierarchy Level	[edit chassis fpc <i>slot-number</i> inline-services]
Release Information	Statement introduced in Junos OS Release 12.1.
Description	Configure the size of hash tables for inline services sampling.
Options	The remaining statements are defined separately.

input-interface-index

Syntax	<code>input-interface-index <i>number</i>;</code>
Hierarchy Level	[edit forwarding-options monitoring <i>name</i> output interface <i>interface-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify a value for the input interface index that overrides the default supplied by SNMP.
Options	<i>number</i> —Input interface index value.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Flow Monitoring on page 13

interface (Accounting or Sampling)

Syntax	<pre>interface <i>interface-name</i> { engine-id <i>number</i>; engine-type <i>number</i>; source-address <i>address</i>; }</pre>
Hierarchy Level	[edit forwarding-options accounting <i>name</i> output], [edit forwarding-options sampling family (inet inet6 mpls) output], [edit forwarding-options sampling instance <i>instance-name</i> family (inet inet6 mpls) output]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the output interface for monitored traffic.
Options	<i>interface-name</i> —Name of the interface. 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	<ul style="list-style-type: none">• Configuring Discard Accounting• Configuring Traffic Sampling

ipv4-flow-table-size

Syntax	<code>ipv4-flow-table-size <i>units</i>;</code>
Hierarchy Level	<code>[edit chassis fpc <i>slot-number</i> inline-services flow-table-size]</code>
Description	Configure the size of the IPv4 flow table in units of 256K entries.



NOTE: Any changes in the configured size of the flow has table sizes initiates an automatic reboot of the FPC.

Options	<p>units—Number of 256K flow entries available for the IPv4 flow table.</p> <p>Range: 1 through 15</p> <p>Default: 15 (3840K)</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Inline Sampling on page 18

ipv6-flow-table-size

Syntax	<code>ipv6-flow-table-size <i>units</i>;</code>
Hierarchy Level	<code>[edit chassis fpc <i>slot-number</i> inline-services ipv6 flow-table-size]</code>
Description	Configure the size of the IPv6 flow table in units of 256K entries.



NOTE: Any changes in the configured size of the flow has table sizes initiates an automatic reboot of the FPC.

Options	<p>units—Number of 256K flow entries available for the IPv6 flow table.</p> <p>Range: 1 through 15</p> <p>Default: 1K</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Inline Sampling on page 18

monitoring

Syntax `monitoring name {
 family inet {
 output {
 cflowd hostname port-number;
 export-format cflowd-version-5;
 flow-active-timeout seconds;
 flow-export-destination {
 (cflowd-collector | collector-pic);
 }
 flow-inactive-timeout seconds;
 interface interface-name {
 number;
 engine-type number;
 input-interface-index number;
 output-interface-index number;
 source-address address;
 }
 }
 }
 }`

Hierarchy Level [edit forwarding-options]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the flow monitoring instance name and properties.

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 Flow Monitoring on page 13](#)

multiservice-options

Syntax	<pre>multiservice-options { (core-dump no-core-dump); (syslog no-syslog); flow-control-options { down-on-flow-control; dump-on-flow-control; reset-on-flow-control; } }</pre>
Hierarchy Level	[edit interfaces <i>mo-fpc/pic/port</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>For flow-monitoring interfaces only, configure multiservice-specific interface properties.</p> <p>The statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Flow Monitoring on page 13

output-interface-index

Syntax	output-interface-index <i>number</i> ;
Hierarchy Level	[edit forwarding-options monitoring <i>name</i> output interface <i>interface-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify a value for the output interface index that overrides the default supplied by SNMP.
	<div style="display: flex; align-items: center;">  <div style="margin-left: 10px;"> <p>NOTE: On J Series routers, cflowd sampling in the input direction of an interface reports the output interface index as 0.</p> </div> </div>
Options	<i>number</i> —Output interface index value.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Flow Monitoring on page 13

output (Monitoring)

Syntax output {
 cflowd *hostname* **port** *port-number*;
 export-format *format*;
 flow-active-timeout *seconds*;
 flow-export-destination {
 (cflowd-collector | collector-pic);
 }
 flow-inactive-timeout *seconds*;
 interface *interface-name* {
 engine-id *number*;
 engine-type *number*;
 input-interface-index *number*;
 output-interface-index *number*;
 source-address *address*;
 }
 }

Hierarchy Level [edit forwarding-options **monitoring** *name* family inet]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure cflowd, output interfaces, and flow properties.

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 Flow Monitoring on page 13](#)

port

Syntax	<code>port <i>port-number</i>;</code>
Hierarchy Level	[edit forwarding-options accounting <i>name</i> output cflowd <i>hostname</i>], [edit forwarding-options monitoring <i>name</i> family inet output cflowd <i>hostname</i>], [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>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the User Datagram Protocol (UDP) port number on the cflowd host system.
Options	<i>port-number</i> —Any valid UDP port number on the host system.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Enabling Flow Aggregation

sampling (Interfaces)

Syntax	<code>sampling <i>direction</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the direction of traffic to be sampled.
Options	<p><i>direction</i> can be one of the following:</p> <p>input—Configure at least one expected ingress point.</p> <p>output—Configure at least one expected egress point.</p> <p>input output—On a single interface, configure at least one expected ingress point and one expect egress point.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Junos OS Services Interfaces Library for Routing Devices • Configuring Flow Monitoring on page 13

source-address (Forwarding Options)

Syntax	source-address <i>address</i> ;
Hierarchy Level	[edit forwarding-options accounting <i>name</i> output <i>interface interface-name</i>], [edit forwarding-options <i>monitoring name family family</i> inet output <i>interface interface-name</i>], [edit forwarding-options sampling instance <i>instance-name</i> family (inet inet6 mpls) output <i>interface interface-name</i>], [edit forwarding-options sampling family (inet inet6 mpls) output <i>interface interface-name</i>], [edit forwarding-options sampling instance <i>instance-name</i> family inet output inline-jflow]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the source address for monitored packets.
Options	<i>address</i> —Interface source address.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring Discard Accounting</i>• Configuring Flow Monitoring on page 13• <i>Configuring Traffic Sampling</i>

syslog

Syntax	(syslog no-syslog);
Hierarchy Level	[edit interfaces <i>mo-fpc/pic/port multiservice-options</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	System logging is enabled by default. The system log information of the Monitoring Services PIC is passed to the kernel for logging in the <i>/var/log</i> directory. <ul style="list-style-type: none">• syslog—Enable PIC system logging.• no-syslog—Disable PIC system logging.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Flow Monitoring on page 13

unit

Syntax	<pre> unit <i>logical-unit-number</i> { family inet { address <i>address</i> { destination <i>destination-address</i>; } filter { group <i>filter-group-number</i>; input <i>filter-name</i>; output <i>filter-name</i>; } sampling <i>direction</i>; } } </pre>
Hierarchy Level	[edit interfaces <i>interface-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.
Options	<p><i>logical-unit-number</i>—Number of the logical unit.</p> <p>Range: 0 through 16,384</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Junos OS Network Interfaces Library for Routing Devices</i> for other statements that do not affect services interfaces. • <i>Junos OS Network Interfaces Library for Routing Devices</i>

PART 3

Administration

- [Flow Monitoring Operational Mode Commands on page 61](#)
- [Flow Monitoring Interface Operational Mode Commands on page 91](#)

