Dynamic Flow Capture

Published: 2013-02-15

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

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

List of Figures

List of Tables

About the Documentation

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.xsl;
       }
     }
   }
   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.xsl; }
   ```

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 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
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`

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

Convention	Description	Examples
Italic text like this	• Introduces or emphasizes important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	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** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• 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** ***metric*****>;**
| (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** **(*string1* | *string2* | *string3*)**
# (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 [** ***community-ids*** **]**

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web 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

CHAPTER 1

Dynamic Flow Capture

Dynamic Flow Capture Architecture

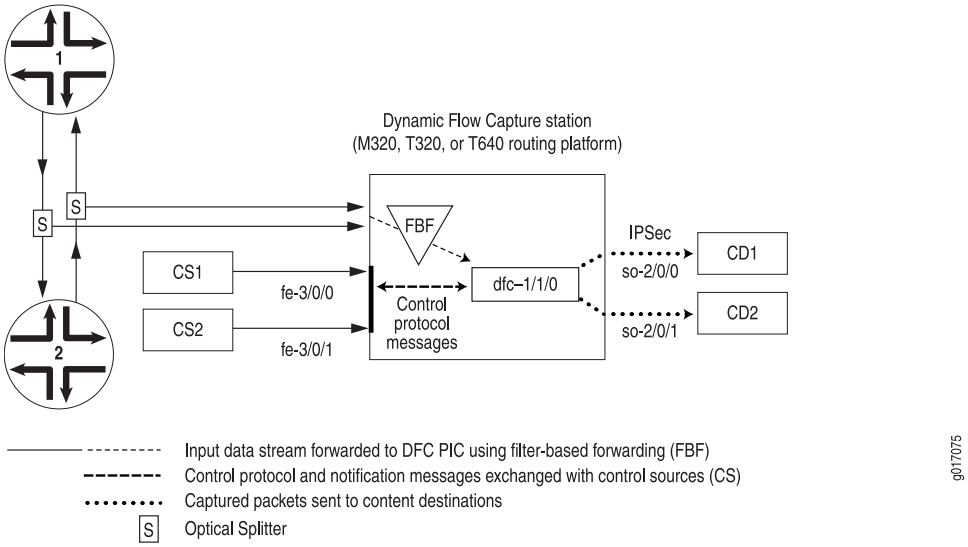
The architecture consists of one or more *control sources* that send requests to a Juniper Networks router to monitor incoming data, and then forward any packets that match specific filter criteria to a set of one or more *content destinations*. The architectural components are defined as follows:

- Control source—A client that monitors electronic data or voice transfer over the network. The control source sends filter requests to the Juniper Networks router using the Dynamic Task Control Protocol (DTCP), specified in draft-cavuto-dtcp-03.txt at **http://www.ietf.org/internet-drafts**. The control source is identified by a unique identifier and an optional list of IP addresses.
- Monitoring platform—A T Series or M320 router containing one or more Dynamic Flow Capture (DFC) PICs, which support dynamic flow capture processing. The monitoring platform processes the requests from the control sources, creates the 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 control source can be physically located on the same host. For more information on IPsec tunnels, see IPsec Properties.

NOTE: The DFC PIC (either a Monitoring Services III PIC or Multiservices 400 PIC) forwards the entire packet content to the content destination, rather than to a content record as is done with cflowd or flow aggregation version 9 templates.

Figure 1 on page 4 shows a sample topology. The number of control sources and content destinations is arbitrary.

Figure 1: Dynamic Flow Capture Topology



Liberal Sequence Windowing

Each DTCP packet (add, delete, list, and refresh packets) contains a 64-bit sequence number to identify the order of the packets. Because the network is connectionless, the DTCP packets can arrive out of order to the router running the DFC application.

The *liberal sequence window* feature implements a negative window for the sequence numbers received in the DTCP packets. It enables the DFC application to accept not only DTCP packets with sequence numbers greater than those previously received, but also DTCP packets with lesser sequence numbers, up to a certain limit. This limit is the negative window size; the positive and negative window sizes are +256 and –256 respectively, relative to the current maximum sequence number received. No configuration is required to activate this feature; the window sizes are hard-coded and nonconfigurable.

Intercepting IPv6 Flows

Starting with Junos OS Release 11.4, the Dynamic Flow Capture (DFC) application also supports intercepting IPv6 flows in M320, T320, T640, and T1600 routers with a Multiservices 400 or Multiservices 500 PIC. The DFC application can intercept passively monitored IPv6 traffic only. All support for IPv4 interception remains the same. The interception of IPv6 traffic happens in the same way the filters capture IPv4 flows. With the introduction of IPv6 interception, both IPv4 and IPv6 filters can coexist. The mediation device , however, cannot be located in an IPv6 network.

The DFC application does not support interception of VPLS and MPLS traffic. The application cannot intercept Address Resolution Protocol (ARP) or other Layer 2 exception packets. The interception filter can be configured to timeout based on factors like total time (seconds), idle time (seconds), total packets or total data transmitted (bytes).

PART 2

Configuration

CHAPTER 2

Configuration Task

Configuring Dynamic Flow Capture

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

```
[edit services]
dynamic-flow-capture {
    capture-group client-name {
        content-destination identifier {
            address address;
            hard-limit bandwidth;
            hard-limit-target bandwidth;
            soft-limit bandwidth;
            soft-limit-clear bandwidth;
            ttl hops;
        }
        control-source identifier {
            allowed-destinations [ destinations ];
            minimum-priority value;
            no-syslog;
            notification-targets address port port-number;
            service-port port-number;
            shared-key value;
            source-addresses [ addresses ];
        }
        duplicates-dropped-periodicity seconds;
        input-packet-rate-threshold rate;
        interfaces interface-name;
        max-duplicates number;
        pic-memory-threshold percentage percentage;
    }
    g-duplicates-dropped-periodicity seconds;
    g-max-duplicates number;
    traceoptions{
        file filename <files number> <size size> <world-readable | non-world-readable>;
    }
}
```

This section describes the following tasks for configuring dynamic flow capture:

Configuring the Capture Group

A capture group defines a profile of dynamic flow capture configuration information. The static configuration includes information about control sources, content destinations, and notification destinations. Dynamic configuration is added through interaction with control sources using a control protocol.

To configure a capture group, include the **capture-group** statement at the **[edit services dynamic-flow-capture]** hierarchy level:

