JUNIPER NETWORKS

Junos® OS

Packet-Triggered Subscribers and Policy Control Feature Guide

Release
14.1

Published: 2014-04-25

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

Junos® OS Packet-Triggered Subscribers and Policy Control Feature Guide
14.1

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 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:

- 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.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.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

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**

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

Convention	Description	Examples
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User 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)	Encloses 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)	Encloses a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identifies 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.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.

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

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to **techpubs-comments@juniper.net**, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/

- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

CHAPTER 1

PTSP Overview

PTSP Overview

The packet-triggered subscribers and policy control (PTSP) feature allows the application of policies to individual source IP addresses flowing through a given interface. A subscriber context is created for each distinct source IP address seen in a given underlying interface. This feature can be used to support dynamic subscribers that are controlled by a subscriber termination device, such as a B-RAS or GGSN device, that is connected to an MX Series 3D Universal Edge Router.

PTSP has the following responsibilities:

- Create a subscriber context for each distinct IPv4 address on a given interface (subscriber context).
- Apply policies to or remove policies from the subscriber context.
- Collect statistics and report for each individual policy for each subscriber context.
- Derive information about subscribers.

You can associate specific subscriber contexts based on IPv4 addresses and provide service activation and deactivation for these subscribers. The Multiservices DPC (MS-DPC) maintains a table of addresses for each subscriber and any corresponding policies. If an address is not found in the subscriber table, then a new subscriber context is created. All policies are defined on a per-subscriber basis. Once the subscribers are present in the subscriber table, PSTP enforces the policies active for the subscriber context. PTSP can report the subscribers to the SAE using the Diameter protocol so that the SRC software can manage the subscribers and services with dynamic policies. You can also configure static policies, but dynamic policies take precedence over static policies. When you

download a new dynamic policy, it takes effect only for new flows. All new flows and TCP connections use the new dynamic policy. Existing flows are not affected by the new policy unless they timeout, after which they are considered a new flow.

Statistics collection that is aggregated on a service rule basis is also shared with the SAE using the Diameter application. These statistics are not written to a flat file. Statistics collection that is aggregated on an application or application group basis is written to a flat file. These statistics are not shared with the SAE using the Diameter protocol.

Hardware Requirements for PTSP for Subscriber Access

PTSP is supported on Juniper Networks MX Series 3D Universal Edge Routers. You must have a Multiservices DPC (MS-DPC) on the MX Series router.

Related Documentation

- Configuring PTSP on page 29

Juniper Networks Session and Resource Control (SRC) and PTSP Overview

The Juniper Networks Session and Resource Control (SRC) environment provides a central administrative point for managing subscribers and their services. The SRC software runs on Juniper Networks C Series Controllers. The SRC software uses the Diameter protocol for communications between the local peer on a Juniper Networks routing platform and the remote SRC peer on a C Series Controller. The local peer is known as PTSP and is part of the AAA application. The remote SRC peer is the service activation engine (SAE); the SAE acts as the controlling agent in the SRC environment.

The SRC software enables the SAE to activate and deactivate subscriber services (described by SRC policies). The SAE installs or removes policies using a service rule policy template called **__svc_rule__**. This policy template indicates which policy is applied to a new subscriber session. Additional policies are bound to new sessions; they do not affect existing sessions. Note that policy name must be unique between PPR requests. You can use the same rule name within a single request, but you cannot use the same name again in a separate request.

Statistics collection that is aggregated on a service rule basis is also shared with the SAE using the Diameter protocol.

NOTE: More than one Diameter-based application (function) can run on a router simultaneously.

NOTE: When the SRC software downloads PTSP policies, it matches all the application groups defined in the rule of the PTSP policy if the **appliation-group-any** keyword is used in the policy. The **application-group-any** keyword is not configured on the router although the application group name is defined in the application identification configuration database on the router to process application-aware access list (AACL) rules for accepting or discarding packets. The keyword is considered as an exception because the application group is defined in the application identification database.

Related Documentation

- Messages Used by Diameter Applications on page 5
- Diameter AVPs and Diameter Applications on page 10
- Understanding PTSP-SAE Interactions on page 19
- Configuring the PTSP Application on page 29
- Configuring PTSP on page 29

Messages Used by Diameter Applications

The following Diameter applications are supported by Junos OS:

- JSRC—A Juniper Networks Diameter application registered with the IANA (http://www.iana.org) as Juniper Policy-Control-JSRC, with an ID of 16777244. Communicates with the SAE (remote SRC peer).
- PTSP—A Juniper Networks Diameter application registered with the IANA (http://www.iana.org) as Juniper JGx, with an ID of 16777273. Communicates with the SAE (remote SRC peer).
- Gx-Plus—An application that extends the 3GPP Gx interface for wireline use cases. 3GPP Gx is registered with the IANA (http://www.iana.org). Communicates with a PCRF.

  If data for a particular AVP included in a message is not available to the router, Gx-Plus simply omits the AVP from the message it sends to the PCRF. If the PCRF determines it has insufficient information to make a decision, it may deny the request. The Diameter answer messages include the Result-Code AVP (AVP 268); the values of this AVP convey success, failure, or errors to the requestor.

Juniper Networks has also registered the Juniper-Session-Recovery application (16777296) and two new command codes (8388628 for Juniper-Session-Events and 8388629 for Juniper-Session-Discovery) with the IANA (http://www.iana.org).

Table 3 on page 6 describes Diameter messages the applications use.

Table 3: Diameter Messages and Diameter Applications

Diameter Message	Code	Application	Description
AA-Request (AAR)	265	JSRC, PTSP	Request from the application to the SAE at new subscriber login or during SAE-application synchronization. The request can be one of three types: address-authorization, provisioning-request, or synchronization.
AA-Answer (AAA)	265	JSRC, PTSP	Response from the SAE to the application's AA-Request message.
Abort-Session-Request (ASR)	274	JSRC, PTSP	Request from the SAE to the application to log out a provisioned subscriber.
Abort-Session-Answer (ASA)	274	JSRC, PTSP	Response from the application to the SAE's ASR message. If the application sends the logout request to AAA, the ASA message includes a success notification (ACK). If the logout failed, the ASA message includes a failure notification (NAK).
Accounting-Request (ACR)	271	JSRC, PTSP	Request from the SAE to the application or from the application to the SAE for statistics.
Accounting-Answer (ACA)	271	JSRC, PTSP	Response to the ACR message to provide statistics for each installed policy (service).