CHAPTER 4

Flow Monitoring Operational Mode Commands

show services accounting aggregation

Syntax	<pre>show services accounting aggregation <i>aggregation-type</i> <<i>aggregation-value</i>> <detail extensive terse> <limit <i>limit-value</i>> < name <i>service-name</i>> <order (bytes packets)></pre>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display information about the aggregated active flows being processed by the accounting service.
Options	<p><i>aggregation-type</i> <<i>aggregation-value</i>>—Display information for a particular aggregation type and optional value:</p> <ul style="list-style-type: none"> as <<i>source-as-value</i> <i>destination-as-value</i> <i>input-snmp-interface-index-value</i> <i>output-snmp-interface-index-value</i>>—Aggregate by autonomous system (AS). destination-prefix <<i>destination-prefix-value</i> <i>destination-as-value</i> <i>output-snmp-interface-index-value</i>>—Aggregate by destination prefix. protocol-port <<i>protocol-value</i> <i>source-port-value</i> <i>destination-port-value</i>>—Aggregate by protocol and port. source-destination-prefix <<i>source-prefix-value</i> <i>destination-prefix-value</i> <i>destination-as-value</i> <i>source-as-value</i> <i>input-snmp-interface-index-value</i> <i>output-snmp-interface-index-value</i>>—Aggregate by source and destination prefix. source-prefix <<i>source-prefix-value</i> <i>source-as-value</i> <i>input-snmp-interface-index-value</i>>—Aggregate by source prefix. <p>detail extensive terse—(Optional) Display the specified level of output.</p> <p>limit <i>limit-value</i>—(Optional) Limit the display output to this number of flows. The default is no limit.</p> <p>name <i>service-name</i>—(Optional) Display information about the aggregated flows for a particular service name.</p> <p>order (bytes packets)—(Optional) Display the flow with the ordering of the highest number, either by byte count or by packet count.</p>
Additional Information	For information about aggregation configuration options, see the <i>Junos OS Services Interfaces Library for Routing Devices</i> .
Required Privilege Level	view
List of Sample Output	show services accounting aggregation protocol-port detail on page 64 show services accounting aggregation source-destination-prefix on page 64

[show services accounting aggregation source-destination- prefix order packet detail on page 64](#)

[show services accounting aggregation source-destination- prefix extensive limit on page 65](#)

[show services accounting aggregation source-destination-prefix name terse on page 65](#)

Output Fields [Table 3 on page 63](#) lists the output fields for the **show services accounting aggregation** command. Output fields are listed in the approximate order in which they appear.

Table 3: show services accounting aggregation Output Fields

Field Name	Field Description
Service Accounting interface	Name of the service accounting interface.
Local interface index	Index corresponding to the service accounting interface.
Service name	Name of a service that was configured at the [edit forwarding-options accounting] hierarchy level. The default display, (default sampling), indicates the service was configured at the [edit forwarding-options sampling-level] hierarchy level.
Protocol	Protocol identifier and number.
Source Port	Source port identifier and number.
Destination Port	Destination port identifier and number.
Source-AS	Source autonomous system (AS) number.
Destination-AS	Destination AS number.
Source Prefix	Source prefix.
Destination Prefix	Destination prefix.
Source address	Source address.
Source prefix length	Source prefix length.
Destination address	Destination address.
Destination prefix length	Destination prefix length.
Input SNMP interface index	SNMP index of the interface the packet came in on.
Output SNMP interface index	SNMP index of the interface the packet went out on.

Table 3: show services accounting aggregation Output Fields (*continued*)

Field Name	Field Description
Start time	Actual time when the packet in this aggregation was first seen.
End time	Actual time when the packet in this aggregation was last seen.
Flow count	Number of flows in the aggregation.
Packet count	Number of packets in the aggregation.
Byte count	Number of bytes in the aggregation.

Sample Output

show services accounting aggregation protocol-port detail

```

user@host> show service accounting aggregation protocol-port detail
Service Accounting interface: mo-2/0/0, Local interface index: 468
Service name: (default sampling)
  Protocol: 6, Source port: 20, Destination port: 20
  Start time: 442349, End time: 6425714
  Flow count: 194, Packet count: 4294964388, Byte count: 4294781184

  Protocol: 0, Source port: 0, Destination port: 0
  Start time: 442349, End time: 6425749
  Flow count: 204, Packet count: 4294964324, Byte count: 4294777088

  Protocol: 17, Source port: 123, Destination port: 123
  Start time: 442364, End time: 6425784
  Flow count: 186, Packet count: 4294964152, Byte count: 4294766080

```

show services accounting aggregation source-destination-prefix

```

user@host> show service accounting aggregation source-destination-prefix
Service Accounting interface: rsp0, Local interface index: 171
Service name: (default sampling)
Interface state: Accounting
Source          Destination    Input          Output          Flow    Packet
Byte           prefix        interface      interface      count   count
prefix         count
11.1.0.0/20     40.0.0.0/24   ge-5/0/1.0     ge-5/0/0.0     256     491761
31472704
11.1.0.0/20     40.0.1.36/32  ge-5/0/1.0     ge-5/0/0.0     1
1926            123264
11.1.0.0/20     40.0.1.59/32  ge-5/0/1.0     ge-5/0/0.0     1
1926            123264
11.1.0.0/20     40.0.3.63/32  ge-5/0/1.0     ge-5/0/0.0     1
1925            123200
11.1.0.0/20     40.0.3.32/32  ge-5/0/1.0     ge-5/0/0.0     1
1925

```

show services accounting aggregation source-destination- prefix order packet detail

```

user@host> show service accounting aggregation source-destination-prefix order packet detail
name t2 input-snmp-interface-index 538

```



```

Service Accounting interface: mo-2/0/0, Local interface index: 468
Service name: t2
Source      Destination  Input SNMP  Output SNMP  Flow  Packet  Byte
Prefix      Prefix      Index      Index      Count Count   Count
11.1.1.2/20 30.0.167.1/0 538        432         1     60     46483
11.1.1.2/20 30.0.168.1/0 538        432         1     60     5191
11.1.1.2/20 30.0.154.1/0 538        432         2     60     45504
11.1.1.2/20 30.0.76.1/0  538        432         1     60     42177
11.1.1.2/20 30.0.149.1/0 538        432         1     60     49184
11.1.1.2/20 30.0.113.1/0 538        432         2     60     48757

```

show services accounting aggregation source-destination- prefix extensive limit

```

user@host> show service accounting aggregation source-destination-prefix name t2 extensive
limit 3

```

```

Service Accounting interface: mo-2/0/0, Local interface index: 542
Service name: t2

```

```

Source address: 11.1.1.2, Source prefix length: 20
Destination address: 44.200.176.1, Destination prefix length: 0
Input SNMP interface index: 24, Output SNMP interface index: 26
Source-AS: 69, Destination-AS: 69
Start time: Fri Feb 21 14:16:57 2003, End time: Fri Feb 21 14:22:50 2003
Flow count: 0, Packet count: 6, Byte count: 5340

```

```

Source address: 11.1.1.2, Source prefix length: 20
Destination address: 45.243.160.1, Destination prefix length: 0
Input SNMP interface index: 24, Output SNMP interface index: 26
Source-AS: 69, Destination-AS: 69
Start time: Fri Feb 21 14:16:57 2003, End time: Fri Feb 21 14:22:50 2003
Flow count: 0, Packet count: 6, Byte count: 5490

```

```

Source address: 11.1.1.2, Source prefix length: 20
Destination address: 45.162.160.1, Destination prefix length: 0
Input SNMP interface index: 24, Output SNMP interface index: 26
Source-AS: 69, Destination-AS: 69
Start time: Fri Feb 21 14:16:57 2003, End time: Fri Feb 21 14:22:50 2003
Flow count: 0, Packet count: 6, Byte count: 4079

```

show services accounting aggregation source-destination-prefix name terse

```

user@host> show service accounting aggregation source-destination-prefix name T3 terse

```

```

Service Accounting interface: rsp0, Local interface index: 171

```

```

Service name: T3

```

```

Interface state: Accounting

```

Source	Destination	Input	Output	Flow	Packet
Byte					
prefix	prefix	interface	interface	count	count
count					
11.1.0.0/20	50.0.0.0/24	ge-5/0/1.0	ge-5/0/0.0	256	639822
40948608					
11.1.0.0/20	50.0.2.67/32	ge-5/0/1.0	ge-5/0/0.0	1	
2485	159040				
11.1.0.0/20	50.0.2.92/32	ge-5/0/1.0	ge-5/0/0.0	1	
2485					

show services accounting aggregation template

Syntax	show services accounting aggregation template <template-name <i>template-name</i>>
Release Information	Command introduced in Junos OS Release 8.3.
Description	Display information for flow aggregation version 9 templates.
Options	<template-name <i>template-name</i>> —(Optional) Display information for the specified template only.
Required Privilege Level	view
List of Sample Output	show services accounting aggregation template on page 66
Output Fields	Table 4 on page 66 lists the output fields for the show services accounting aggregation template command. Output fields are listed in the approximate order in which they appear.

