

# Flow-Tap



---

Published: 2012-02-28

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://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-Tap*

Copyright © 2012, Juniper Networks, Inc.  
All rights reserved.

The information in this document is current as of the date on the title page.

#### YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

#### END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

	About the Documentation . . . . .	ix
	Documentation and Release Notes . . . . .	ix
	Supported Platforms . . . . .	ix
	Using the Examples in This Manual . . . . .	ix
	Merging a Full Example . . . . .	x
	Merging a Snippet . . . . .	x
	Documentation Conventions . . . . .	xi
	Documentation Feedback . . . . .	xiii
	Requesting Technical Support . . . . .	xiii
	Self-Help Online Tools and Resources . . . . .	xiii
	Opening a Case with JTAC . . . . .	xiv
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Flow-Tap . . . . .</b>	<b>3</b>
	Flow-Tap Architecture . . . . .	3
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 2</b>	<b>Configuration Tasks . . . . .</b>	<b>7</b>
	Configuring the Flow-Tap Service . . . . .	7
	Configuring the Flow-Tap Interface . . . . .	7
	Strengthening Flow-Tap Security . . . . .	8
	Restrictions on Flow-Tap Services . . . . .	8
	Configuring FlowTapLite . . . . .	9
<b>Chapter 3</b>	<b>Example . . . . .</b>	<b>11</b>
	Examples: Configuring Flow-Tap Services . . . . .	11
<b>Chapter 4</b>	<b>Configuration Statements . . . . .</b>	<b>13</b>
	flow-tap . . . . .	13
	interface . . . . .	14
<b>Part 3</b>	<b>Index</b>	
	Index . . . . .	17



# List of Figures

Part 1	Overview	
Chapter 1	Flow-Tap .....	3
	Figure 1: Flow-Tap Topology .....	4



# List of Tables

<b>About the Documentation</b> .....	<b>ix</b>
Table 1: Notice Icons .....	xi
Table 2: Text and Syntax Conventions .....	xi





# About the Documentation

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

## Documentation and Release Notes

---

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

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

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

## Supported Platforms

---

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

- M Series
- T Series
- MX 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 [Junos OS CLI User Guide](#).

## Documentation Conventions

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

Table 1: Notice Icons





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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> <b>show chassis alarms</b> No alarms currently active

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

Convention	Description	Examples
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces important new terms.</li> <li>Identifies book names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS System Basics Configuration Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name:  [edit] root@# <b>set system domain-name</b> <i>domain-name</i>
<b>Text like this</b>	Represents names of configuration statements, commands, files, and directories; interface names; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the [edit protocols ospf area area-id] hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul>
< > (angle brackets)	Enclose optional keywords or variables.	<b>stub</b> <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.	<b>broadcast   multicast</b>  ( <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.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	<b>community name members [</b> <i>community-ids</i> <b>]</b>
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.	
<b>J-Web GUI Conventions</b>		
<b>Bold text like this</b>	Represents J-Web graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> <li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li> <li>To cancel the configuration, click <b>Cancel</b>.</li> </ul>
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

---

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to [techpubs-comments@juniper.net](mailto: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-Tap on page 3](#)





## CHAPTER 1

# Flow-Tap

- [Flow-Tap Architecture on page 3](#)

## Flow-Tap Architecture

---

The flow-tap architecture consists of one or more *mediation devices* that send requests to a Juniper Networks router to monitor incoming data and forward any packets that match specific filter criteria to a set of one or more *content destinations*:

- **Mediation device**—A client that monitors electronic data or voice transfer over the network. The mediation device sends filter requests to the Juniper Networks router using the DTCP. The clients are not identified for security reasons, but have permissions defined by a set of special login classes. Each system can support up to 16 different mediation devices for each user, up to a maximum of 64 mediation devices for the whole system.
- **Monitoring platform**—An M Series or T Series router containing one or more Adaptive Services (AS) or Multiservices PICs, which are configured to support the flow-tap application. The monitoring platform processes the requests from the mediation devices, applies the dynamic filters, monitors incoming data flows, and sends the matched packets to the appropriate content destinations.
- **Content destination**—Recipient of the matched packets from the monitoring platform. Typically the matched packets are sent using an IP Security (IPsec) tunnel from the monitoring platform to another router connected to the content destination. The content destination and the mediation device can be physically located on the same host. For more information about IPsec tunnels, see IPsec Properties.
- **Dynamic filters**—Firewall filters automatically generated by the Packet Forwarding Engine and applied to all routing instances. Each term in the filter includes a **flow-tap** action that is similar to the existing **sample** or **port-mirroring** actions. As long as one of the filter terms matches an incoming packet, the router copies the packet and forwards it to the Adaptive Services or Multiservices PIC that is configured for flow-tap service. The Adaptive Services or Multiservices PIC runs the packet through the client filters and sends a copy to each matching content destination.