Table 3: Diameter Messages and Diameter Applications *(continued)*

Diameter Message	Code	Application	Description
Credit-Control-Request (CCR)	272	Gx-Plus	Request from Gx-Plus to the PCRF at subscriber login, logout, or update. An initial request (CCR-I) is sent when a subscriber logs in and AAA is requested to activate the subscriber's session. Gx-Plus retries the CCR-I message if a CCA-I message is not received from the PCRF within 10 seconds. The CCR-I message is retried up to 3 times. If no CCA-I is received after the 4 CCR-I messages have been sent—the first message plus 3 retries—then Gx-Plus starts sending CCR-N messages. CCR-N messages are retried forever until a success or failure response is received from the PCRF. CCR-N messages include the Juniper-Provisioning-Source AVP (AVP code 2101) set to local to notify the PCRF that the router has the authority to make a local decision regarding subscriber service activation. An update request (CCR-U) message is sent when a usage threshold is reached. The CCR-U reports the actual usage for all statistics. The PCRF may return a CCA-U message that includes new monitoring thresholds, service activations, service deactivations. A CCR-U is also sent to report the status of service activation or deactivation. A termination request (CCR-T) is sent at subscriber logout to inform the PCRF that a provisioned subscriber session is being terminated. CCR-T messages are retried forever until a success response is received from the PCRF.

Table 3: Diameter Messages and Diameter Applications *(continued)*

Diameter Message	Code	Application	Description
Credit-Control-Answer (CCA)	272	Gx-Plus	Reply from the PCRF to a CCR message. In response to a CCR-I, the PCRF returns a CCA-I message that indicates success (DIAMETER_SUCCESS) or failure (DIAMETER AUTHORIZATION REJECTED) depending on whether the subscriber has sufficient credit for the requested services. All other responses are ignored and the CCR-I is retried. In response to a CCR-T, the PCRF returns a CCA-T message that indicates a successful termination with a value of 2001 (DIAMETER SUCCESS) in the Result-Code AVP. All other responses are ignored and the CCR-T is retried. A CCA-N is a response to a CCR-N.
Juniper-Session-Discovery-Request (JSDR)	8388629	Gx-Plus	Discovery request from the PCRF to Gx-Plus to discover subscriber sessions on the router.
Juniper-Session-Discovery-Answer (JSDA)	8388629	Gx-Plus	Reply from router to a JSDR message; describes session information. The Result-Code AVP includes one of the following values, or an error value: • 2001—DIAMETER_SUCCESS; the end of the database was reached, meaning all information has been sent. • 2002—DIAMETER_LIMITED_SUCCESS; some of the session information was sent, but more remains to be sent.
Juniper-Session-Event-Request (JSER)	8388628	Gx-Plus	Request from router to PCRF regarding events that take place on the router. Notifies the PCRF of certain events on the router by including the Juniper-Event-Type AVP (AVP code 2103). Events reported include cold or warm boots, explicit discovery requests, substantial configuration changes, non-response or error response from PCRF, and exhaustion of fault-tolerant resources.
Juniper-Session-Event-Answer (JSEA)	8388628	Gx-Plus	Reply from PCRF to a JSER message.
Push-Profile-Request (PPR)	288	JSRC, PTSP	Request from the SAE to the router to activate or deactivate services for a subscriber.

Table 3: Diameter Messages and Diameter Applications *(continued)*

Diameter Message	Code	Application	Description
Push-Profile-Answer (PPA)	288	JSRC, PTSP	Response from the router to the SAE's PPR message. Includes success or failure notification for each of the service activation or deactivation commands in the request.
Re-Auth-Request (RAR)	258	Gx-Plus	Audit request from the PCRF to router to determine whether a specific subscriber is still present.
Re-Auth-Answer (RAA)	258	Gx-Plus	Reply from router to a RAR message; indicates whether the subscriber is active. The Result-Code AVP includes one of the following values: • 2001—DIAMETER_SUCCESS; subscriber entry was found. • 5002—DIAMETER_UNKNOWN_SESSION_ID; subscriber entry was not found. • 3002—DIAMETER_UNABLE_TO_DELIVER; Gx-Plus is not configured.
Session-Resource-Query (SRQ)	277	JSRC, PTSP	Request from the router to the SAE or from the SAE to the router to initiate synchronization between router and the SAE.
Session-Resource-Reply (SRR)	277	JSRC, PTSP	Response to the SRQ message to begin synchronization.
Session-Termination-Request (STR)	275	JSRC, PTSP	Notification from the router to the SAE that a provisioned subscriber has logged out.
Session-Termination-Answer (STA)	275	JSRC, PTSP	Response from the SAE to the router's STR message. Includes success or failure notification.

Related Documentation

- *Juniper Networks Session and Resource Control (SRC) and JSRC Overview*
- *Understanding JSRC-SAE Interactions*
- Juniper Networks Session and Resource Control (SRC) and PTSP Overview on page 4
- Understanding PTSP-SAE Interactions on page 19
- *Gx-Plus for Provisioning Subscribers Overview*
- *Understanding Gx-Plus Interactions Between the Router and the PCRF*

Diameter AVPs and Diameter Applications

Diameter conveys information by including various attribute-value pairs (AVPs) in Diameter messages. Table 4 on page 10 lists the standard Diameter AVPs used in interactions with the supported Diameter applications. Diameter reserves AVP code numbers 0 through 255 for RADIUS AVPs that are implemented in Diameter.

Table 4: Standard Diameter AVPs

Attribute Number	Diameter AVP	Application	Description	Type
1	User-Name	Gx-Plus, JSRC	Specifies the username. For a subscriber managed by AAA, the value is the subscriber's login name. For a static interface, the value is the interface name, which is used as the subscriber's login name.	UTF8String
8	Framed-IP-Address	Gx-Plus, JSRC, PTSP	Identifies the IPv4 address configured for the subscriber. This is the same value as for RADIUS Framed-IP-Address attribute [8].	OctetString
55	Event-Timestamp	Gx-Plus, JSRC, PTSP	Specifies the time of the event that triggered the message in which this AVP is included. Time is indicated in seconds since January 1, 1900, 00:00 UTC.	Time
85	Acct-Interim-Interval	JSRC, PTSP	Number of seconds between each interim accounting update for this session. The router uses the following guidelines for interim accounting: • Attribute value is within the acceptable range (600 through 86,400 seconds)—Accounting is updated at the specified interval. • Attribute value is less than the minimum acceptable value—Accounting is updated at the minimum interval (600 seconds). • Attribute value is greater than the maximum acceptable value—Accounting is updated at the maximum interval (86,400 seconds).	Unsigned32
87	NAS-Port-Id	Gx-Plus, JSRC, PTSP	Identifies the port of the NAS that authenticates the user. This is the same value as for RADIUS NAS-Port-Id attribute [87].	UTF8String
263	Session-ID	Gx-Plus, JSRC, PTSP	Specifies the subscriber session identifier. The router assigns the value to uniquely identify a subscriber session.	UTF8String