Table 4: show services accounting aggregation template Output Fields

Field Name	Field Description
MPLS Label 1	Position of first MPLS label.
MPLS Label 2	Position of second MPLS label.
MPLS Label 3	Position of third MPLS label.
MPLS Top Level Address	Outer top label FEC IP address.
Packet Count	Number of packets sent.

Sample Output

show services accounting aggregation template

```

user@host> show services accounting aggregation template template-name mpls
MPLS label 1: 299808, MPLS label 2: 0, MPLS label 3: 0
Source address: 11.1.1.2, Destination address: 10.255.15.22, Top Label Address:
22.15.255.10
Source port: 0, Destination port: 0
Protocol: 61, TOS: 0, TCP flags: 0
Source mask: 24, Destination mask: 32
Input SNMP interface index: 503, Output SNMP interface index: 505
Start time: 40780, End time: 157330
Packet count: 3949198, Byte count: 181663062

```

show services accounting errors

Syntax	<code>show services accounting errors</code> <code><inline-jflow name (* all service-name)></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display active flow error statistics.
Options	<p>none—Display error statistics for all services accounting instances.</p> <p>inline-jflow fpc-slot slot-number—(Optional) Display error statistics for inline jflow.</p> <p>name (* all service-name)—(Optional) Display active flow error statistics. Use a wildcard character, specify all services, or provide a specific service name.</p>
Required Privilege Level	view
List of Sample Output	<p>show services accounting errors (Monitoring PIC interface) on page 68</p> <p>show services accounting errors (Service PIC interface) on page 69</p> <p>show services accounting errors inline-jflow fpc-slot slot-number (when only IPv6 is configured) on page 69</p> <p>show services accounting errors inline-jflow fpc-slot slot-number (when both IPv4 and IPv6 are configured) on page 69</p> <p>show services accounting errors inline-jflow (MX80 Router when both IPv4 and IPv6 are configured) on page 69</p>
Output Fields	<p>Table 5 on page 67 lists the output fields for the show services accounting errors command. Output fields are listed in the approximate order in which they appear.</p>

Table 5: show services accounting errors Output Fields

Field	Field Description
Service Accounting interface	Name of the service accounting interface.
Local interface index	Index counter of the local interface.
FPC slot	Slot number of the FPC for which the flow information is displayed. (Available only when the inline-jflow fpc-slot slot-number option is used.)
Service name	Name of a service that was configured at the [edit forwarding-options accounting] hierarchy level. The default display, (default sampling) , indicates the service was configured at the [edit forwarding-options sampling-level] hierarchy level.
Error Information	
Packets dropped (no memory)	Number of packets dropped because of memory shortage.

Table 5: show services accounting errors Output Fields (*continued*)

Field	Field Description
Packets dropped (not IP)	Number of non-IP packets dropped.
Packets dropped (not IPv4)	Number of packets dropped because they failed the IPv4 version check.
Packets dropped (header too small)	Number of packets dropped because the packet length or IP header length was too small.
Memory allocation failures	Number of flow record memory allocation failures. A small number reflects failures to replenish the free list. A large number indicates the monitoring station is almost out of memory space.
Memory free failures	Number of flow record memory free failures.
Memory free list failures	Number of flow records received from the free list that failed. Memory is nearly exhausted, or too many new flows greater than 128 KB are being created per second.
Memory overload	Whether the memory has been overloaded. The response can be Yes or No .
PPS overload	Whether the PIC is receiving more packets per second than the configured threshold. The response can be Yes or No .
BPS overload	Whether the PIC is receiving more bits per second than the configured threshold. The response can be Yes or No .
Flow Creation Failures	Number of times flow creation failed.
Route Record Lookup Failures	Number of times the route record lookup failed.
AS Lookup Failures	Number of times autonomous system lookup failed.
Export Packet Failures	Number of times packet export failed.

Sample Output

show services accounting errors (Monitoring PIC interface)

```

user@host> show services accounting errors
Service Accounting interface: mo-1/1/0, Local interface index: 15
Service name: (default sampling)
Error information
  Packets dropped (no memory): 0, Packets dropped (not IP): 0
  Packets dropped (not IPv4): 0, Packets dropped (header too small): 0
  Memory allocation failures: 0, Memory free failures: 0
  Memory free list failures: 0
  Memory overload: No, PPS overload: No, BPS overload: No

```

Sample Output

show services accounting errors (Service PIC interface)

```

user@host> show services accounting errors
Service Accounting interface: sp-0/1/0
Service name: (default sampling)
Error information
  Service sets dropped: 0, Active timeout failures: 0
  Export packet failures: 0, Flow creation failures: 0
  Memory overload: No

Service Accounting interface: sp-1/0/0
Service name: (default sampling)
Error information
  Service sets dropped: 0, Active timeout failures: 0
  Export packet failures: 0, Flow creation failures: 0
  Memory overload: No

```

show services accounting errors inline-jflow fpc-slot slot-number (when only IPv6 is configured)

```

user@host> show services accounting errors inline-jflow fpc-slot 5
Error information
  FPC Slot: 5
  Flow Creation Failures: 0
  Route Record Lookup Failures: 0, AS Lookup Failures: 0
  Export Packet Failures: 0
  Memory Overload: No, Memory Alloc Fail Count: 0

```

show services accounting errors inline-jflow fpc-slot slot-number (when both IPv4 and IPv6 are configured)

```

user@host> show services accounting errors inline-jflow fpc-slot 5
Error information
  FPC Slot: 5
  Flow Creation Failures: 0
  Route Record Lookup Failures: 0, AS Lookup Failures: 0
  Export Packet Failures: 0
  Memory Overload: No, Memory Alloc Fail Count: 0

IPv4:
IPv4 Flow Creation Failures: 0
IPv4 Route Record Lookup Failures: 0, IPv4 AS Lookup Failures: 0
IPv4 Export Packet Failures: 0

IPv6:
IPv6 Flow Creation Failures: 0
IPv6 Route Record Lookup Failures: 0, IPv6 AS Lookup Failures: 0
IPv6 Export Packet Failures: 0

```

show services accounting errors inline-jflow (MX80 Router when both IPv4 and IPv6 are configured)

```

user@host> show services accounting errors inline-jflow
Error information
  TFEB Slot: 0
  Flow Creation Failures: 0
  Route Record Lookup Failures: 0, AS Lookup Failures: 0
  Export Packet Failures: 0
  Memory Overload: No

IPv4:
IPv4 Flow Creation Failures: 0

```

IPv4 Route Record Lookup Failures: 0, IPv4 AS Lookup Failures: 0
IPv4 Export Packet Failures: 0

IPv6:

IPv6 Flow Creation Failures: 0
IPv6 Route Record Lookup Failures: 0, IPv6 AS Lookup Failures: 0
IPv6 Export Packet Failures: 0

show services accounting flow

Syntax	<code>show services accounting flow</code> <code><inline-jflow logical-system name (* all service-name)></code>
Release Information	Command introduced before Junos OS Release 7.4. Junos OS Release 10.0 added the capability to display output from multiple sampling instances.
Description	Display active flow statistics.
Options	<p>none—Display active flow statistics for all service instances.</p> <p>logical-system (all logical-system)—(Optional) Display active flow statistics for the specified logical system or all logical systems on the device.</p> <p>inline-jflow (fpc-slot slot-number)—(Optional) Display inline flow statistics for the specified FPC.</p> <p>name (* all service-name)—(Optional) Display services accounting active flow statistics. Use a wildcard character, specify all services, or provide a specific service name.</p>
Required Privilege Level	view
List of Sample Output	show services accounting flow (flow aggregation v5/v8 configuration) on page 72 show services accounting flow (flow aggregation v9 configuration) on page 72 show services accounting flow name on page 73 show services accounting flow name all on page 73 show services accounting flow (multiple sampling instances) on page 73 show services accounting flow inline-jflow fpc-slot slot-number (for IPv4 flow) on page 74 show services accounting flow inline-jflow fpc-slot slot-number (with IPv4 and IPv6 Configuration) on page 74 show services accounting flow inline-jflow (MX80 Router with IPv4 and IPv6 Configuration) on page 74
Output Fields	Table 6 on page 71 lists the output fields for the show services accounting flow command. Output fields are listed in the approximate order in which they appear.

Table 6: 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.
Service name	Name of a service that was configured at the [edit forwarding-options accounting] hierarchy level. The default display, (default sampling) , indicates the service was configured at the [edit forwarding-options sampling-level] hierarchy level.

Table 6: show services accounting flow Output Fields (*continued*)

Output Field	Output Field Description
Flow Information	
FPC Slot	Slot number of the FPC for which the flow information is displayed. (Available only when the inline-jflow fpc-slot slot-number option is used.)
Flow packets	Number of packets received by an operational PIC.
Flow bytes	Number of bytes received by an operational PIC.
Flow packets 10-second rate	Number of packets per second handled by the PIC and displayed as a 10-second average.
Flow bytes 10-second rate	Number of bytes per second handled by the PIC and displayed as a 10-second average.
Active flows	Number of currently active flows tracked by the PIC.
Total flows	Total number of flows received by an operational PIC.
Flows exported	Total number of flows exported by an operational PIC.
Flows packets exported	Total number of cflowd packets exported by an operational PIC.
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 (flow aggregation v5/v8 configuration)

```

user@host> show services accounting flow
Service Accounting interface: rsp0, Local interface index: 171
Service name: (default sampling)
Interface state: Accounting
Flow information
  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

```

show services accounting flow (flow aggregation v9 configuration)

```

user@host> show services accounting flow
Flow information
  Service Accounting interface: sp-7/1/0, Local interface index: 149
  Flow packets: 0, Flow bytes: 0
  Flow packets 10-second rate: 0, Flow bytes 10-second rate: 0
  Active flows: 0, Total flows: 0

```



```
Flows exported: 0, Flows packets exported: 1
Flows inactive timed out: 0, Flows active timed out: 0
```

show services accounting flow name

```
user@host> show services accounting flow count2
Service Accounting interface: mo-1/1/0, Local interface index: 15
Service name: count2
Flow information
  Flow packets: 0, Flow bytes: 0
  Flow packets 10-second rate: 0, Flow bytes 10-second rate: 0
  Active flows: 0, Total flows: 0
  Flows exported: 0, Flows packets exported: 0
  Flows inactive timed out: 0, Flows active timed out: 0
```

show services accounting flow name all

```
user@host> show services accounting flow name all
Service Accounting interface: rsp0, Local interface index: 171
Service name: T2
Interface state: Accounting
Flow information
  Flow packets: 37609891, Flow bytes: 2407033024
  Flow packets 10-second rate: 45762, Flow bytes 10-second rate: 2928953
  Active flows: 1000, Total flows: 1000
  Flows exported: 6705, Flows packets exported: 198
  Flows inactive timed out: 0, Flows active timed out: 13000

Service Accounting interface: rsp0, Local interface index: 171
Service name: T3
Interface state: Accounting
Flow information
  Flow packets: 37750807, Flow bytes: 2416051712
  Flow packets 10-second rate: 45762, Flow bytes 10-second rate: 2928940
  Active flows: 1000, Total flows: 1000
  Flows exported: 13437, Flows packets exported: 378
  Flows inactive timed out: 0, Flows active timed out: 13000

Service Accounting interface: rsp0, Local interface index: 171
Service name: T4
Interface state: Accounting
Flow information
  Flow packets: 0, Flow bytes: 0
  Flow packets 10-second rate: 0, Flow bytes 10-second rate: 0
  Active flows: 0, Total flows: 0
  Flows exported: 0, Flows packets exported: 0
  Flows inactive timed out: 0, Flows active timed out: 0

Service Accounting interface: rsp0, Local interface index: 171
Service name: count1
Interface state: Accounting
Flow information
  Flow packets: 0, Flow bytes: 0
  Flow packets 10-second rate: 0, Flow bytes 10-second rate: 0
  Active flows: 0, Total flows: 0
  Flows exported: 0, Flows packets exported: 0
  Flows inactive timed out: 0, Flows active timed out: 0
```

show services accounting flow (multiple sampling instances)

```
user@host> show services accounting flow
```

Flow information

Service Accounting interface: sp-2/0/0, Local interface index: 215
Flow packets: 9867, Flow bytes: 631488
Flow packets 10-second rate: 0, Flow bytes 10-second rate: 628
Active flows: 2, Total flows: 10
Flows exported: 4028, Flows packets exported: 6150
Flows inactive timed out: 8, Flows active timed out: 4026

Service Accounting interface: sp-2/1/0, Local interface index: 223
Flow packets: 0, Flow bytes: 0
Flow packets 10-second rate: 0, Flow bytes 10-second rate: 0
Active flows: 0, Total flows: 0
Flows exported: 0, Flows packets exported: 1
Flows inactive timed out: 0, Flows active timed out: 0

show services accounting flow inline-jflow fpc-slot slot-number (for IPv4 flow)

```
user@host> show services accounting flow inline-jflow fpc-slot 5
Flow information
FPC Slot: 5
Flow Packets: 0, Flow Bytes: 0
Active Flows: 0, Total Flows: 0
Flows Exported: 0, Flow Packets Exported: 0
Flows Inactive Timed Out: 0, Flows Active Timed Out: 0
```

show services accounting flow inline-jflow fpc-slot slot-number (with IPv4 and IPv6 Configuration)

```
user@host> show services accounting flow inline-jflow fpc-slot 5
Flow information
FPC Slot: 5
Flow Packets: 0, Flow Bytes: 0
Active Flows: 0, Total Flows: 0
Flows Exported: 0, Flow Packets Exported: 0
Flows Inactive Timed Out: 0, Flows Active Timed Out: 0

IPv4 Flows:
IPv4 Flow Packets: 0, IPv4 Flow Bytes: 0
IPv4 Active Flows: 0, IPv4 Total Flows: 0
IPv4 Flows Exported: 0, IPv4 Flow Packets exported: 0
IPv4 Flows Inactive Timed Out: 0, IPv4 Flows Active Timed Out: 0

IPv6 Flows:
IPv6 Flow Packets: 0, IPv6 Flow Bytes: 0
IPv6 Active Flows: 0, IPv6 Total Flows: 0
IPv6 Flows Exported: 0, IPv6 Flow Packets Exported: 0
IPv6 Flows Inactive Timed Out: 0, IPv6 Flows Active Timed Out: 0
```