```
capture-group client-name {
  content-destination identifier {
    address address;
    hard-limit bandwidth;
    hard-limit-target bandwidth;
    soft-limit bandwidth;
    soft-limit-clear bandwidth;
    ttl hops;
  }
  control-source identifier {
    allowed-destinations [ destinations ];
    minimum-priority value;
    no-syslog;
    notification-targets address port port-number;
    service-port port-number;
    shared-key value;
    source-addresses [ addresses ];
  }
  duplicates-dropped-periodicity seconds;
  input-packet-rate-threshold rate;
  interfaces interface-name;
  max-duplicates number;
  pic-memory-threshold percentage percentage;
}
```

To specify the **capture-group**, assign it a unique ***client-name*** that associates the information with the requesting control sources.

Configuring the Content Destination

You must specify a destination for the packets that match DFC PIC filter criteria. To configure the content destination, include the **content-destination** statement at the **[edit services dynamic-flow-capture capture-group *client-name*]** hierarchy level:

```
content-destination identifier {
  address address;
  hard-limit bandwidth;
  hard-limit-target bandwidth;
  soft-limit bandwidth;
  soft-limit-clear bandwidth;
  ttl hops;
}
```

Assign the **content-destination** a unique ***identifier***. You must also specify its IP address and you can optionally include additional settings:

- **address**—The DFC PIC interface appends an IP header with this destination address on the matched packet (with its own IP header and contents intact) and sends it out to the content destination.
- **ttl**—The time-to-live (TTL) value for the IP-IP header. By default, the TTL value is 255. Its range is 0 through 255.
- Congestion thresholds—You can specify per-content destination bandwidth limits that control the amount of traffic produced by the DFC PIC during periods of congestion. The thresholds are arranged in two pairs: **hard-limit** and **hard-limit-target**, and **soft-limit** and **soft-limit-clear**. You can optionally include one or both of these paired settings. All four settings are 10–second average bandwidth values in bits per second. Typically **soft-limit-clear** < **soft-limit** < **hard-limit-target** < **hard-limit**. When the content bandwidth exceeds the **soft-limit** setting:

  1. A congestion notification message is sent to each control source of the criteria that point to this content destination
  2. If the control source is configured for **syslog**, a system log message is generated.
  3. A latch is set, indicating that the control sources have been notified. No additional notification messages are sent until the latch is cleared, when the bandwidth falls below the **soft-limit-clear** value.

  When the bandwidth exceeds the **hard-limit** value:

  1. The dynamic flow capture application begins deleting criteria until the bandwidth falls below the **hard-limit-target** value.
  2. For each criterion deleted, a CongestionDelete notification is sent to the control source for that criterion.
  3. If the control source is configured for **syslog**, a log message is generated.

  The application evaluates criteria for deletion using the following data:

  - Priority—Lower priority criteria are purged first, after adjusting for control source minimum priority.

- Bandwidth—Higher bandwidth criteria are purged first.
- Timestamp—The more recent criteria are purged first.

Configuring the Control Source

You configure information about the control source, including allowed source addresses and destinations and authentication key values. To configure the control source information, include the **control-source** statement at the **[edit services dynamic-flow-capture capture-group *client-name*]** hierarchy level:

```
control-source identifier {
  allowed-destinations [ destination-identifiers ];
  minimum-priority value;
  no-syslog;
  notification-targets address port port-number;
  service-port port-number;
  shared-key value;
  source-addresses [ addresses ];
}
```

Assign the **control-source** statement a unique ***identifier***. You can also include values for the following statements:

- **allowed-destinations**—One or more content destination identifiers to which this control source can request that matched data be sent in its control protocol requests. If you do not specify any content destinations, all available destinations are allowed.
- **minimum-priority**—Value assigned to the control source that is added to the priority of the criteria in the DTCP ADD request to determine the total priority for the criteria. The lower the value, the higher the priority. By default, **minimum-priority** has a value of 0 and the allowed range is 0 through 254.
- **notification-targets**—One or more destinations to which the DFC PIC interface can log information about control protocol-related events and other events such as PIC bootup messages. You configure each **notification-target** entry with an IP **address** value and a User Datagram Protocol (UDP) **port** number.
- **service-port**—UDP port number to which the control protocol requests are directed. Control protocol requests that are not directed to this port are discarded by DFC PIC interfaces.
- **shared-key**—20-byte authentication key value shared between the control source and the DFC PIC monitoring platform.
- **source-addresses**—One or more allowed IP addresses from which the control source can send control protocol requests to the DFC PIC monitoring platform. These are /32 addresses.

Configuring the DFC PIC Interface

You specify the interface that interacts with the control sources configured in the same capture group. A Monitoring Services III PIC can belong to only one capture group, and you can configure only one PIC for each group.

To configure a DFC PIC interface, include the **interfaces** statement at the **[edit services dynamic-flow-capture capture-group *client-name*]** hierarchy level:

interfaces *interface-name*;

You specify DFC interfaces using the **dfc-** identifier at the **[edit interfaces]** hierarchy level. You must specify three logical units on each DFC PIC interface, numbered **0**, **1**, and **2**. You cannot configure any other logical interfaces.

- **unit 0** processes control protocol requests and responses.
- **unit 1** receives monitored data.
- **unit 2** transmits the matched packets to the destination address.

The following example shows the configuration necessary to set up a DFC PIC interface and intercept both IPv4 and IPv6 traffic:

```
[edit interfaces dfc-0/0/0]
unit 0 {
   family inet {
      filter {
         output high; #Firewall filter to route control packets
         # through 'network-control' forwarding class. Control packets
         # are loss sensitive.
      }
      address 10.1.0.0/32 { # DFC PIC address
         destination 10.36.100.1; # DFC PIC address used by
         # the control source to correspond with the
         # monitoring platform
      }
   }
unit 1 { # receive data packets on this logical interface
   family inet; # receive IPv4 traffic for interception
   family inet6; # receive IPv6 traffic for interception
}
unit 2 { # send out copies of matched packets on this logical interface
   family inet;
}
```

In addition, you must configure the dynamic flow capture application to run on the DFC PIC in the correct chassis location. The following example shows this configuration at the **[edit chassis]** hierarchy level:

```
fpc 0 {
   pic 0 {
      monitoring-services application dynamic-flow-capture;
   }
}
```

For more information on configuring chassis properties, see the Junos OS System Basics Configuration Guide.

Configuring the Firewall Filter

You can specify the firewall filter to route control packets through the network control forwarding class. The control packets are loss sensitive. To configure the firewall filter, include the following statements at the **[edit]** hierarchy level:

```
firewall {
  family inet {
    filter high {
      term all {
        then forwarding-class network-control;
      }
    }
  }
}
```

Configuring System Logging

By default, control protocol activity is logged as a separate system log facility, **dfc**. To modify the filename or level at which control protocol activity is recorded, include the following statements at the **[edit syslog]** hierarchy level:

```
file dfc.log {
  dfc any;
}
```

To cancel logging, include the **no-syslog** statement at the **[edit services dynamic-flow-capture capture-group** *client-name* **control-source** *identifier***]** hierarchy level:

```
no-syslog;
```

NOTE: The dynamic flow capture (dfc-) interface supports up to 10,000 filter criteria. When more than 10,000 filters are added to the interface, the filters are accepted, but system log messages are generated indicating that the filter is full.

Configuring Tracing Options for Dynamic Flow Capture Events

You can enable tracing options for dynamic flow capture events by including the **traceoptions** statement at the **[edit services dynamic-flow-capture]** hierarchy level.

When you include the **traceoptions** configuration, you can also specify the trace file name, maximum number of trace files, the maximum size of trace files, and whether the trace file can be read by all users or not.

To enable tracing options for dynamic flow capture events, include the following configuration at the **[edit services dynamic-flow-capture]** hierarchy level:

```
traceoptions{
  file filename <files number> <size size> <world-readable | non-world-readable>;
}
```

To disable tracing for dynamic flow control events, delete the **traceoptions** configuration from the **[edit services dynamic-flow-capture]** hierarchy level.

NOTE: In Junos OS releases earlier than 9.2R1, tracing of dynamic flow control was enabled by default, and the logs were saved to the /var/log/dfcd directory.

Configuring Thresholds

You can optionally specify threshold values for the following situations in which warning messages will be recorded in the system log:

- Input packet rate to the DFC PIC interfaces
- Memory usage on the DFC PIC interfaces

To configure threshold values, include the **input-packet-rate-threshold** or **pic-memory-threshold** statements at the **[edit services dynamic-flow-capture capture-group *client-name*]** hierarchy level:

```
input-packet-rate-threshold rate;
pic-memory-threshold percentage percentage;
```

If these statements are not configured, no threshold messages are logged. The threshold settings are configured for the capture group as a whole.

The range of configurable values for the **input-packet-rate-threshold** statement is 0 through 1 Mpps. The PIC calibrates the value accordingly; the Monitoring Services III PIC caps the threshold value at 300 Kpps and the Multiservices 400 PIC uses the full configured value. The range of values for the **pic-memory-threshold** statement is 0 to 100 percent.

Limiting the Number of Duplicates of a Packet

You can optionally specify the maximum number of duplicate packets the DFC PIC is allowed to generate from a single input packet. This limitation is intended to reduce the load on the PIC when packets are sent to multiple destinations. When the maximum number is reached, the duplicates are sent to the destinations with the highest criteria class priority. Within classes of equal priority, criteria having earlier timestamps are selected first.

To configure this limitation, include the **max-duplicates** statement at the **[edit services dynamic-flow-capture capture-group *client-name*]** hierarchy level:

```
max-duplicates number;
```

You can also apply the limitation on a global basis for the DFC PIC by including the **g-max-duplicates** statement at the **[edit services dynamic-flow-capture]** hierarchy level:

```
g-max-duplicates number;
```

By default, the maximum number of duplicates is set to 3. The range of allowed values is 1 through 64. A setting for **max-duplicates** for an individual capture-group overrides the global setting.

In addition, you can specify the frequency with which the application sends notifications to the affected control sources that duplicates are being dropped because the threshold has been reached. You configure this setting at the same levels as the maximum duplicates settings, by including the **duplicates-dropped-periodicity** statement at the **[edit services dynamic-flow-capture capture-group *client-name*]** hierarchy level or the **g-duplicates-dropped-periodicity** statement at the **[edit services dynamic-flow-capture]** hierarchy level:

```
duplicates-dropped-periodicity seconds;
g-duplicates-dropped-periodicity seconds;
```

As with the **g-max-duplicates** statement, the **g-duplicates-dropped-periodicity** statement applies the setting globally for the application and is overridden by a setting applied at the capture-group level. By default, the frequency for sending notifications is 30 seconds.

CHAPTER 3

Example

Example: Configuring Dynamic Flow Capture

The following example includes all parts of a complete dynamic flow capture configuration.

Configure the DFC PIC interface:

```
[edit interfaces dfc-0/0/0]
unit 0 {
   family inet {
      filter {
         output high; #Firewall filter to route control packets
         # through 'network-control' forwarding class. Control packets
         # are loss sensitive.
      }
      address 10.1.0.0/32 { # DFC PIC address
         destination 10.36.100.1; # DFC PIC address used by
         # the control source to correspond with the
         # monitoring platform
      }
   }
unit 1 { # receive data packets on this logical interface
   family inet;
   family inet6;
}
unit 2 { # send out copies of matched packets on this logical interface
   family inet;
}
```

Configure the capture group:

```
services dynamic-flow-capture {
   capture-group g1 {
      interfaces dfc-0/0/0;
      input-packet-rate-threshold 90k;
      pic-memory-threshold percentage 80;
      control-source cs1 {
         source-addresses 10.36.41.1;
         service-port 2400;
         notification-targets {
```

```
            10.36.41.1 port 2100;
          }
          shared-key "$9$ASxdsYoX7wg4aHk";
          allowed-destinations cd1;
        }
        content-destination cd1 {
          address 10.36.70.2;
          ttl 244;
        }
      }
    }
```

Configur3 filter-based forwarding (FBF) to the DFC PIC interface, logical unit 1.

For more information about configuring passive monitoring interfaces, see Enabling Passive Flow Monitoring.