Table 4: Standard Diameter AVPs *(continued)*

Attribute Number	Diameter AVP	Application	Description	Type
268	Result-Code	Gx-Plus, JSRC, PTSP	Indicates whether a request completed successfully. Provides an error code if the request failed. The following classes are recognized by Diameter: • 1xxx—Informational • 2xxx—Success • 3xxx—Protocol errors • 4xxx—Transient errors • 5xxx—Permanent failures Unrecognized classes, which begin with numerals 6–9 or 0, are handled as permanent failures. JSRC and PTSP support the following values; all non-success values are treated as permanent failures: • 1001—DIAMETER MULTI ROUND AUTH • 2001—DIAMETER SUCCESS • 5002—DIAMETER UNKNOWN SESSION ID • 5012—DIAMETER UNABLE TO COMPLY JSRC also supports the following value, which is treated as a permanent failure: • 3004—DIAMETER TOO BUSY; this is a transient condition, typically when the router already has a request in process for a specified subscriber. Gx-Plus supports the following values for errors in a PCRF response; when these values are received or the response is malformed or unrecognizable, the request is retried. • 3001—DIAMETER COMMAND NOT SUPPORTED; the application is not running or the command is not recognized. • 3004—DIAMETER TOO BUSY; the received message is above either the quota of downstream transactions or the outstanding message memory limit for messages from the network. • 5012—DIAMETER UNABLE TO COMPLY; the received message is greater than the local limit.	Unsigned32

Table 4: Standard Diameter AVPs *(continued)*

Attribute Number	Diameter AVP	Application	Description	Type
277	Auth-Session-State	JSRC, PTSP	Indicates whether AAA session state is maintained. • 0—STATE MAINTAINED • 1—NO STATE MAINTAINED	Enumerated
295	Termination-Cause	JSRC, PTSP	Indicates the reason why a session was terminated on the access device. • 1—DIAMETER LOGOUT • 2—DIAMETER SERVICE NOT PROVIDED • 3—DIAMETER BAD ANSWER • 4—DIAMETER ADMINISTRATIVE • 5—DIAMETER LINK BROKEN • 6—DIAMETER AUTH EXPIRED • 7— DIAMETER USER MOVED • 8—DIAMETER SESSION TIMEOUT	Enumerated
415	CC-Request-Number	Gx-Plus	Identifies a request within a session. The combination of Session-Id and CC-Request-Type is globally unique. The number is incremented for each request during the course of a session. The number is reset when a router high availability event takes place.	Unsigned32
416	CC-Request-Type	Gx-Plus	Specifies the type of credit control request: • INITIAL REQUEST (1) • UPDATE REQUEST (2) • TERMINATION_REQUEST (3) • EVENT REQUEST (4)	Enumerated
431	Granted-Service-Unit	Gx-Plus	Contains the amount that can be provided of one or more of the following requested units specified by the client: CC-Input-Octets, CC-Output-Octets, CC-Time, or CC-Total-Octets. Included in CCA-I messages, and may be included in CCA-U messages.	Grouped
446	Used-Service-Unit	Gx-Plus	Contains the amount of the requested units that have been actually used; measured from 4 when the service is activated. The units are one or more of the following requested units specified by the client: CC-Input-Octets, CC-Output-Octets, CC-Time, or CC-Total-Octets. Included in CCR-U messages.	Grouped

Table 4: Standard Diameter AVPs *(continued)*

Attribute Number	Diameter AVP	Application	Description	Type
480	Accounting-Record-Type	JSRC, PTSP	Specifies the type of account record for service accounting: • INTERIM_RECORD—Accounting record sent between the start and stop records, at intervals specified by the Acct-Interim-Interval AVP (AVP code 85). It contains cumulative accounting data for the existing accounting session. • START_RECORD—Accounting record sent when the service is activated to initiate the accounting session. It contains accounting data relevant to the initiation of that session. • STOP_RECORD—Accounting record sent when the service is deactivated to terminate the accounting session. It contains cumulative data relevant to that session.	Enumerated
1001	Charging-Rule-Install	Gx-Plus	Requests the installation of the rule (activation of the service) designated by the included Charging-Rule-Name AVP (1005). This AVP has a vendor ID of 10415 (3GPP).	Grouped
1002	Charging-Rule-Remove	Gx-Plus	Requests the removal of the rule (deactivation of the service) designated by the included Charging-Rule-Name AVP (1005). This AVP has a vendor ID of 10415 (3GPP).	Grouped
1005	Charging-Rule-Name	Gx-Plus	Name of a specific rule that has been installed, modified, or removed.	OctetString
1066	Monitoring-Key	Gx-Plus	Specifies which of the monitoring structures to use. Included in Charging-Rule-Install AVP (1001). The MX router does not support aggregation of statistics across services, so the value of this AVP must be different for each service. This AVP has a vendor ID of 10415 (3GPP).	OctetString
1067	Usage-Monitoring-Information	Gx-Plus	Sets monitoring thresholds. When service statistics match at least one of the granted service values, the router sends a CCR-U report with the current statistics to the PCRF. Includes the Monitoring-Key AVP (1066) and the Granted-Service-Unit AVP (431). This AVP has a vendor ID of 10415 (3GPP).	Grouped

Juniper Networks AVPs are used in addition to the standard Diameter AVPs. These AVPs have an enterprise number of 2636. Table 5 on page 14 lists the Juniper Networks AVPs that the supported Diameter applications use.

Table 5: Juniper Networks Diameter AVPs

Attribute Number	Diameter AVP	Application	Description	Type
2004	Juniper-Service-Bundle	JSRC	Specifies the name of the service bundle.	OctetString
2010	Juniper-DHCP-Options	JSRC	Specifies the client's DHCP options.	OctetString
2011	Juniper-DHCP-GI-Address	JSRC	Specifies the DHCP relay agent's IP address.	OctetString
2020	Juniper-Policy-Install	JSRC, PTSP	Specifies policies to be activated for the subscriber. Includes Juniper-Policy-Name and Juniper-Policy-Definition	Grouped
2021	Juniper-Policy-Name	JSRC, PTSP	Defines the name of a policy decision.	OctetString
2022	Juniper-Policy-Definition	JSRC, PTSP	Defines a policy decision. Includes Juniper-Policy-Name, Juniper-Template-Name, and Juniper-Substitution.	Grouped
2023	Juniper-Template-Name	JSRC, PTSP	Profile name defined by the router. PTSP supports only the **__svc_rule__** policy template.	UTF8String
2024	Juniper-Substitution	JSRC, PTSP	Defines the substitution attributes. Includes Juniper-Substitution-Name and Juniper-Substitution-Value.	OctetString
2025	Juniper-Substitution-Name	JSRC, PTSP	Defines the name of the variable to be replaced.	OctetString
2026	Juniper-Substitution-Value	JSRC, PTSP	Defines the value of the variable to be replaced.	OctetString
2027	Juniper-Policy-Remove	JSRC, PTSP	Specifies policies to be deactivated for the subscriber. Includes Juniper-Policy-Name.	Grouped
2035	Juniper-Policy-Failed	JSRC, PTSP	Specifies the name of the policy activation or deactivation that failed.	OctetString
2038	Juniper-Policy-Success	JSRC, PTSP	Specifies the name of the policy activation or deactivation that succeeded.	OctetString
2046	Juniper-Logical-System	JSRC, PTSP	Specifies the logical system.	UTF8String
2047	Juniper-Routing-Instance	JSRC, PTSP	Specifies the routing instance.	UTF8String
2048	Juniper-Jsrc-Partition	JSRC, PTSP	Specifies the logical system and routing instance for the subscriber or request. Includes Juniper-Logical-System and Juniper-Routing-Instance	Grouped