show services accounting flow inline-jflow (MX80 Router with IPv4 and IPv6 Configuration)

```
user@host> show services accounting flow inline-jflow
Flow information
TFEB Slot: 0
Flow Packets: 0, Flow Bytes: 0
Active Flows: 0, Total Flows: 0
Flows Exported: 0, Flow Packets Exported: 0
Flows Inactive Timed Out: 0, Flows Active Timed Out: 0

IPv4 Flows:
IPv4 Flow Packets: 0, IPv4 Flow Bytes: 0
IPv4 Active Flows: 0, IPv4 Total Flows: 0
IPv4 Flows Exported: 0, IPv4 Flow Packets exported: 0
IPv4 Flows Inactive Timed Out: 0, IPv4 Flows Active Timed Out: 0
```

```
IPv6 Flows:  
IPv6 Flow Packets: 0, IPv6 Flow Bytes: 0  
IPv6 Active Flows: 0, IPv6 Total Flows: 0  
IPv6 Flows Exported: 0, IPv6 Flow Packets Exported: 0  
IPv6 Flows Inactive Timed Out: 0, IPv6 Flows Active Timed Out: 0
```

show services accounting flow-detail

Syntax `show services accounting flow-detail`
 `<detail | extensive | terse>`
 `<filters>`
 `<limit limit-value>`
 `<name (* | all | service-name)>`
 `<order (bytes | packets)>`

Release Information Command introduced before Junos OS Release 7.4.

Description Display information about the flows being processed by the accounting service.

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

filters—(Optional) Filter the display output of the currently active flow records. The following filters query actively changing data structures and result in different results for multiple invocations:

- **destination-as**—Display flow records filtered by destination autonomous system information.
- **destination-port**—Display flow records filtered by destination port information.
- **destination-prefix**—Display flow records filtered by destination prefix information.
- **input-snmp-interface-index**—Display flow records filtered by SNMP input interface index information.
- **output-snmp-interface-index**—Display flow records filtered by SNMP output interface index information.
- **proto**—Display flow records filtered by protocol type.
- **source-as**—Display flow records filtered by source autonomous system information.
- **source-port**—Display flow records filtered by source port information.
- **source-prefix**—Display flow records filtered by source prefix information.
- **tos**—Display flow records filtered by type of service classification.

limit limit-value—(Optional) Limit the display output to the specified number of flows. The default is no limit.

name (* | all | service-name)—(Optional) Display information about the flows being processed. Use a wildcard character, specify all services, or provide a specific services name.

order (bytes | packets)—(Optional) Display the flow with the ordering of the highest number, either by byte count or by packet count.

Additional Information When no PIC is active, or when no route record has been downloaded from the PIC, this command reports no flows, even though packets are being sampled. This command

displays information about two concurrent sessions only. If a third session is attempted, the command pauses with no output until one of the previous sessions is completed.

Required Privilege Level view

List of Sample Output [show services accounting flow-detail on page 78](#)
[show services accounting flow-detail limit on page 79](#)
[show services accounting flow-detail name extensive on page 79](#)
[show services accounting flow-detail limit order bytes on page 79](#)
[show services accounting flow-detail source-port on page 80](#)

Output Fields [Table 7 on page 77](#) lists the output fields for the **show services accounting flow-detail** command. Output fields are listed in the approximate order in which they appear.

Table 7: show services accounting flow-detail Output Fields

Field Name	Field Description	Output Level
Service Accounting interface	Name of the service accounting interface.	All levels
Service name	Name of a service that was configured at the [edit forwarding-options accounting] hierarchy level. The default display, (default sampling) , indicates the service was configured at the [edit forwarding-options sampling] hierarchy level.	All levels
Local interface index	Index counter of the local interface.	All levels
TOS	Type-of-service value from the IP header.	extensive
Input SNMP interface index	SNMP index of the interface on which the packet came in.	extensive
Output SNMP interface index	SNMP index of the interface on which the packet went out.	extensive
Source-AS	Source AS number.	extensive
Destination-AS	Destination AS number.	extensive
Protocol	Name of the protocol used for the packet flow from the corresponding source address.	All levels
Input interface	Interface on which the packets were received.	All levels
Output interface	Interface on which the packets were transmitted.	All levels
TCP flags	Number of TCP header flags detected in the flow.	extensive
Source address	Address where the flow originated.	All levels
Source port	Name of the source port.	All levels

Table 7: show services accounting flow-detail Output Fields (*continued*)

Field Name	Field Description	Output Level
Source prefix length	Source prefix length.	extensive
Destination address	Address where the flow is sent.	All levels
Destination prefix length	Destination prefix length.	extensive
Destination port	Name of the destination port.	All levels
Start time	Actual time when the packet in this aggregation was first seen.	detail extensive
End time	Actual time when the packet in this aggregation was last seen.	detail extensive
Packet count	Number of packets in the aggregation.	All levels
Byte count	Number of bytes in the aggregation.	All levels
Time since last active timeout	Amount of time elapsed since the last active timeout, in the format <i>hh:mm:ss</i> .	None specified
Packet count for last active timeout	Number of packets in the aggregation since the last active timeout.	None specified
Byte count for last active timeout	Number of bytes in the aggregation since the last active timeout.	None specified

Sample Output

show services accounting flow-detail

In this sample, the output is split into three sections, with ellipses (...) indicating where the sections are continued.

```

user@host> show services accounting flow-detail
Service Accounting interface: rsp0, Local interface index: 171
Service name: (default sampling)
Interface state: Accounting

```

Protocol	Input interface	Source address	Source port	Output interface...
tcp(6)	ge-5/0/1.0	11.1.1.2	0	ge-5/0/0.0
tcp(6)	ge-5/0/1.0	11.1.1.2	0	ge-5/0/0.0

Destination address	Destination port	Packet count	Byte count	Time since last active timeout...
40.0.3.149	0	2660	170240	00:00:58
40.0.3.138	0	2660	170240	00:00:58

Packet count for last active timeout	Byte count for last active timeout
2805	179520
2805	179520

show services accounting flow-detail limit

In this sample, the output is split into three sections, with ellipses (...) indicating where the sections are continued.

```
user@host> show services accounting flow-detail limit 1
Service Accounting interface: rsp0, Local interface index: 171
Service name: (default sampling)
Interface state: Accounting
Protocol   Input          Source          Source   Output
           interface    address         port     interface...
tcp(6)     ge-5/0/1.0    11.1.1.2        0        ge-5/0/0.0

Destination      Destination      Packet   Byte   Time since last
address          port            count    count active timeout...
40.0.3.149              0            2158    138112      00:00:47

Packet count for   Byte count for
last active timeout last active timeout
                2827                180928
```

show services accounting flow-detail name extensive

```
user@host> show services accounting flow-detail name cf-2 extensive
Service Accounting interface: mo-0/2/0, Local interface index: 145
Service name: cf-2
  TOS: 0, Protocol: udp(17), TCP flags: 0
  Source address: 10.10.10.1, Source prefix length: 0, Destination address:
20.20.20.20,
  Destination prefix length: 0, Source port: 1173, Destination port: 69
  Input SNMP interface index: 65, Output SNMP interface index: 0, Source-AS: 0,
  Destination-AS: 0
  Start time: 62425, End time: 635265, Packet count: 165845, Byte count: 9453165
```