```
interfaces so-1/2/0 {
  encapsulation ppp;
  unit 0 {
    passive-monitor-mode;
    family inet {
      filter {
        input catch;
      }
    }
  }
}
```

Configure the firewall filter:

```
firewall {
  filter catch {
    interface-specific;
    term def {
      then {
        count counter;
        routing-instance fbf_inst;
      }
    }
  }
  family inet {
    filter high {
      term all {
        then forwarding-class network-control;
      }
    }
  }
}
```

Configure a forwarding routing instance. The next hop points specifically to the logical interface corresponding to **unit 1**, because only this particular logical unit is expected to relay monitored data to the DFC PIC.

```
routing-instances fbf_inst {
  instance-type forwarding;
  routing-options {
    static {
```

```
        route 0.0.0.0/0 next-hop dfc-0/0/0.1;
      }
    }
  }
```

Configure routing table groups:

```
  [edit]
  routing-options {
    interface-routes {
      rib-group inet common;
    }
    rib-groups {
      common {
        import-rib [ inet.0 fbf_inst.inet.0 ];
      }
    }
    forwarding-table {
      export pplb;
    }
  }
```

Configure interfaces to the control source and content destination:

```
  interfaces fe-4/1/2 {
    description "to cs1 from dfc";
    unit 0 {
      family inet {
        address 10.36.41.2/30;
      }
    }
  }
  interfaces ge-7/0/0 {
    description "to cd1 from dfc";
    unit 0 {
      family inet {
        address 10.36.70.1/30;
      }
    }
  }
```

CHAPTER 4

Configuration Statements

address (Services Dynamic Flow Capture)

Syntax address *address*;

Hierarchy Level [edit services dynamic-flow-capture capture-group *client-name* content-destination *identifier*]

Release Information Statement introduced in Junos OS Release 7.4.

Description Configure an IP address for the flow capture destination.

Options ***address***—IP address for the content destination.

Usage Guidelines See "Configuring the Content Destination" on page 9.

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

allowed-destinations

Syntax allowed-destinations [*identifiers*];

Hierarchy Level [edit services dynamic-flow-capture capture-group *client-name* control-source *identifier*]

Release Information Statement introduced in Junos OS Release 7.4.

Description Identify flow capture destinations that are allowed in messages sent from this control source.

Options ***identifier***—Allowed content destination name.

Usage Guidelines See "Configuring the Control Source" on page 10.

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

capture-group

Syntax

```
capture-group client-name {
  content-destination identifier {
    address address;
    hard-limit bandwidth;
    hard-limit-target bandwidth;
    soft-limit bandwidth;
    soft-limit-clear bandwidth;
    ttl hops;
  }
  control-source identifier {
    allowed-destinations [ destinations ];
    minimum-priority value;
    no-syslog;
    notification-targets address port port-number;
    service-port port-number;
    shared-key value;
    source-addresses [ addresses ];
  }
  duplicates-dropped-periodicity seconds;
  input-packet-rate-threshold rate;
  interfaces interface-name;
  max-duplicates number;
  pic-memory-threshold percentage percentage;
}
```

Hierarchy Level [edit services dynamic-flow-capture]

Release Information Statement introduced in Junos OS Release 7.4.

Description Define the capture group values.

Options The remaining statements are explained separately.

Usage Guidelines See "Configuring the Capture Group" on page 8.

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

content-destination

Syntax

```
content-destination identifier {
    address (Services Dynamic Flow Capture) address;
    hard-limit bandwidth;
    hard-limit-target bandwidth;
    soft-limit bandwidth;
    soft-limit-clear bandwidth;
    ttl hops;
}
```

Hierarchy Level [edit services dynamic-flow-capture capture-group *client-name*]

Release Information Statement introduced in Junos OS Release 7.4.

Description Identify the destination for captured packets.

Options ***identifier***—Name of the destination.

The remaining statements are explained separately.

Usage Guidelines See "Configuring the Content Destination" on page 9.

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

control-source

Syntax

```
control-source identifier {
  allowed-destinations [ destinations ];
  minimum-priority value;
  no-syslog;
  notification-targets address port port-number;
  service-port port-number;
  shared-key value;
  source-addresses [ addresses ];
}
```

Hierarchy Level [edit services dynamic-flow-capture capture-group *client-name*]

Release Information Statement introduced in Junos OS Release 7.4.

Description Identify the source of the dynamic flow capture request.

Options *identifier*—Name of control source.

The remaining statements are explained separately.

Usage Guidelines See "Configuring the Control Source" on page 10.

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

duplicates-dropped-periodicity

Syntax duplicates-dropped-periodicity *seconds*;

Hierarchy Level [edit services dynamic-flow-capture capture-group *client-name*]

Release Information Statement introduced in Junos OS Release 9.2.

Description Specify the frequency for sending notifications to affected control sources when transmission of duplicate sets of data is restricted because the **max-duplicates** threshold has been reached.

Options *seconds*—Period for sending DuplicatesDropped notifications.

Default: 30 seconds

Usage Guidelines See "Limiting the Number of Duplicates of a Packet" on page 13.

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

Related Documentation

- g-duplicates-dropped-periodicity on page 24, max-duplicates on page 27

dynamic-flow-capture

Syntax