Following is a sample filter configuration; note that it is dynamically generated by the router (no user configuration required):

```
filter combined_LEA_filter {
```

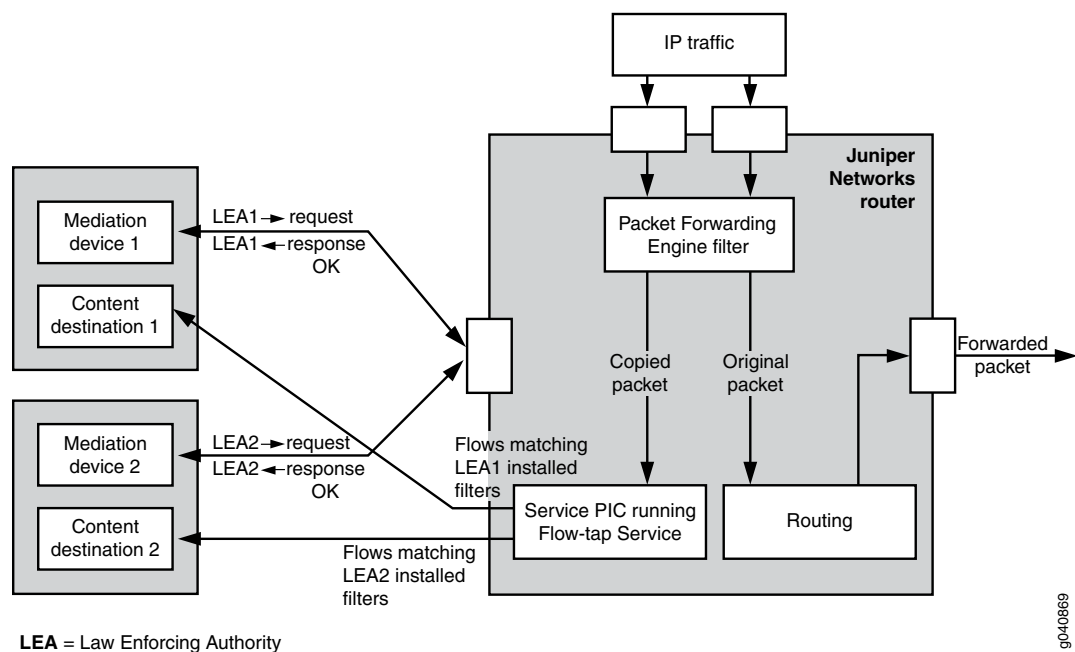
```

term LEA1_filter {
  from {
    source-address 1.2.3.4;
    destination-address 3.4.5.6;
  }
  then {
    flow-tap;
  }
}
term LEA2_filter {
  from {
    source-address 10.1.1.1;
    source-port 23;
  }
  then {
    flow-tap;
  }
}
}

```

Figure 1 on page 4 shows a sample topology that uses two mediation devices and two content destinations.

Figure 1: Flow-Tap Topology



## PART 2

# Configuration

- [Configuration Tasks on page 7](#)
- [Example on page 11](#)
- [Configuration Statements on page 13](#)



## CHAPTER 2

# Configuration Tasks

- [Configuring the Flow-Tap Service on page 7](#)
- [Configuring FlowTapLite on page 9](#)

## Configuring the Flow-Tap Service

---

This section describes the following tasks for configuring flow-tap service:

- [Configuring the Flow-Tap Interface on page 7](#)
- [Strengthening Flow-Tap Security on page 8](#)
- [Restrictions on Flow-Tap Services on page 8](#)

## Configuring the Flow-Tap Interface

To configure an adaptive services interface for flow-tap service, include the **interface** statement at the **[edit services flow-tap]** hierarchy level:

```
interface sp-fpc/pic/port.unit-number;
```

You can assign any Adaptive Services or Multiservices PIC in the active monitoring router for flow-tap service, and use any logical unit on the PIC.