Table 5: Juniper Networks Diameter AVPs *(continued)*

Attribute Number	Diameter AVP	Application	Description	Type
2050	Juniper-Request-Type	JSRC, PTSP	Describes the type of request: • 1—ADDRESS_AUTHORIZATION • 2—PROVISIONING_REQUEST • 3—SYNCHRONIZATION	Enumerated
2051	Juniper-Synchronization-Type	JSRC, PTSP	Describes the type of synchronization: • 1—FULL-SYNC • 2—FAST-SYNC • 3—NO-STATE-TO-SYNC	Enumerated
2052	Juniper-Synchronization	JSRC, PTSP	Describes the state of synchronization: • 1—NO-SYNC; this is the default state • 2—SYNC-IN-PROGRESS • 3—SYNC-COMPLETE	Enumerated
2053	Juniper-Acct-Record	JSRC, PTSP	Statistics data for each policy installed for this subscriber. Includes Juniper-Policy-Name.	Grouped
2054	Juniper-Acct-Collect	JSRC, PTSP	Specifies whether to collect accounting data for the installed policy (service) when included in the Juniper-Policy-Install AVP: • 1—COLLECT_ACCT • 2—NOT_COLLECT_ACCT	Enumerated
2058	Juniper-State-ID	JSRC, PTSP	Specifies the value assigned to each synchronization cycle for the purpose of identifying which messages to discard. All solicited requests containing the same **Juniper-State-ID** belong to the same Session-Resource-Query (SRQ) synchronization cycle. Messages from a previous synchronization cycle are discarded. When a new cycle begins, the value of the **Juniper-State-ID** AVP is increased by 1. NOTE: For solicited synchronization requests, the SRQ message contains the incremented **Juniper-State-ID** value. For unsolicited synchronization requests, the Session-Resource-Reply (SRR) message contains the incremented **Juniper-State-ID** value.	Unsigned32
2100	Juniper-Virtual-Router	Gx-Plus, JSRC	Specifies the name of the virtual router associated with the session.	UTF8String

Table 5: Juniper Networks Diameter AVPs *(continued)*

Attribute Number	Diameter AVP	Application	Description	Type
2101	Juniper-Provisioning-Source	Gx-Plus	Specifies the provisioning source for the session in CCR-N and JSDA messages: • 1—Local • 2—Remote	Enumerated
2102	Juniper-Provisioning-Descriptor	Gx-Plus	Defines the group used in JSDA messages that includes the session ID, and optionally Juniper-Provisioning-Source and subscriber data.	Grouped
2103	Juniper-Event-Type	Gx-Plus	Communicates the event type in JSER messages: • 1–Cold boot; all sessions are lost • 2—Warm boot; sessions are preserved • 3—Discovery requested by the operator • 4—*Are you there?* (AYT); application level ping sent when the notification is due to no response or an erroneous response from the PCRF, or due to a configuration change. • 5—AWD; application-level watchdog sent by the router when there has been no other activity for 15 seconds. The watchdog is sent every 5 seconds unless preempted by higher-priority synchronization event.	Enumerated
2104	Juniper-Discovery-Descriptor	Gx-Plus	Defines the group used in JSDR and JSDA messages that includes parameters of a discovery request: discovery type, request string, verbosity, max results.	Grouped
2105	Juniper-Discovery-Type	Gx-Plus	Specifies the discovery subcommand for JSDR and JSDA messages: • 1—Exact: look up the data for the specified session. • 2—Bulk: Provide get-bulk kinds of information after the specified string. • 3—Done: Stop retries for all sessions up to the specified session.	Enumerated

Table 5: Juniper Networks Diameter AVPs *(continued)*

Attribute Number	Diameter AVP	Application	Description	Type
2106	Juniper-Verbosity-Level	Gx-Plus	Specifies the verbosity level for JSDR and JSDA messages: • 1—Summary; include only the Session-Id AVP. • 2—Brief; include the Session-Id, Juniper-Virtual-Router, and Framed-IP-Address AVPs. • 3—Detail; include the Session-Id, Juniper-Provisioning-Source, Juniper-Virtual-Router, Framed-IP-Address, and Event-Timestamp AVPs. 4—Extensive; include all available session information.	Enumerated
2107	Juniper-String-A	Gx-Plus	Specifies a generic string that is interpreted according to the context.	UTF8String
2108	Juniper-String-B	Gx-Plus	Specifies a generic string that is interpreted according to the context.	UTF8String
2109	Juniper-String-C	Gx-Plus	Specifies a generic string that is interpreted according to the context.	UTF8String
2110	Juniper-Unsigned32-A	Gx-Plus	Specifies a generic, unsigned 32-bit integer that is interpreted according to the context.	Unsigned32
2111	Juniper-Unsigned32-B	Gx-Plus	Specifies a generic, unsigned 32-bit integer that is interpreted according to the context.	Unsigned32
2112	Juniper-Unsigned32-C	Gx-Plus	Specifies a generic, unsigned 32-bit integer that is interpreted according to the context.	Unsigned32

Tekelec AVPs are used only for Gx-Plus. These AVPs have an enterprise number of 21274. Table 6 on page 17 lists the Tekelec AVPs. These four variables are used to provide substitution values for user-defined CoS service variables.