```
dynamic-flow-capture {
  capture-group client-name {
    content-destination identifier {
      address address;
      hard-limit bandwidth;
      hard-limit-target bandwidth;
      soft-limit bandwidth;
      soft-limit-clear bandwidth;
      ttl hops;
    }
    control-source identifier {
      allowed-destinations [ destinations ];
      minimum-priority value;
      no-syslog;
      notification-targets address port port-number;
      service-port port-number;
      shared-key value;
      source-addresses [ addresses ];
    }
    duplicates-dropped-periodicity seconds;
    input-packet-rate-threshold rate;
    interfaces interface-name;
    max-duplicates number;
    pic-memory-threshold percentage percentage;
  }
  g-duplicates-dropped-periodicity seconds;
  g-max-duplicates number;
}
```

Hierarchy Level [edit services]

Release Information Statement introduced in Junos OS Release 7.4.

Description Define the dynamic flow capture properties to be applied to traffic.

Options The remaining statements are explained separately.

Usage Guidelines See Dynamic Flow Capture.

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

g-duplicates-dropped-periodicity

Syntax g-duplicates-dropped-periodicity *seconds*;

Hierarchy Level [edit services dynamic-flow-capture]

Release Information Statement introduced in Junos OS Release 9.2.

Description Specify the frequency for sending notifications to affected control sources when transmission of duplicate sets of data is restricted because the **g-max-duplicates** threshold has been reached. This setting is applied globally; the **duplicates-dropped-periodicity** setting applied at the **capture-group** level overrides the global setting.

Default The default period for sending notifications is 30 seconds.

Options ***seconds***—Period for sending DuplicatesDropped notifications.

Usage Guidelines See "Limiting the Number of Duplicates of a Packet" on page 13.

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

Related Documentation

- duplicates-dropped-periodicity on page 22

g-max-duplicates

Syntax g-max-duplicates *number*;

Hierarchy Level [edit services dynamic-flow-capture]

Release Information Statement introduced in Junos OS Release 9.2.

Description Specify the maximum number of content destinations to which DFC PICs can send data from a single input set of packets. Limiting the number of duplicates reduces the load on the PIC. This setting is applied globally; the **max-duplicates** setting applied at the **capture-group** level overrides the global setting.

Default If no value is configured, a default setting of 3 is used.

Options ***number***—Maximum number of content destinations.
Range: 1 through 64

Usage Guidelines See "Limiting the Number of Duplicates of a Packet" on page 13.

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

Related Documentation
- max-duplicates on page 27

hard-limit

Syntax hard-limit *bandwidth*;

Hierarchy Level [edit services dynamic-flow-capture capture-group *client-name* content-destination *identifier*]

Release Information Statement introduced in Junos OS Release 9.2.

Description Specify a bandwidth threshold at which the dynamic flow capture application begins deleting criteria, until the bandwidth falls below the **hard-limit-target** value.

Options ***bandwidth***—Hard limit threshold, in bits per second.

Usage Guidelines See "Configuring the Content Destination" on page 9.

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

Related Documentation
- hard-limit-target on page 26

hard-limit-target

Syntax hard-limit-target *bandwidth*;

Hierarchy Level [edit services dynamic-flow-capture capture-group *client-name* content-destination *identifier*]

Release Information Statement introduced in Junos OS Release 9.2.

Description Specify a bandwidth threshold at which the dynamic flow capture application stops deleting criteria.

Options ***bandwidth***—Target value, in bits per second.

Usage Guidelines See "Configuring the Content Destination" on page 9.

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

Related Documentation

- hard-limit on page 25

input-packet-rate-threshold

Syntax input-packet-rate-threshold *rate*;

Hierarchy Level [edit services dynamic-flow-capture capture-group *client-name*]

Release Information Statement introduced in Junos OS Release 7.4.

Description Specify a packet rate threshold value that triggers a system log warning message.

Options ***rate***—Threshold value.

Usage Guidelines See "Configuring Thresholds" on page 13.

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

interfaces (Services Dynamic Flow Capture)

Syntax interfaces *interface-name*;

Hierarchy Level [edit services dynamic-flow-capture capture-group *client-name*]

Release Information Statement introduced in Junos OS Release 7.4.

Description Specify the DFC interface used with the control source configured in the same capture group.

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

Usage Guidelines See "Configuring the DFC PIC Interface" on page 10.

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

max-duplicates

Syntax max-duplicates *number*;

Hierarchy Level [edit services dynamic-flow-capture capture-group *client-name*]

Release Information Statement introduced in Junos OS Release 9.2.

Description Specify the maximum number of content destinations to which the DFC PIC can send data from a single input set of packets. Limiting the number of duplicates reduces the load on the PIC. This setting overrides the globally applied **g-max-duplicates** setting.

Default If no value is configured, a default setting of 3 is used.

Options ***number***—Maximum number of content destinations.
Range: 1 through 64

Usage Guidelines See "Limiting the Number of Duplicates of a Packet" on page 13.

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

Related Documentation

- g-max-duplicates on page 25

minimum-priority

Syntax minimum-priority *value*;

Hierarchy Level [edit services dynamic-flow-capture capture-group *client-name* control-source *identifier*]

Release Information Statement introduced in Junos OS Release 9.2.

Description Specify the minimum priority for the control source.

Options *value*—Minimum priority value; if not specified, defaults to 0.
Range: 0 through 254

Usage Guidelines See "Configuring the Control Source" on page 10.

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

no-syslog

Syntax no-syslog;

Hierarchy Level [edit services dynamic-flow-capture capture-group *client-name* control-source *identifier*]

Release Information Statement introduced in Junos OS Release 7.4.

Description Disable system logging of control protocol requests and responses. By default, these messages are logged.

Usage Guidelines See "Configuring System Logging" on page 12.

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

notification-targets

Syntax notification-targets *address* port *port-number*;

Hierarchy Level [edit services dynamic-flow-capture capture-group *client-name* control-source *identifier*]

Release Information Statement introduced in Junos OS Release 7.4.

Description List of destination IP addresses and User Datagram Protocol (UDP) ports to which DFC PICs log exception information and control protocol state transitions, such as timeout values.

Options **address *address***—Allowed destination IP address.

port *port-number*—Allowed destination UDP port number.

Usage Guidelines See "Configuring the Control Source" on page 10.

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

pic-memory-threshold

Syntax pic-memory-threshold percentage *percentage*;

Hierarchy Level [edit services dynamic-flow-capture capture-group *client-name*]

Release Information Statement introduced in Junos OS Release 7.4.

Description Specify a PIC memory usage percentage that triggers a system log warning message.

Options **percentage *percentage***—PIC memory threshold value.

Usage Guidelines See "Configuring Thresholds" on page 13.

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

service-port

Syntax service-port *port-number*;

Hierarchy Level [edit services dynamic-flow-capture capture-group *client-name* control-source *identifier*]

Release Information Statement introduced in Junos OS Release 7.4.

Description Identify the User Datagram Protocol (UDP) port number for control protocol requests.

Options ***port-number***—Port number for control protocol request messages.

Usage Guidelines See "Configuring the Control Source" on page 10.

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

shared-key

Syntax shared-key *value*;

Hierarchy Level [edit services dynamic-flow-capture capture-group *client-name* control-source *identifier*]

Release Information Statement introduced in Junos OS Release 7.4.

Description Configure the authentication key value.

Options ***value***—Secret authentication value shared between a control source and destination.

Usage Guidelines See "Configuring the Control Source" on page 10.

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

soft-limit

Syntax soft-limit *bandwidth*;

Hierarchy Level [edit services dynamic-flow-capture capture-group *client-name* content-destination *identifier*]

Release Information Statement introduced in Junos OS Release 9.2.

Description Specify a bandwidth threshold at which congestion notifications are sent to each control source of the criteria that point to this content destination. If the control source is configured with the **syslog** statement, a log message will also be generated.

Options ***bandwidth***—Soft limit threshold, in bits per second.

Usage Guidelines See "Configuring the Content Destination" on page 9.

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

soft-limit-clear

Syntax soft-limit-clear *bandwidth*;

Hierarchy Level [edit services dynamic-flow-capture capture-group *client-name* content-destination *identifier*]

Release Information Statement introduced in Junos OS Release 9.2.

Description Specify a bandwidth threshold at which the latch set by the soft-limit threshold is cleared.

Options ***bandwidth***—Soft-limit clear threshold, in bits per second.

Usage Guidelines See "Configuring the Content Destination" on page 9.

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

Related Documentation

- soft-limit on page 31

source-addresses

Syntax source-addresses [*addresses*];

Hierarchy Level [edit services dynamic-flow-capture capture-group *client-name* control-source *identifier*]

Release Information Statement introduced in Junos OS Release 7.4.

Description List of IP addresses from which the control source can send control protocol requests to the Juniper Networks router.

Options ***address***—Allowed IP source address.

Usage Guidelines See "Configuring the Control Source" on page 10.

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

ttl

Syntax ttl *hops*;

Hierarchy Level [edit services dynamic-flow-capture capture-group *client-name* content-destination *identifier*]

Release Information Statement introduced in Junos OS Release 7.4.

Description Time-to-live (TTL) value for the IP-IP header.

Options ***hops***—TTL value.

Usage Guidelines See "Configuring the Content Destination" on page 9.

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

PART 3

Administration

CHAPTER 5

Flow Collection and Monitoring Operational Mode Commands

clear services dynamic-flow-capture

Syntax clear services dynamic-flow-capture capture-group *group-name*
<criteria-identifier *identifier*>
<destination-identifier *identifier*>
<force>
<static>

Release Information Command introduced in Junos OS Release 7.4.

Description (M320 routers and T Series routers only) Clear dynamic flow capture information for specified capture group.

Options

capture-group *group-name*—Capture-group identifier.

criteria-identifier *identifier*—(Optional) Criteria identifier.

destination-identifier *identifier*—(Optional) Content destination identifier.

force—(Optional) Force clearing of criteria.

static—(Optional) Clear static criteria.

Required Privilege Level network

List of Sample Output clear services dynamic-flow-capture on page 36

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services dynamic-flow-capture