show services accounting flow-detail limit order bytes

The output of the following command is displayed over 141 columns, not the standard 80 columns. In this sample, the output is split into three sections, with ellipses (...) indicating where the sections are continued.

```
user@host> show services accounting flow-detail limit 5 order bytes
Service Accounting interface: mo-2/0/0, Local interface index: 356
Service name: (default sampling)
Protocol   Input          Source          Source   Output
           interface    address         port     interface...
icmp(1)    ge-2/3/0.0    11.1.1.2        0        .local.
icmp(1)    ge-2/3/0.0    11.1.1.2        0        .local.
icmp(1)    ge-2/3/0.0    11.1.1.2        0        .local.
icmp(1)    ge-2/3/0.0    11.1.1.2        0        .local.
icmp(1)    ge-2/3/0.0    11.1.1.2        0        .local.

Destination      Destination      Packet   Byte   Time since last
address          port            count    count active timeout...
51.88.128.2              0            16      12148      Not applicable
52.78.144.2              0            16      15229      Not applicable
51.147.192.2             0            16      13296      Not applicable
51.136.16.2              0            16      13924      Not applicable
50.214.48.2              0            16      13428      Not applicable

Packet count for   Byte count for
```

last active timeout	last active timeout
Not applicable	Not applicable
Not applicable	Not applicable
Not applicable	Not applicable
Not applicable	Not applicable
Not applicable	Not applicable

show services accounting flow-detail source-port

```
user@host> show services accounting flow-detail name cf-2 detail source-port 1173
Service Accounting interface: mo-0/2/0, Local interface index: 145
Service name: cf-2
  Protocol: udp(17), Source address: 10.10.10.1, Source port: 1173, Destination
address:
20.20.20.20, Destination port: 69
  Start time: 62425, End time: 811115, Packet count: 142438, Byte count: 8118966
```


show services accounting memory

Syntax	show services accounting memory
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display memory and flow record statistics.
Options	This command has no options.
Required Privilege Level	view
List of Sample Output	show services accounting memory (Monitoring PIC interface) on page 81 show services accounting memory (Service PIC interface) on page 82
Output Fields	Table 8 on page 81 lists the output fields for the show services accounting memory command. Output fields are listed in the approximate order in which they appear.

Table 8: show services accounting memory Output Fields

Output Field	Output Field Description
Service Accounting interface	Name of the service accounting interface.
Memory Utilization	
Local interface index	Index counter of the local interface.
Allocation count	Number of flow records allocated.
Free count	Number of flow records freed.
Maximum allocated	Maximum number of flow records allocated since the monitoring station booted. This number represents the peak number of flow records allocated at a time.
Allocations per second	Flow records allocated per second during the last statistics interval on the PIC.
Frees per second	Flow records freed per second during the last statistics interval on the PIC.
Total memory used	Total amount of memory currently used (in bytes).
Total memory free	Total amount of memory currently free (in bytes).

Sample Output

show services accounting memory (Monitoring PIC interface)

```
user@host> show services accounting memory
Service Accounting interface: mo-2/0/0, Local interface index: 468
Memory utilization
```

```
Allocation count: 437340, Free count: 433699, Maximum allocated: 6782
Allocations per second: 3366, Frees per second: 6412
Total memory used (in bytes): 133460320,
Total memory free (in bytes): 133918352
```

Sample Output

show services accounting memory (Service PIC interface)

```
user@host> show services accounting memory
Service Accounting interface: sp-0/1/0
  Memory utilization
    Allocation count: 1000, Free count: 0
    Allocations per second: 0, Frees per second: 0
    Total memory used (in bytes): 218158272
    Total memory free (in bytes): 587147696

Service Accounting interface: sp-1/0/0
  Memory utilization
    Allocation count: 1000, Free count: 0
    Allocations per second: 0, Frees per second: 0
    Total memory used (in bytes): 218157592
    Total memory free (in bytes): 587148376
```

show services accounting packet-size-distribution

Syntax	show services accounting packet-size-distribution <name (* all <i>service-name</i>)>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display a packet size distribution histogram.
Options	<p>none—Display a packet size distribution histogram of all accounting services.</p> <p>name (* all <i>service-name</i>)—(Optional) Display a packet size distribution histogram. Use a wildcard character, specify all services, or provide a specific services name.</p>
Required Privilege Level	view
List of Sample Output	show services accounting packet-size-distribution name on page 83
Output Fields	Table 9 on page 83 lists the output fields for the show services accounting packet-size-distribution command. Output fields are listed in the approximate order in which they appear.

Table 9: show services accounting packet-size-distribution Output Fields

Field Name	Field Description
Service Accounting interface	Name of the service accounting interface.
Service name	Name of a service that was configured at the [edit-forwarding-options accounting] hierarchy level. The default display, (default sampling), indicates the service was configured at the [edit-forwarding-options sampling-level] hierarchy level.
Local interface index	Index counter of the local interface.
Range start	Smallest packet length (in bytes) to count.
Range end	Largest packet length (in bytes) to count.
Number of packets	Count of packets detected in the size between Range start and Range end.
Percentage packets	Percentage of the total number of packets that are in this size range.

Sample Output

show services accounting packet-size-distribution name

```
user@host> show services accounting packet-size-distribution name test3
Service Accounting interface: mo-0/2/0, Local interface index: 163
Service name: test3
```

Range start	Range end	Number of packets	Percentage packets
32	64	2924	100

show services accounting status

Syntax	<code>show services accounting status</code> <code><inline-jflow name (* all service-name)></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display available Physical Interface Cards (PICs) for accounting services.
Options	<p>none—Display available PICs for all accounting services.</p> <p>inline-jflow fpc-slot slot-number—(Optional) Display inline flow accounting status for the specified FPC.</p> <p>name (* all service-name)—(Optional) Display available PICs. Use a wildcard character, specify all services, or provide a specific services name.</p>
Required Privilege Level	view
List of Sample Output	<p>show services accounting status name (Monitoring PIC interface) on page 86</p> <p>show services accounting status name (Service PIC interface) on page 86</p> <p>show services accounting status inline-jflow fpc-slot slot-number (when both IPv4 and IPv6 are configured) on page 87</p> <p>show services accounting status inline-jflow (MX80 Router when both IPv4 and IPv6 are configured) on page 87</p>
Output Fields	Table 10 on page 85 lists the output fields for the show services accounting status command. Output fields are listed in the approximate order in which they appear.

Table 10: show services accounting status Output Fields

Field	Field Description
Service Accounting interface	Name of the service accounting interface.
Service name	Name of a service that was configured at the <code>[edit-forwarding-options accounting]</code> hierarchy level. The default display, <code>(default sampling)</code> , indicates the service was configured at the <code>[edit-forwarding-options sampling-level]</code> hierarchy level.
FPC Slot	Slot number of the FPC for which the flow information is displayed. (Available only when the <code>inline-jflow fpc-slot slot-number</code> option is used.)
Local interface index	Index counter of the local interface.

Table 10: show services accounting status Output Fields (*continued*)

Field	Field Description
Interface state	Accounting state of the passive monitoring interface. <ul style="list-style-type: none"> • Accounting—PIC is actively accounting. • Disabled—PIC has been disabled from the CLI. • Not accounting—PIC is up but not accounting. This can happen while the PIC is coming online, or when the PIC is up but has no logical unit configured under the physical interface. • Unknown
Group index	Integer that represents the monitoring group of which the PIC is a member. Group index is a mapping from the group name to an index. It is not related to the number of monitoring groups.
Export interval (in seconds)	Configured export interval for cflowd records, in seconds.
Export format	Configured export format .
Protocol	Protocol the PIC is configured to monitor .
Engine type	Configured engine type that is inserted in output cflowd packets.
Engine ID	Configured engine ID that is inserted in output cflowd packets.
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.