Table 6: Tekelec Diameter AVPs

Attribute Number	Diameter AVP	Application	Description	Type
5555	Tekelec-Charging-Rule-Argument-Name	Gx-Plus	Defines the name of the service variable to be replaced.	OctetString
5556	Tekelec-Charging-Rule-Argument-Value	Gx-Plus	Defines the value of the service variable to be replaced.	OctetString

Table 6: Tekelec Diameter AVPs *(continued)*

Attribute Number	Diameter AVP	Application	Description	Type
5557	Tekelec-Charging-Rule-Argument	Gx-Plus	Defines the substitution attributes used to replace service variables. Includes Tekelec-Charging-Rule-Argument-Name AVP (5555) and Tekelec-Charging-Rule-Argument-Value AVP (5556).	Grouped
5558	Tekelec-Charging-Rule-With-Arguments	Gx-Plus	Requests the installation of the rule (activation of the service) designated by the included Charging-Rule-Name AVP (1005). Requested service variable substitutions are provided by the optionally included Tekelec-Charging-Rule-Argument AVP (5557).	Grouped

Related Documentation

- *Understanding JSRC-SAE Interactions*
- Understanding PTSP-SAE Interactions on page 19
- *Understanding Gx-Plus Interactions Between the Router and the PCRF*
- *Diameter Base Protocol Overview*
- *Juniper Networks Session and Resource Control (SRC) and JSRC Overview*
- Juniper Networks Session and Resource Control (SRC) and PTSP Overview on page 4
- *Gx-Plus for Provisioning Subscribers Overview*

Understanding PTSP-SAE Interactions

This topic describes the sequences of Diameter messages exchanged between PTSP and the SAE as they interact to perform the following tasks for subscriber access:

- Subscriber login

  When a packet-triggered subscriber logs in, PTSP sends a Diameter AA-Request message to request service provisioning from the SAE that includes the Session-Id attribute for the new subscriber. If the AA-Request fails, then the subscriber is not considered logged in and the subscriber session is not managed by the SAE. Only the static PTSP rules apply to the subscriber.

  The SAE returns a Diameter AA-Answer message with the Result-Code. The AA-Answer message can include the Juniper-Policy-Install AVP (AVP code 2020), which is used to specify a service to attach to the subscriber's IP address.

  PTSP can send an AA-Request message to the SAE to confirm activation. The SAE returns a AA-Answer message in acknowledgment. If the AA-Request message fails or the SAE does not respond with an AA-Answer message, the subscriber session is managed by the SAE.

- Service activation and deactivation

  The SAE policies provision subscriber services. After a packet-triggered subscriber is logged in, the SAE can send a PPR message to PTSP to activate or deactivate services. A given PPR can include the Juniper-Policy-Install AVP (AVP code 2020) to activate a service or the Juniper-Policy-Remove AVP (AVP code 2027) to deactivate a service.

  PTSP sends a PPA message to the SAE when it has completed the tasks requested in the PPR. The PPA indicates the success or failure of the actions requested in the PPR.

- Resynchronization

  Either PTSP or the SAE initiates the resynchronization.

  The SAE initiates resynchronization at startup or when a backup SAE takes over session control due to resource limits or conditions on the primary SAE. The SAE clears its database of all entries in preparation for the synchronization.

  PTSP initiates resynchronization at startup, such as when AAA starts or restarts. PTSP uses the Juniper-Last-Origin-Host AVP (AVP code 2055) to keep track of the active SAE host in a multi-SAE environment. When an SAE in a multi-SAE environment becomes active, it must send an SRQ to PTSP as its first message. PTSP initiates a synchronization when it receives any other message type from an SAE that is different from the SAE indicated in the Juniper-Last-Origin-Host AVP.

  Both entities initiate a resynchronization by sending an SRQ message. The recipient responds with an SRR message.

- Statistics collection and reporting per service rule

  Statistics information can be sent from the router to the SAE or from the SAE to the router. Both the Diameter Accounting-Request and Accounting-Answer messages

include the Juniper-Acct-Record AVP (AVP code 2053) which identifies the policy for which accounting information is requested.

- Subscriber logout

  PTSP can determine when there is a logout request for a packet-triggered subscriber in two ways:

  - The SAE terminates a subscriber session by sending an ASR message to PTSP.
  - PTSP monitors a subscriber session and starts the logout process after 30 minutes of inactivity.

  The subscriber logout triggers the final statistics aggregation for all policies and the removal of any policies installed by the SAE. PTSP sends an STR message that indicates the logout event to the SAE.

Related Documentation

- Juniper Networks Session and Resource Control (SRC) and PTSP Overview on page 4
- Messages Used by Diameter Applications on page 5
- Diameter AVPs and Diameter Applications on page 10
- Configuring the PTSP Application on page 29
- Configuring PTSP on page 29

Packet-Triggered Subscribers Services Overview

The packet-triggered subscribers and policy control (PTSP) feature allows the application of policies to dynamic subscribers that are controlled by a subscriber termination device. You can associate specific subscriber contexts based on IPv4 addresses and provide dynamic service activation and deactivation for these subscribers. Once the subscribers are present in the subscriber database on the router, PSTP can report the subscribers to the SAE using the PTSP application so that the SRC software can manage the subscribers and services.

PTSP policies can be downloaded dynamically from the external policy manager (such as SRC) or configured statically on the router. The PTSP policies can be configured for each distinct IPv4 source address for a given interface on which the service is configured. Each distinct IPv4 address is considered a subscriber and all PTSP policies are applied on a per-subscriber basis. Dynamic policies, which are always specific to a subscriber, take precedence over static policies.

You can set up PTSP policies to:

- Manage traffic by configuring filtering, rate-limiting, and QoS enforcement in the rules.
- Steer traffic by specifying the forwarding instance in the forward rule.
- Collect accounting information by service rule or by application.

When you configure PTSP policies, you must specify the type of statistics collection (**count**) and the IP address used to identify the packet-triggered subscriber (**demux**) in

the service rule. All service rules attached to a given service set must have the same settings for these options.

For the statistics collection type, terms and rules also cannot mix and match the following styles:

- rule—Statistics are aggregated in one bucket for the service rule and Diameter is used to report the statistics.
- application—Statistics are aggregated by application for a specific application, for a specific application group, or in one bucket. The statistics are reported in a flat file.

Subscriber instantiation is triggered for ingress packets by the IP address. When source address is specified, the source IP address of the ingress packets is used to establish the subscriber context. When destination address is specified, the destination IP address of the ingress packets is used to establish the subscriber context. If the IP address does not correspond to a known subscriber, then a new subscriber context is created to log in the packet-triggered subscriber.

The match conditions include local address, local port, remote address, and remote port. The following table describes how the **demux** value changes the IP address or port used for these terms.

Match Conditions	demux source-address		demux destination-address	
	Ingress Flows	Egress Flows	Ingress Flows	Egress Flows
local-address	Source address	Destination address	Destination address	Source address
remote-address	Destination address	Source address	Source address	Destination address
local-port	Source port	Destination port	Destination port	Source port
remote-port	Destination port	Source port	Source port	Destination port

Subscriber Identification Method for PTSP Partition

The PSTP functionality uses RADIUS attributes, such as *User-Name* to identify subscribers in a RADIUS partition. If a service provider uses a different RADIUS attribute other than User-Name, the authentication of subscribers and establishment of client sessions fail. To enable service providers to use a subscriber-identification method that suits their network needs, you can add flexible configurations in the packet-triggered subscriber process.

The PTSP configurable user-identification feature allows you to do the following:

- Configure the subscriber identification method for PTSP partitions, based on the network topology and the service provider requirements.
- Insert subscriber-specific tags for the subscriber's HTTP traffic for which the reference to subscriber-specific tagging is provided using subscriber identification.