**NOTE:** You cannot configure dynamic flow capture and flow-tap features on the same router simultaneously.

You must also configure the logical interface at the **[edit interfaces]** hierarchy level:

```
interface sp-fpc/pic/port {  
  unit logical-unit-number {  
    family inet;  
    family inet6;  
  }  
}
```



**NOTE:** If you do not include the **family inet6** statement in the configuration, IPv6 flows will not be intercepted.

## Strengthening Flow-Tap Security

You can add an extra level of security to Dynamic Tasking Control Protocol (DTCP) transactions between the mediation device and the router by enabling DTCP sessions on top of the SSH layer. To configure SSH settings, include the **flow-tap-dtcp** statement at the **[edit system services]** hierarchy level:

```
flow-tap-dtcp {  
  ssh {  
    connection-limit value;  
    rate-limit value;  
  }  
}
```

To configure client permissions for viewing and modifying flow-tap configurations and for receiving tapped traffic, include the **permissions** statement at the **[edit system login class *class-name*]** hierarchy level:

```
permissions [permissions];
```

The permissions needed to use flow-tap features are as follows:

- **flow-tap**—Can view flow-tap configuration
- **flow-tap-control**—Can modify flow-tap configuration
- **flow-tap-operation**—Can tap flows

You can also specify user permissions on a RADIUS server, for example:

```
Bob Auth-Type := Local, User-Password = = "abc123"  
Juniper-User-Permissions = "flow-tap-operation"
```

For details on **[edit system]** and RADIUS configuration, see the [Junos OS System Basics Configuration Guide](#).

## Restrictions on Flow-Tap Services

The following restrictions apply to flow-tap services:

- You cannot configure dynamic flow capture and flow-tap features on the same router simultaneously.
- Flow-tap service does not support interception of MPLS and virtual private LAN service (VPLS).
- Flow-tap service cannot intercept Address Resolution Protocol (ARP) and other Layer 2 exceptions.
- IPv4 and IPv6 intercept filters can coexist on a system, subject to a combined maximum of 100 filters.
- When the dynamic flow capture process or the Adaptive Services or Multiservices PIC configured for flow-tap processing restarts, all filters are deleted and the mediation devices are disconnected.

- Only the first fragment of an IPv4 fragmented packet stream is sent to the content destination.
- Port mirroring might not work in conjunction with flow-tap processing.
- Running the flow-tap application over an IPsec tunnel on the same router can cause packet loops and is not supported.
- M10i routers do not support the standard flow-tap application, but do support FlowTapLite (see [“Configuring FlowTapLite” on page 9](#)). Flow-tap and FlowTapLite cannot be configured simultaneously on the same chassis.
- PIC-based flow-tap is not supported on M7i and M10i routers equipped with an Enhanced Compact Forwarding Engine Board (CFEB-E).

## Configuring FlowTapLite

A lighter version of the flow-tap application is available on MX Series routers and also on M320 routers with Enhanced III Flexible PIC Concentrators (FPCs). All of the functionality resides in the Packet Forwarding Engine rather than a service PIC or Dense Port Concentrator (DPC).



**NOTE:** On M320 routers only, if the replacement of FPCs results in a mode change, you must restart the dynamic flow capture process manually by disabling and then re-enabling the CLI configuration.

FlowTapLite uses the same DTCP-SSH architecture to install the Dynamic Tasking Control Protocol (DTCP) filters and authenticate the users as the original flow-tap application and supports up to 3000 filters per chassis.



**NOTE:** The original flow-tap application and FlowTapLite cannot be used at the same time.

To configure FlowTapLite, include the **flow-tap** statement at the **[edit services]** hierarchy level:

```
flow-tap {
  tunnel-interface interface-name;
}
```

For the Packet Forwarding Engine to encapsulate the intercepted packet, it must send the packet to a tunnel logical (**vt-**) interface. You need to allocate a tunnel interface and assign it to the dynamic flow capture process for FlowTapLite to use. To create the tunnel interface, include the following configuration:

```
chassis {
  fpc number {
    pic number {
      tunnel-services {
        bandwidth (1g | 10g);
      }
    }
  }
}
```

```
}  
}  
}  
}
```



**NOTE:** Currently FlowTapLite supports only one tunnel interface per instance.

For more information about this configuration, see the [Junos OS System Basics Configuration Guide](#).