```
user@host> clear services dynamic-flow-capture capture-group flow-a
```

show services dynamic-flow-capture content-destination

Syntax show services dynamic-flow-capture content-destination capture-group *group-name* destination-identifier *identifier* <terse>

Release Information Command introduced in Junos OS Release 7.4.

Description (M320 routers and T Series routers only) Display information about the content destination that receives packets from the dynamic flow capture (DFC) interface.

Options

capture-group *group-name*—Capture-group identifier.

destination-identifier *identifier*—Content destination identifier.

terse—(Optional) Display summary information.

Required Privilege Level view

List of Sample Output show services dynamic-flow-capture content-destination on page 38

Output Fields Table 3 on page 37 lists the output fields for the **show services dynamic-flow-capture content-destination** command. Output fields are listed in the approximate order in which they appear.

Table 3: show services dynamic-flow-capture content-destination Output Fields

Output Field	Output Field Description	Level of Output
Capture group	Name of the capture group.	to be provided
Content destination	Name of the content destination.	to be provided
Criteria	Number of criteria specified.	to be provided
Bandwidth	Bandwidth used by the matched traffic.	to be provided
Matched packets	Number of matched packets sent to the content destination.	to be provided
Matched bytes	Number of matched bytes sent to the content destination.	to be provided
Congestion notifications	Number of notification messages sent.	to be provided

Sample Output

show services dynamic-flow-capture content-destination

```
user@host> show services dynamic-flow-capture content-destination capture-group g1
destination-identifier cd1 terse
  Capture group: g1, Content destination: cd1, Criteria: 0, Bandwidth: 0, Matched
 packets: 0, Matched bytes: 0, Congestion notifications: 0
```

show services dynamic-flow-capture control-source

Syntax

show services dynamic-flow-capture control-source capture-group *group-name*
control-source *identifier*
<detail | terse>

Release Information

Command introduced in Junos OS Release 7.4.

Description

(M320 routers and T Series routers only) Display information about the control source that makes dynamic flow capture requests to the dynamic flow capture interface.

Options

capture-group *group-name*—Capture group identifier.

control-source *identifier*—Control source identifier.

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

Required Privilege Level

view

List of Sample Output

show services dynamic-flow-capture control-source on page 40
show services dynamic-flow-capture control-source detail on page 40

Output Fields

Table 4 on page 39 lists the output fields for the **show services dynamic-flow-capture control-source** scommand. Output fields are listed in the approximate order in which they appear.

Table 4: show services dynamic-flow-capture control-source Output Fields

Output Field	Output Field Description
Capture group	Name of the capture group.
Control source	Name of the control source.
Criteria added, Criteria add failed	Number of criteria added or added and failed.
Active criteria	Number of active criteria.
Static criteria, Dynamic criteria	Number of static or dynamic criteria.
Control protocol requests	Total number of control protocol requests.
Requests	Number of **Add**, **Delete**, **List**, **Refresh**, and **No-op** control protocol requests.
Failed	Number of **Add**, **Delete**, **List**, **Refresh**, and **No-op** failed control protocol requests.
Add request rate	Rate of add requests.

Table 4: show services dynamic-flow-capture control-source Output Fields *(continued)*

Output Field	Output Field Description
Add request peak rate	Peak rate of add requests.
Bandwidth across all criteria	Bandwidth used by all the requests.
Total notifications	Total number of notifications sent and the number of notifications by category: **Restart**, **Rollover**, **Timeout**, **Congestion**, **Congestion delete**, and **Dups** (duplicates) dropped.
Criteria deleted	Total number of criteria deleted and the number of deleted criteria by category: **Timeout idle**, **Timeout total**, **Packets**, and **Bytes**.
Sequence number	Sequence number.

Sample Output

show services dynamic-flow-capture control-source