Sample Output

show services accounting status name (Monitoring PIC interface)

```

user@host> show services accounting status name count1
Service Accounting interface: mo-2/0/0, Local interface index: 468
Service name: count1
Interface state: Accounting
Group index: 0
Export interval (in seconds): 60, Export format: cflowd v8
Protocol: IPv4, Engine type: 55, Engine ID: 5

```

Sample Output

show services accounting status name (Service PIC interface)

```

user@host> show services accounting status name
Service Accounting interface: sp-0/1/0
Interface state: Accounting
Export format: 9, Route record count: 0

```

```
IFL to SNMP index count: 7, AS count: 0
Configuration set: Yes, Route record set: No, IFL SNMP map set: Yes

Service Accounting interface: sp-1/0/0
Interface state: Accounting
Export format: 9, Route record count: 33
IFL to SNMP index count: 7, AS count: 1
Configuration set: Yes, Route record set: Yes, IFL SNMP map set: Yes
```

show services accounting status inline-jflow fpc-slot slot-number (when both IPv4 and IPv6 are configured)

```
user@host> show services accounting status inline-jflow fpc-slot 5
FPC Slot: 5
  IPv4 export format: Version-IPFIX, IPv6 export format: Version-IPFIX
  VPLS export format: Not set
  IPv4 Route Record Count: 5, IPv6 Route Record Count: 7
  Route Record Count: 12, AS Record Count: 1
  Route-Records Set: Yes, Config Set: Yes
```

show services accounting status inline-jflow (MX80 Router when both IPv4 and IPv6 are configured)

```
user@host> show services accounting status inline-jflow

Status information
  TFEB Slot: 0
  Export format: IP-FIX
  IPv4 Route Record Count: 6, IPv6 Route Record Count: 8
  Route Record Count: 14, AS Record Count: 1
  Route-Records Set: Yes, Config Set: Yes
```

show services accounting usage

Syntax	show services accounting usage <name <i>service-name</i> >
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display the CPU usage of PIC used for active flow monitoring.
Options	<p>none—Display CPU usage for all service names.</p> <p>name <i>service-name</i>—(Optional) Display CPU usage for the specified service name.</p>
Additional Information	When no route record has been downloaded from the PIC, this command reports no flows, even though packets are being sampled.
Required Privilege Level	view
List of Sample Output	show services accounting usage (Monitoring PIC interface) on page 89 show services accounting usage (Service PIC interface) on page 89
Output Fields	Table 11 on page 88 lists the output fields for the show services accounting usage command. Output fields are listed in the approximate order in which they appear.

Table 11: show services accounting usage Output Fields

Output Field	Output Field Description
Service Accounting interface	Name of the service accounting interface.
Service name	Name of a service that was configured at the [edit-forwarding-options accounting] hierarchy level. The default display, (default sampling), indicates the service was configured at the [edit-forwarding-options sampling-level] hierarchy level.
Local interface index	Index counter of the local interface.
Uptime	Time that the PIC has been operational (in milliseconds).
Interrupt time	Total time that the PIC has spent processing packets since the last PIC reset (in microseconds).
Load (5 second)	CPU load on the PIC, averaged more than 5 seconds. The number is a percentage obtained by dividing the time spent on active tasks by the total elapsed time.
Load (1 minute)	CPU load on the PIC, averaged more than 1 minute. The number is a percentage obtained by dividing the time spent on active tasks by the total elapsed time.

Sample Output

show services accounting usage (Monitoring PIC interface)

```
user@host> show services accounting usage
Service Accounting interface: mo-1/1/0, Local interface index: 15
Service name: (default sampling)
CPU utilization
  Uptime: 600413856 milliseconds, Interrupt time: 2403 microseconds
  Load (5 second): 43%, Load (1 minute): 24%
```

Sample Output

show services accounting usage (Service PIC interface)

```
user@host> show services accounting usage
Service Accounting interface: sp-0/1/0
Service name: (default sampling)
CPU utilization
  Uptime: 7853940 milliseconds, Interrupt time: 0 microseconds
  Load (5 second): 2%, Load (1 minute): 0%

Service Accounting interface: sp-0/1/0
Service name: (default sampling)
CPU utilization
  Uptime: 331160 milliseconds, Interrupt time: 0 microseconds
  Load (5 second): 2%, Load (1 minute): 0%
```


CHAPTER 5

Flow Monitoring Interface Operational Mode Commands

show interfaces (Flow Monitoring)

Syntax	<pre>show interfaces mo-fpc/pic/port:channel <brief detail extensive terse> <descriptions> <media> <snmp-index snmp-index> <statistics></pre>
Release Information	Command introduced before Junos OS Release 7.4.
Description	(M Series and T Series routers only) Display status information about the specified flow monitoring interface.
Options	<p>mo-fpc/pic/port:channel—Display standard status information about the specified flow monitoring interface.</p> <p>brief detail extensive terse—(Optional) Display the specified level of output.</p> <p>descriptions—(Optional) Display interface description strings.</p> <p>media—(Optional) Display media-specific information about network interfaces.</p> <p>snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.</p> <p>statistics—(Optional) Display static interface statistics.</p>
Required Privilege Level	view
List of Sample Output	show interfaces extensive (Flow Monitoring) on page 95
Output Fields	Table 12 on page 92 lists the output fields for the show interfaces (Flow Monitoring) command. Output fields are listed in the approximate order in which they appear.

Table 12: Flow Monitoring show interfaces Output Fields

Field Name	Field Description	Level of Output
Physical Interface		
Physical interface	Name of the physical interface.	All levels
Link	Status of the link: up or down .	All levels
Enabled	State of the interface. Possible values are described in the “Enabled Field” section under <i>Common Output Fields Description</i> .	All levels
Interface index	Physical interface index number, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	SNMP index number for the physical interface.	detail extensive none

Table 12: Flow Monitoring show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Description	Description and name of the interface.	All levels
Type	Type of interface.	All levels
Link-level type	Encapsulation type used on the physical interface.	All levels
MTU	Maximum Transmit Unit (MTU). Size of the largest packet to be transmitted.	All levels
Clocking	Reference clock source of the interface.	All levels
Speed	Network speed on the interface.	All levels
Device flags	Information about the physical device. Possible values are described in the "Device Flags" section under <i>Common Output Fields Description</i> .	All levels
Interface flags	Information about the interface. Possible values are described in the "Interface Flags" section under <i>Common Output Fields Description</i> .	All levels
Link type	Data transmission type.	All levels
Link flags	Information about the link. Possible values are described in the "Link Flags" section under <i>Common Output Fields Description</i> .	All levels
Physical info	Information about the physical interface.	All levels
Hold-times	Current interface hold-time up and hold-time down. Value is in milliseconds.	detail extensive
Current address	Configured MAC address.	detail extensive none
Hardware address	Media access control (MAC) address of the interface.	detail extensive none
Alternate link address	Backup link address.	detail extensive none
Last flapped	Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second timezone (hour:minute:second ago) . For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago)	detail extensive
Statistics last cleared	Time when the statistics for the interface were last set to zero.	detail extensive