The PTSP application generates the subscriber-identification parameter as a text-string by combining the RADIUS attribute value and the internal attribute value of the PTSP partition. The text-string is generated in the same order as the attributes that are configured in the PTSP partition.

NOTE: Only RADIUS partitions support user-identification to configure the subscriber-identification method for PTSP partitions.

PTSP Services on Aggregated and Redundant Services PICs

The packet-triggered subscribers and policy control (PTSP) feature supports both Aggregated Multiservices (AMS) and Redundant Multiservices (RMS) PICs. RMS services interfaces support 1:1 redundancy between two logical PICs and in an active or standby model. AMS services interfaces support load sharing and N:1 redundancy between N logical PICs.

NOTE: The PTSP services do not support load balancing on AMS.

In 1:1 redundancy, if services PIC fails:

- The subscriber is logged out, the traffic is switched to the redundant services PIC, and the subscriber receives a new session ID to log in with.
- The subscriber's last configured accounting data is retrieved as the latest interim accounting record.

In AMS, the PTSP subscriber's traffic is redistributed to other services PIC and the same subscriber may appear on different services PICs. The subscriber with no new data flow is logged out after idle timeout with the complete accounting data. The following example depicts the AMS scenario:

```
ams0 {
  load-balancing-options {
    member-interface mams-4/0/0;
    member-interface mams-4/1/0;
    member-interface mams-5/0/0;
    member-failure-options {
      redistribute-all-traffic;
    }
  }
  unit 1 {
    family inet;
  }
}
```

The traffic on ms-4/0/0 is redistributed to ms-4/1/0 only after ms-5/0/0 has failed. In this example, there are two subscribers: s1 on ms-4/0/0 and s2 on ms-4/1/0. The two subscribers have the same source IP address. If there is no new traffic, s1 is eventually logged out after idle timeout.

NOTE: PTSP does not support any type of hash key for traffic sharing among logical PICs configured with the same PTSP service set. For PTSP to work, all traffic for any given subscriber needs to reach the same logical PIC within an AMS container. For this to happen, the AMS hashing algorithm needs to align with the PTSP demux type, as follows:

- If PTSP is configured for source-demux, then the AMS hashing algorithm must be based on the source-ip-address only.
- If PTSP is configured for destination-demux, then the AMS hashing algorithm must be based on the destination-ip-address only.
- No other type of AMS hashing algorithm is compatible with PTSP.

NOTE: The packet level idle timeout for every packet is assigned from a given subscriber transiting the router. If the timeout limit sets in, the subscriber is logged out. The valid range for the subscriber packet idle timeout is 15 to 1440 minutes.

Related Documentation

- Configuring PTSP on page 29
- Configuring Static PTSP Rules on page 35

Understanding the Subscriber Profiles for Client Sessions per PSTP Partition

Subscriber profiles for service activation enables you to specify which service plug-ins become activated on a per-subscriber basis. Previously, the only control mechanism for specifying service activation was to attach a service-set configuration to a selected interface or route. The new utility allows you to enable or disable services based on the subscriber associated with every data flow. As a result, you can apply differentiated services to different sets of subscribers. You can exercise the control mechanism in one of two ways: by using a CLI operational command or a RADIUS attribute.

NOTE: This feature applies only to MP-SDK services and does not depend on the specific services enabled or disabled, except that PTSP must be included in the chain.

The procedure consists of three steps:

1. Configure a service set that includes all the services to be applied to flows. You can include a default subscriber profile that controls which services are and are not active by default. The default profile applies to all subscribers until overridden for a specific subscriber. In the absence of a default subscriber profile, all services specified in the service set are applied by default. You can also include one or more alternative

subscriber profiles that can be implemented to override the default profile. The following sample configuration illustrates these components:

```
services {
  service-set ss1 {
    application-identification-profile appidr1;
    idp-profile idpr1;
    aacl-rules aaclr1;
    hcm_rules hcmr1;
    sfw_rules sfwr1;
    subscriber-profile {
      sp1;
    }
    interface-service {
      service-interface ms-3/0/0.0;
    }
  }
  }
  subscriber-profile sp1 {
    disable HCM;
    enable IDP {
      concurrent-data-sessions 10;
    }
    disable AACL;
    max-data-sessions-per-subscriber {
      limit 10;
      exceed-action [ syslog drop ];
    }
  }
  subscriber-profile sp2 {
    enable HCM;
    disable IDP;
    enable AACL,
    max-data-sessions-per-subscriber {
      limit 100;
      exceed-action [ syslog ];
    }
  }
```

Initially, all traffic reaching the service plane under service set ss1 receives all the services configured in service set ss1 that are enabled by the default subscriber profile sp1 applied to it. In the example, APPID, stateful firewall, and IDP are enabled, whereas HCM and AACL are disabled. However IDP is enabled for only at most 10 sessions concurrently. Beyond that threshold, IDP is also disabled. Also, because of the max-data-sessions-per-subscriber setting, any subscriber is allowed a maximum of ten concurrent data sessions. Beyond that threshold, data sessions are logged and dropped.

2. There are two ways to dynamically override the default subscriber profile associated with a particular PTSP subscriber:

   - CLI operational command
   - RADIUS attribute or VSA in an access-accept message.

From the previous example, assume that the subscriber profile for subscriber X is dynamically set to sp2. After that, any new data session associated with subscriber X has a different set of services applied to it. In the example, it would be APPID, stateful firewall, HCM, and AACL. Also, because the max-data-sessions-per-subscriber setting changes to 100, subscriber X now has no upper limit on the number of concurrent data sessions, although if that number crosses the 100 threshold, the threshold-crossing event is logged.

The following examples illustrate the dynamic override settings:

Operational command

```
user@router>request services subscriber clear subscriber-profile
client-id client-id
```

```
user@router>request services subscriber set subscriber-profile
subscriber-profile-name client-id client-id
```

RADIUS configuration

```
user@router# set system services packet-triggered-subscribers
partition-radius foo subscriber-service-profile attribute-26.4874.31
```

3. Processing of a new data session at the service plane takes place as follows, with respect to subscriber profiles:
   1. A new flow starts. MP-SDK sends a SESSION-INTEREST event to the service plug-ins. The first plug-in in the chain is the subscribers (PTSP) plug-in.
   2. The subscribers plug-in matches the flow to its subscriber by searching its database. It sets the subscriber ID in the session metadata.
   3. The subscriber plug-in checks for the corresponding subscriber profile and which services are enabled. It then sets the services mask of enabled and disabled services in the session metadata.
   4. MP-SDK or JSF invokes only the services that are enabled per the services mask. The other services are skipped, even if configured in the service set.

NOTE: : Subscriber-profile changes affect only the upcoming flows. Existing flows remain unaffected.