```
user@host> show services dynamic-flow-capture control-source source-identifier cs0_cg0
capture-group cg_0
Capture group: cg_0, Control source: cs0_cg0
 Criteria added: 28, Criteria add failed: 0, Active criteria: 0, Control protocol
 requests: 28,  Add request rate: 0,
 Add request peak rate: 1, Bandwidth across all criteria: 0, Total notifications:
 1, Criteria deleted: 28, Sequence number: 0
```

show services dynamic-flow-capture control-source detail

```
user@host> show services dynamic-flow-capture control-source source-identifier cs0_cg0
capture-group cg_0 detail
Capture group: cg_0, Control source: cs0_cg0
  Criteria added: 28, Criteria add failed: 0
  Active criteria: 0
    Static criteria: 0, Dynamic criteria: 0
  Control protocol requests: 28
                     Add        Delete          List       Refresh         No-op

    Requests          28             0             0             0             0

    Failed             0             0             0             0             0

  Add request rate: 0
  Add request peak rate: 1
  Bandwidth across all criteria: 0
  Total notifications: 1
    Restart: 1, Rollover: 0, No-op: 0, Timeout: 0, Congestion: 0, Congestion
delete: 0, Dups dropped: 0
  Criteria deleted: 28
    Timeout idle: 0, Timeout total: 0, Packets: 0, Bytes: 0
  Sequence number: 0
```

show services dynamic-flow-capture statistics

Syntax show services dynamic-flow-capture statistics capture-group *group-name*

Release Information Command introduced in Junos OS Release 7.4.

Description (M320 routers and T Series routers only) Display statistics information about the capture group specified for dynamic flow capture.

Options **capture-group *group-name***—Capture group identifier.

Required Privilege Level view

List of Sample Output show services dynamic-flow-capture statistics on page 43

Output Fields Table 5 on page 41 lists the output fields for the **show services dynamic-flow-capture statistics** command. Output fields are listed in the approximate order in which they appear.

Table 5: show services dynamic-flow-capture statistics Output Fields

Output Field	Output Field Description
Input	Incoming dynamic flow capture packet statistics: • **Control protocol packets**—Number of control protocol packets received. • **Captured data packets**—Number of data packets captured. • **Control IRI packets**—Number of control IRI packets received.
Control protocol drops	Control protocol packets dropped for the following reasons: • **Not IP packets**—Dropped packets were not IP packets. • **Not UDP packets**—Dropped packets were not User Datagram Protocol (UDP) packets. • **Invalid destination address**—Dropped packets had invalid destination addresses. • **No memory**—Packets dropped because of insufficient memory. • **Unauthorized control source**—Packets dropped because the control source was not authenticated. • **Bad request**—Packets dropped because the request was invalid. • **Unknown control source**—Packets dropped because the control source was not known. • **Not DTCP**—Dropped packets did not adhere to the control protocol format. • **Bad command line**—Packets dropped because of a version mismatch. • **Bandwidth exceeded**—Packets dropped because the bandwidth was exceeded. • **Drop rate due to exceeded bandwidth**—Rate of traffic dropped because the bandwidth was exceeded. • **Other**—Packets dropped for other reasons or undetermined causes.

Table 5: show services dynamic-flow-capture statistics Output Fields *(continued)*

Output Field	Output Field Description
Input drops	Incoming dynamic flow capture packets dropped for the following reasons: • **Unknown packets**—Packets dropped because the packet type was not recognized. • **Captured data not IPv4**—Packets dropped because they were not IPv4 packets. • **Captured data too small**—Packets dropped because they were smaller than the size reported in their headers. • **Captured data drops**—Data packets dropped because of undetermined causes. • **Captured data not matched**—Packets dropped because they did not match filter criteria. • **Bandwidth exceeded**—Packets dropped because the bandwidth was exceeded. • **Drop rate due to exceeded bandwidth**—Rate of traffic dropped because the bandwidth was exceeded.
Output	Outgoing dynamic flow capture packet statistics: • **Control protocol packets**—Number of control protocol packets sent. • **Captured data packets**—Number of captured data packets sent.
Output drops	Outgoing packets dropped: • **Control protocol drops**—Number of control protocol packets dropped. • **Captured data drops**—Number of captured data packets dropped.
Flow Statistics	DFC flow statistics: • **Active flow cache entries** • **Active flow cache usage percentage** • **Flow cache entries allocated** • **Number of control sources** • **Number of content destinations** • **Number of criteria** • **Maximum criteria matching one flow** • **Cached flows purged for memory** • **Maximum filters matching one packet**

Sample Output

show services dynamic-flow-capture statistics

```
user@host> show services dynamic-flow-capture statistics capture-group g1
Input:

  Control protocol packets: 643, Captured data packets: 69977, Control IRI packets:
 337

Control protocol drops:

  Not IP packets: 0, Not UDP packets: 3, Invalid destination address: 0, No memory:
 0, Unauthorized control source: 0,

  Bad request: 0, Unknown control source: 0, Not DTCP: 0, Bad command line: 0,
Bandwidth exceeded: 0,