Table 12: Flow Monitoring show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Traffic statistics	<p>Number and rate of bytes and packets received and transmitted on the physical interface.</p> <ul style="list-style-type: none"> • Input bytes, Output bytes—Number of bytes received and transmitted on the interface. • Input packets, Output packets—Number of packets received and transmitted on the interface. 	detail extensive
Input errors	<ul style="list-style-type: none"> • Errors—Input errors on the interface. • Drops—Number of packets dropped by the output queue of the I/O Manager ASIC. • Framing errors—Number of packets received with an invalid frame checksum (FCS). • Runts—Frames received smaller than the runt threshold. • Giants—Frames received larger than the giant threshold. • Policed Discards—Frames that the incoming packet match code discarded because the frames did not recognize them or were not of interest. Usually, this field reports protocols that Junos does not support. • Resource errors—Sum of transmit drops. 	extensive
Output errors	<ul style="list-style-type: none"> • Carrier transitions—Number of times the interface has gone from down to up. 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, possibly once every 10 seconds, the cable, the remote system, or the interface is malfunctioning. • Errors—Sum of outgoing frame aborts and FCS errors. • Drops—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 dropped by the ASIC Red mechanism. • Resource errors—Sum of transmit drops. 	extensive
Logical Interface		
Logical interface	Name of the logical interface.	All levels
Index	Logical interface index number, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	Logical interface SNMP interface index number.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Flags	Information about the logical interface; values are described in the “Logical Interface Flags” section under <i>Common Output Fields Description</i> .	All levels
Encapsulation	Encapsulation on the logical interface.	All levels

Table 12: Flow Monitoring show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Traffic statistics	<p>Total number of bytes and packets received and transmitted on the logical interface. These statistics are the sum of the local and transit statistics. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</p> <ul style="list-style-type: none"> • Input bytes, Output bytes—Number of bytes received and transmitted on the interface. • Input packets, Output packets—Number of packets received and transmitted on the interface. 	detail extensive
Local statistics	Statistics for traffic received from and transmitted to the Routing Engine. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.	detail extensive
Transit statistics	Statistics for traffic transiting the router. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.	detail extensive
Protocol	Protocol family configured on the logical interface (such as iso or inet6).	detail extensive none
MTU	MTU size on the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Route table	Route table in which this address exists; for example, Route table:0 refers to inet.0 .	detail extensive
Flags	Information about the protocol family flags. Possible values are described in the “Family Flags” section under <i>Common Output Fields Description</i> .	detail extensive none

Sample Output

show interfaces extensive (Flow Monitoring)

```

user@host> show interfaces mo-4/0/0 extensive
Physical interface: mo-4/0/0, Enabled, Physical link is Up
  Interface index: 144, SNMP ifIndex: 42, Generation: 28
  Description: monitor pic 2
  Type: Adaptive-Services, Link-level type: Adaptive-Services, MTU: Unlimited,
  Clocking: Unspecified, Speed: 800mbps
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps 16384
  Link type      : Full-Duplex
  Link flags     : None
  Physical info  : Unspecified
  Hold-times    : Up 0 ms, Down 0 ms
  Current address: Unspecified, Hardware address: Unspecified
  Alternate link address: Unspecified
  Last flapped  : 2005-05-24 16:43:12 PDT (00:17:46 ago)
  Statistics last cleared: Never

```

Traffic statistics:

Input bytes :	756824218	8328536 bps
Output bytes :	872916185	8400160 bps
Input packets:	508452	697 pps
Output packets:	15577196	18750 pps

Input errors:

Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
Policed discards: 0, Resource errors: 0

Output errors:

Carrier transitions: 2, Errors: 0, Drops: 0, MTU errors: 0,
Resource errors: 0

Logical interface mo-4/0/0.0 (Index 83) (SNMP ifIndex 43) (Generation 26)

Flags: Point-To-Point SNMP-Traps Encapsulation: Adaptive-Services

Traffic statistics:

Input bytes :	756781796
Output bytes :	872255328
Input packets:	507233
Output packets:	15575988

Local statistics:

Input bytes :	0
Output bytes :	0
Input packets:	0
Output packets:	0

Transit statistics:

Input bytes :	756781796	8328536 bps
Output bytes :	872255328	8400160 bps
Input packets:	507233	697 pps
Output packets:	15575988	18750 pps

Protocol inet, MTU: Unlimited, Generation: 38, Route table: 0

Flags: None

Logical interface mo-4/0/0.16383 (Index 84) (SNMP ifIndex 58) (Generation 27)

...

PART 4

Index

- [Index on page 99](#)

Index

Symbols

#, comments in configuration statements.....	xiv
(), in syntax descriptions.....	xiv
< >, in syntax descriptions.....	xiv
[], in configuration statements.....	xiv
{ }, in configuration statements.....	xiv
(pipe), in syntax descriptions.....	xiv

A

active flow monitoring	
aggregated flows, displaying.....	62
available PICs, displaying.....	85
CPU usage, displaying.....	88
error statistics, displaying.....	67
flow statistics, displaying.....	71
flows, detailed information, displaying.....	76
memory statistics, displaying.....	81
packet size distribution, displaying.....	83
address statement	
flow monitoring.....	38
aggregated flows, displaying.....	62
AS PIC	
redundancy.....	27

B

braces, in configuration statements.....	xiv
brackets	
angle, in syntax descriptions.....	xiv
square, in configuration statements.....	xiv

C

comments, in configuration statements.....	xiv
conventions	
text and syntax.....	xiii
core-dump statement.....	40
usage guidelines.....	13
curly braces, in configuration statements.....	xiv
customer support.....	xv
contacting JTAC.....	xv

D

destination statement.....	41
documentation	
comments on.....	xiv

E

engine-id statement	
flow monitoring.....	42
engine-type statement.....	43
export-format statement.....	44
usage guidelines.....	16

F

filter statement	
flow monitoring.....	46
flow aggregation	
multiple flow servers.....	23
templates.....	66
Flow monitoring	
overview.....	3
flow monitoring	
active	
aggregated flows, displaying.....	62
CPU usage, displaying.....	88
detailed information, displaying.....	76
error statistics, displaying.....	67
flow statistics, displaying.....	71
memory statistics, displaying.....	81
packet size distribution, displaying.....	83
PICs, displaying available.....	85
redundancy.....	27
flow monitoring interfaces	
status information, displaying.....	92
flow server	
replicating flows to multiple servers.....	23
flow-active-timeout statement.....	47
usage guidelines.....	16
flow-export-destination statement.....	48
usage guidelines.....	16
flow-inactive-timeout statement.....	49
usage guidelines.....	16
font conventions.....	xiii
forwarding-options statement	
usage guidelines.....	34

I

inline-jflow statement	
usage guidelines.....	18, 22
input-interface-index statement.....	50

L

local-dump statement	
usage guidelines.....	26

M

manuals	
comments on.....	xiv
monitoring statement.....	52
usage guidelines.....	14
multiservice-options statement.....	53

N

no-core-dump statement.....	40
usage guidelines.....	13
no-local-dump statement	
usage guidelines.....	26
no-syslog statement	
flow monitoring.....	56

O

output statement	
flow monitoring.....	54
output-interface-index statement.....	53

P

packet size distribution, displaying.....	83
parentheses, in syntax descriptions.....	xiv
passive flow monitoring.....	3
PICs	
active flow monitoring	
available PICs, displaying.....	85
CPU usage, displaying.....	88
port statement	
flow monitoring.....	55

R

redundancy	
flow monitoring.....	27

S

sampling	
monitoring interface.....	13
sampling statement.....	55
show interfaces (Flow Monitoring) command.....	92
show services accounting aggregation	
command.....	62
show services accounting aggregation template	
command.....	66
show services accounting errors command.....	67

show services accounting flow command.....	71
show services accounting flow-detail	
command.....	76
show services accounting memory command.....	81
show services accounting packet-size-distribution	
command.....	83
show services accounting status command.....	85
show services accounting usage command.....	88
source-address statement	
flow monitoring.....	56
usage guidelines.....	14
statistics	
active flow error.....	67
active flow instances.....	71
active flow memory utilization.....	81
aggregated active flow.....	62
support, technical See technical support	
syntax conventions.....	xiii
syslog statement	
flow monitoring.....	56

T

technical support	
contacting JTAC.....	xv
templates	
flow aggregation.....	66

U

unit statement	
flow monitoring.....	57

V

version-ipfix statement	
usage guidelines.....	18, 22