PART 2

Configuration

CHAPTER 2

Configuration Overview

Configuring the PTSP Application

You can configure the PTSP client application to work with the Session and Resource Control (SRC) peer to centrally manage packet-triggered subscribers and services. PTSP requests address and service authorizations from the remote SRC peer (the SAE), activates and deactivates services as specified by the SAE, logs out subscribers as specified by the SAE, and synchronizes subscriber state and service information with the SAE. The PTSP application also performs statistics collection and reporting.

To configure the PTSP application:

1. Configure the PTSP partition.

   See "Configuring the PTSP Partition" on page 31.

2. Assign the PTSP partition.

   See "Assigning the PTSP Partition" on page 32.

3. Configure statistics collection and reporting.

   See "Tracing Packet-Triggered Subscriber Operations" on page 93.

Related Documentation

- Juniper Networks Session and Resource Control (SRC) and PTSP Overview on page 4

Configuring PTSP

You can configure the packet-triggered subscribers and policy control (PTSP) feature on MX Series routers to allow the application of policies to dynamic subscribers that are controlled by a subscriber termination device, such as a B-RAS or GGSN device, connected to an MX Series router. The subscribers are associated by their IPv4 address and dynamic or static policies can be applied. Dynamic policies take precedence over static policies. When you download a new dynamic policy, it takes effect only for new flows. All new flows and TCP connections use the new dynamic policy. Existing flows are not affected by the new policy unless they timeout, after which they are considered a new flow.

To configure PTSP services on the MX Series router:

1. Configure the Multiservices DPC.

   See "Configuring the Multiservices DPC for PTSP" on page 33.

2. Configure the Diameter application to support the download of dynamic PTSP policies from the external policy manager (such as SRC). The PTSP application also provides statistics collection and reporting.

   See "Configuring the PTSP Application" on page 29.

3. Configure the static PTSP service rules.

   See "Configuring Static PTSP Rules" on page 35.

4. Configure statistics collection and reporting in a flat file.

   See "Configuring a Statistics Profile for PTSP" on page 95 and "Tracing PTSP Operations" on page 97.

Related Documentation

- PTSP Overview on page 3

CHAPTER 3

Configuration Tasks for the PTSP Application

Configuring the PTSP Partition

PTSP works within a specific logical system:routing instance context, called a partition. The partition is configured to connect to the external policy manager.

NOTE: Currently, only a single partition is supported; you must configure it within the default logical system:routing instance context.

Before you configure the PTSP partition to connect to the external policy manager, perform the following task:

- Configure the Diameter instance for the remote SRC peer at the **[edit diameter]** hierarchy level. See *Configuring Diameter*.

Configuration for the PTSP partition consists of naming the partition and then associating a Diameter instance, the SAE hostname, and the SAE realm with the partition.

To configure the PTSP partition:

1. Create the partition at the **[edit system services packet-triggered-subscribers]** hierarchy level.

   ```
   [edit system services packet-triggered-subscribers]
   user@host# edit partition ptsp–default
   ```

2. Specify the Diameter instance for the PTSP partition.

   ```
   [edit system services packet-triggered-subscribers partition ptsp–default]
   user@host# set diameter-instance master
   ```

3. Configure the destination host for the PTSP partition.

   ```
   [edit system services packet-triggered-subscribers partition ptsp–default]
   user@host# set destination-host sae1
   ```

4. Configure the destination realm for the PTSP partition.

   ```
   [edit system services packet-triggered-subscribers partition ptsp–default]
   user@host# set destination-realm generic.example.com
   ```

5. Configure the subscriber ID for the PTSP partition.

   ```
   [edit system services packet-triggered-subscribers partition-radius
     radius-partition-name]
   user@host# set subscriber-identification
   ```

Related Documentation

- Configuring the PTSP Application on page 29

Assigning the PTSP Partition

You must associate the PTSP partition with the logical system:routing instance.

NOTE: Currently, only the global logical system:routing instance, *master* logical system and default routing instance, is supported.

Before you assign the PTSP partition, perform the following task:

- Configure the PTSP partition. See "Configuring the PTSP Partition" on page 31.

To assign the PTSP partition:

- Specify the partition name at the **[edit system]** hierarchy level.

  ```
  [edit system]
  user@host# set packet-triggered-subscribers-partition ptsp–default
  ```

Related Documentation

- Configuring the PTSP Application on page 29

CHAPTER 4

Configuration Tasks for PTSP

Configuring the Multiservices DPC for PTSP

To configure the Multiservices Dense Port Concentrator (MS-DPC) to support PTSP services, perform the following tasks:

Enabling the PTSP Service Package on the Multiservices DPC

The PTSP feature runs on the Multiservices DPC, you must enable the PTSP service package on the Multiservices DPC before you can configure the PTSP software. The name of the PTSP service package is **jservices-ptsp**.

To enable the PTSP service package:

1. Determine the FPC slot number and the PIC number of the MS-DPC on which you want to enable the PTSP service package.

   ```
   user@host> show chassis hardware
   ```

   In this example, the FPC slot number is 3 and the PIC number is 0.

2. Enable the jservices-ptsp package on the Multiservices DPC.

   ```
   [edit chassis]
   user@host# set fpc 3 pic 0 adaptive-services service-package extension-provider
     package jservices-ptsp
   ```

Configuring Services Interface for PTSP

NOTE: ams- interfaces and rms- interfaces can be configured for PTSP.

To configure the services interface for PTSP:

1. Enter edit mode for the interface.

   ```
   [edit]
   user@host# edit interfaces ms-3/0/0
   ```

2. Configure a logical unit and specify the protocol family.

   ```
   [edit interfaces ms-3/0/0]
   user@host# set unit 0 family inet
   ```

Related Documentation

- Configuring PTSP on page 29
- PTSP Overview on page 3

Configuring PTSP Service Rules

PTSP policies can be downloaded dynamically from the external policy manager (such as SRC) or configured statically on the router. The PTSP policies can be configured for each distinct IPv4 source address for a given interface on which the service is configured. Each distinct IPv4 address is considered a subscriber and all PTSP policies are applied on a per-subscriber basis.

Dynamic policies, which are always specific to a subscriber, take precedence over static policies. When you download a new dynamic policy, it takes effect only for new flows. All new flows and TCP connections use the new dynamic policy. Existing flows are not affected by the new policy unless they timeout, after which they are considered a new flow.

To configure the PTSP policies, perform these tasks:

- To download dynamic policies and to collect statistics with Diameter, configure the Diameter application for PTSP. See "Configuring the PTSP Application" on page 29.
- To configure static policies, see "Configuring Static PTSP Rules" on page 35. To collect statistics in a flat file, see "Configuring a Statistics Profile for PTSP" on page 95.

Related Documentation

- Configuring PTSP on page 29
- PTSP Overview on page 3

Configuring Static PTSP Rules

You can configure the static PTSP policies on the router. If the PTSP service is configured on the underlying interface, the PTSP service enforces the policies associated with the subscriber context.