To configure the logical interfaces and assign them to the dynamic flow capture process, include the following configuration:

```
interfaces {  
  vt-fpc/pic/port {  
    unit 0 {  
      family inet;  
      family inet6;  
    }  
  }  
}
```



**NOTE:** If a service PIC or DPC is available, you can use its tunnel interface for the same purpose.



**NOTE:** If you do not include the family inet6 statement in the configuration, IPv6 flows will not be intercepted.



## CHAPTER 3

# Example

- [Examples: Configuring Flow-Tap Services on page 11](#)

### Examples: Configuring Flow-Tap Services

---

The following example shows all parts of a complete flow-tap configuration. The example configuration intercepts IPv4 and IPv6 flows.

```
services {
  flow-tap {
    interface sp-1/2/0.100;
  }
}
interfaces {
  sp-1/2/0 {
    unit 100 {
      family inet;
      family inet6;
    }
  }
}
system {
  services {
    flow-tap-dtcp {
      ssh {
        connection-limit 5;
        rate-limit 5;
      }
    }
  }
  login {
    class ft-class {
      permissions flow-tap-operation;
    }
    user ft-user1 {
      class ft-class;
      authentication {
        encrypted-password "xxxx";
      }
    }
  }
}
```

The following example shows a FlowTapLite configuration that intercepts IPv4 and IPv6 flows:

```
system {
  login {
    class flowtap {
      permissions flow-tap-operation;
    }
    user ftap {
      uid 2000;
      class flowtap;
      authentication {
        encrypted-password "$1$nZfwNn4L$TWi/oxFwFZyOyyxN/87Jv0"; ##
        SECRET-DATA
      }
    }
  }
}
services {
  flow-tap-dtcp {
    ssh;
  }
}
chassis {
  fpc 0 {
    pic 0 {
      tunnel-services {
        bandwidth 10g;
      }
    }
  }
}
interfaces {
  vt-0/0/0 {
    unit 0 {
      family inet;
      family inet6;
    }
  }
}
services {
  flow-tap {
    tunnel-interface vt-0/0/0.0;
  }
}
```

## CHAPTER 4

# Configuration Statements

### flow-tap

---

<b>Syntax</b>	<pre>flow-tap {     (<b>interface</b> <i>interface-name</i>   tunnel-interface <i>interface-name</i>); }</pre>
<b>Hierarchy Level</b>	[edit services]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	Enable the flow-tap or FlowTapLite application on an interface. FlowTapLite is a lighter version of the flow-tap application that is available on MX Series platforms, M120 routers, and M320 routers with Enhanced III FPCs only.
<b>Options</b>	<p><b>interface <i>interface-name</i></b>—Specify the interface name for the flow-tap application.</p> <p><b>tunnel-interface <i>interface-name</i></b>—Specify the tunnel interface name for the FlowTapLite application.</p> <p>The remaining statements are explained separately.</p>
<b>Usage Guidelines</b>	See Flow-Tap.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

## interface

---

<b>Syntax</b>	<code>interface sp-fpc/pic/port.logical-unit-number;</code>
<b>Hierarchy Level</b>	[edit services flow-tap]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	Specify the AS PIC interface used with the flow-tap application. Any AS PIC available in the router can be assigned, and any logical interface on the AS PIC can be used.
<b>Options</b>	<i>interface-name</i> —Name of the DFC interface.
<b>Usage Guidelines</b>	See <a href="#">“Configuring the Flow-Tap Interface” on page 7</a> .
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## PART 3

# Index

- [Index on page 17](#)



# Index

## Symbols

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

## B

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

## C

comments, in configuration statements.....	xii
configuration	
flow-tap application.....	11
content destinations	
flow-tap.....	3
conventions	
text and syntax.....	xi
curly braces, in configuration statements.....	xii
customer support.....	xiii
contacting JTAC.....	xiii

## D

documentation	
comments on.....	xiii

## F

flow-tap	
architecture.....	3
interface.....	7
permissions statement.....	8
RADIUS configuration.....	8
restrictions.....	8
security.....	8
flow-tap application	
example configuration.....	11
flow-tap statement.....	13

flow-tap-dtcp statement.....	8
font conventions.....	xi

## I

interface statement	
flow-tap.....	14
usage guidelines.....	7

## L

lawful intercept architecture.....	3
------------------------------------	---

## M

manuals	
comments on.....	xiii
mediation devices	
flow-tap.....	3

## P

parentheses, in syntax descriptions.....	xii
--	-----

## S

support, technical See technical support	
syntax conventions.....	xi

## T

technical support	
contacting JTAC.....	xiii