  Drop rate due to exceeded bandwidth: 0, Other: 0

Input drops:

  Unknown packets: 0, Captured data not IPv4: 0, Captured data too small: 0,
Captured data drops: 0, Captured data not matched: 0,

  Bandwidth exceeded: 0, Drop rate due to exceeded bandwidth: 0

Output:

  Control protocol packets: 644, Captured data packets: 1119624

Output drops:

  Control protocol drops: 0, Captured data drops: 0

Flow Statistics:

  Active flow cache entries: 40, Active flow cache usage percentage: 0, Flow cache
 entries allocated: 40,

  Number of control sources: 4, Number of content destinations: 64, Number of
criteria: 640,

  Maximum criteria matching one flow: 16, Cached flows purged for memory: 0,
Maximum filters matching one packet: 16
```

CHAPTER 6

Flow Collector and Monitoring Interface Operational Mode Commands

show interfaces (Dynamic Flow Capture)

Syntax show interfaces dfc-*fpc/pic/port*:*channel*
<brief | detail | extensive | terse>
<descriptions>
<media>
<snmp-index *snmp-index*>
<statistics>

Release Information Command introduced in Junos OS Release 7.4.

Description (M320 and M120 routers and T Series routers only) Display status information about the specified dynamic flow capture interface.

Options

dfc-*fpc/pic/port*:*channel*—Display standard status information about the specified dynamic flow capture interface.

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

descriptions—(Optional) Display interface description strings.

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

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

statistics—(Optional) Display static interface statistics.

Required Privilege Level view

List of Sample Output show interfaces (Dynamic Flow Capture) on page 49

Output Fields Table 6 on page 46 lists the output fields for the **show interfaces** (Dynamic Flow Capture) command. Output fields are listed in the approximate order in which they appear.

Table 6: Dynamic Flow Capture show interfaces Output Fields

Field Name	Field Description	Level of Output
Physical Interface		
Physical interface	Name of the physical interface.	All levels
Enabled	Sate of the interface. Possible values are described in the "Enabled Field" section under Common Output Fields Description.	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
Type	Type of interface.	All levels

Table 6: Dynamic Flow Capture show interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
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
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 Common Output Fields Description.	All levels
Interface flags	Information about the interface. Possible values are described in the "Interface Flags" section under Common Output Fields Description.	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 Common Output Fields Description.	All levels
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**
Input Rate	Input rate in bits per second (bps) and packets per second (pps).	None specified
Output Rate	Output rate in bps and pps.	None specified
Traffic statistics	Number and rate of bytes and packets received and transmitted on the physical interface. • **Input rate**, **Output rate**—Number of bits per second (packets per second) received and transmitted on the interface. • **Input packets**, **Output packets**—Number of packets received and transmitted on the interface.	**detail extensive**
Input errors	• **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 the Junos OS does not support. • **Resource errors**—Sum of transmit drops.	**extensive**

Table 6: Dynamic Flow Capture show interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
Output errors	• **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
Flags	Information about the logical interface; values are described in the "Logical Interface Flags" section under Common Output Fields Description.	All levels
Encapsulation	Encapsulation on the logical interface.	All levels
Input packets	Number of packets received on the logical interface.	None specified
Output packets	Number of packets transmitted on the logical interface.	None specified
Traffic statistics	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. • **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**
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
Flags	Information about the protocol family flags. Possible values are described in the "Family Flags" section under Common Output Fields Description.	**detail extensive** none
Addresses, Flags	Addresses associated with the logical interface and information about the address flags. Possible values are described in the "Addresses Flags" section under Common Output Fields Description.	**detail extensive** none

Table 6: Dynamic Flow Capture show interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
Destination	IP address of the remote side of the connection.	**detail extensive** none
Local	IP address of the logical interface.	**detail extensive** none

Sample Output

show interfaces (Dynamic Flow Capture)

```
user@host> show interfaces dfc-0/0/0
Physical interface: dfc-0/0/0, Enabled, Physical link is Up
 Interface index: 146, SNMP ifIndex: 36
 Type: Adaptive-Services, Link-level type: Dynamic-Flow-Capture, MTU: 9192, Speed:
 2488320kbps
 Device flags : Present Running
 Interface flags: Point-To-Point SNMP-Traps 16384
 Link type : Full-Duplex
 Link flags : None
 Last flapped : 2005-08-26 15:08:36 PDT (01:18:42 ago)
 Input rate : 0 bps (0 pps)
 Output rate : 44800440 bps (100000 pps)

Logical interface dfc-0/0/0.0 (Index 67) (SNMP ifIndex 43)
 Flags: Point-To-Point SNMP-Traps Encapsulation: Dynamic-Flow-Capture
Input packets : 74
Output packets: 132
 Protocol inet, MTU: 9192
  Flags: Receive-options, Receive-TTL-Exceeded
  Addresses, Flags: Is-Preferred Is-Primary
   Destination: 10.36.100.1, Local: 10.36.100.2

Logical interface dfc-0/0/0.1 (Index 68) (SNMP ifIndex 49)
 Flags: Point-To-Point SNMP-Traps Encapsulation: Dynamic-Flow-Capture
Input packets : 0
Output packets: 402927263
 Protocol inet, MTU: 9192
  Flags: Receive-options, Receive-TTL-Exceeded

Logical interface dfc-0/0/0.2 (Index 69) (SNMP ifIndex 50)
 Flags: Point-To-Point SNMP-Traps Encapsulation: Dynamic-Flow-Capture
Input packets : 0
Output packets: 0
 Protocol inet, MTU: 9192
  Flags: Receive-options, Receive-TTL-Exceeded

Logical interface dfc-0/0/0.16383 (Index 70) (SNMP ifIndex 44)
 Flags: Point-To-Point SNMP-Traps Encapsulation: Dynamic-Flow-Capture
Input packets : 1427
Output packets: 98
 Protocol inet, MTU: 9192
  Flags: Receive-options, Receive-TTL-Exceeded
  Addresses, Flags: Is-Preferred Is-Primary
   Destination: 10.0.0.16, Local: 10.0.0.1
```

PART 4

Index

Index

Symbols

A

B

C

D

F

G

H