To configure static PTSP rules:

1. Specify the rule that you want to configure.

   ```
   [edit services ptsp]
   user@host# edit rule ptspRule1
   ```

2. Specify the direction in which the rule match is applied.

   ```
   [edit services ptsp rule ptspRule1]
   user@host# set match-direction input
   ```

3. Specify the IP address used for the subscriber context. Subscriber instantiation is always triggered for ingress packets, so this value indicates which IP address in the ingress packets for the flow is used.

   ```
   [edit services ptsp rule ptspRule1]
   user@host# set demux source-address
   ```

4. Specify the statistics aggregation, collection, and reporting style. Terms and rules cannot mix and match different styles.

   ```
   [edit services ptsp rule ptspRule1]
   user@host# set count-type rule
   ```

   If you specify the rule style, statistics collection is performed by the Diameter application. If you specify the application style, statistics collection is in a flat file controlled by the local policy decision function (L-PDF).

5. (Optional) Specify the forward rule used for forwarding packets. See "Configuring the PTSP Forwarding Instance" on page 38.

   ```
   [edit services ptsp rule ptspRule1]
   user@host# set forward-rule forward-rule-name
   ```

6. Configure the term precedence for the rule.

   ```
   [edit services ptsp rule ptspRule1]
   user@host# edit term 1
   ```

7. Configure the match conditions for the term. See Table 7 on page 36.

   ```
   [edit services ptsp rule ptspRule1 term 1]
   user@host# set from remote-address-range low 203.0.0.2 high 203.0.0.100
   user@host# set from remote-address-range low 204.0.0.2 high 204.0.0.253
   ```

8. (Optional) Specify the action taken when the match conditions are met. See Table 8 on page 36.

   ```
   [edit services ptsp rule ptspRule1 term 1]
   user@host# set then count rule
   user@host# set then accept
   ```

Table 7 on page 36 describes the match conditions for PTSP rules.

Table 7: PTSP Match Conditions

Match Condition	Description
application-group-any	Application group name defined in the application identification configuration.
application-groups [*application-group-name*]	Application group name defined in the application identification configuration.
applications	Application name defined in the application identification configuration.
local-port-range low *low-value* **high** *high-value*	Local port range.
local-ports *value-list*	Local ports.
protocol *protocol-number*	IP protocol number.
remote-address (*address* **| any-unicast)**	Remote IP address. IPv4 only.
remote-address-range low *low-value* **high** *low-value*	Remote address range. IPv4 only.
remote-port-range low *low-value* **high** *high-value*	Remote port range.
remote-ports *value-list*	Remote ports.
remote-prefix-list *prefix-list-name*	Prefixes in the specified list.

Table 8 on page 36 describes the actions for PTSP rules.

Table 8: PTSP Actions

Action or Action Modifier	Description
accept	Accept the packet.
count	Increment the specified counter.
discard	Drop the packet.
forwarding-class	Classify the packet into the specified forwarding class.
police	Rate-limit packets based on the specified policer.

Related Documentation

- Configuring the PTSP Forwarding Instance on page 38
- Configuring a Statistics Profile for PTSP on page 95

- Configuring PTSP on page 29
- PTSP Overview on page 3
- Packet-Triggered Subscribers Services Overview on page 20

Configuring PTSP Rule Sets

You can define a collection of PTSP rules to determine the actions performed on packets.

To configure static PTSP rule sets:

1. Specify the rule set that you want to configure.

   ```
   [edit services ptsp]
   user@host# edit rule-set ptspRules
   ```

2. Specify the rules in the order that you want them processed.

   ```
   [edit services ptsp rule-set ptspRules]
   user@host# set rule ptspRule1
   user@host# set rule ptspRule2
   ```

Related Documentation

- Configuring Static PTSP Rules on page 35

Configuring PTSP Service Sets

To configure the service set for the PTSP application:

1. Configure the service set that you want to contain the PTSP service.

   ```
   [edit services service-set ptspServiceSet]
   user@host# set service-set ptspServiceSet
   ```

2. Specify the PTSP rules that constitute the service set that is applied to the services interface.

   ```
   [edit services service-set ptspServiceSet]
   user@host# set ptsp-rules ptsp-rule1
   user@host# set ptsp-rules ptsp-rule2
   ```

3. Configure the services interface.

   NOTE: ams- interfaces and rms- interfaces are supported for PTSP.

   ```
   [edit services service-set ptspServiceSet]
   user@host# set interface-service service-interface ms-3/0/0.0
   ```

4. Associate the service set with the underlying interface from which the subscribers originate. The service set must be applied to the interface facing the subscriber, that is, the interface with the IP address of the subscriber.

   ```
   [edit interfaces ge-4/0/0 unit 0 family inet service]
   user@host# set input service-set ptspServiceSet
   ```

```
user@host# set output service-set ptspServiceSet
```

Related Documentation

- Configuring Static PTSP Rules on page 35
- Configuring PTSP Rule Sets on page 37

Configuring the PTSP Forwarding Instance

Before you can forward PTSP traffic, perform these tasks for each forwarding instance:

1. Configure each PTSP forwarding instance as a routing instance type of forwarding.
2. Configure a firewall filter with an action that specifies the routing instance configured in Step 1.
3. Configure the unit number for the Multiservices interface that specifies the filter configured in Step 2 as the input filter.

   NOTE: To avoid service set dependency on specific unit numbers, use the same unit number across all Multiservices interfaces where PTSP services are applied.

4. Configure the PTSP forward rule to specify the forwarding instance.

   NOTE: When the forwarding instance action is performed on the flow, any postservice filters are not applied to the underlying interface.

If you want to forward traffic for PTSP subscribers, you must specify the forwarding instance for specific subscribers based on IP address, network, or prefix list. The match direction for forward rules is always input.

To configure the PTSP forwarding instance:

1. Specify the PTSP forward rule that you want to use when configuring a PTSP forwarding instance.

   ```
   [edit services ptsp]
   user@host# edit forward-rule ptspForward
   ```

2. Set the term precedence for the forward rule. Term with lowest precedence is evaluated first.

   ```
   [edit services ptsp forward-rule ptspForward]
   user@host# edit term 5
   ```

3. Configure the match conditions for the IP address, address range, or prefix list. See Table 9 on page 39.

   ```
   [edit services ptsp forward-rule ptspForward term 5]
   user@host# set from local-address 200.0.0.1
   ```

Table 9: PTSP Forward Rule Match Conditions

Match Condition	Description
application-groups [*application-group-name*]	Application group name defined in the application identification configuration.
applications	Application name defined in the application identification configuration.
local-address (*address* | **any-unicast**)	Local IP address. IPv4 only.
local-address-range low *low-value* **high** *high-value*	Local address range. IPv4 only.
local-prefix-list *prefix-list-name*	Prefixes in the specified list.

NOTE: You can specify match conditions for applications or application groups that support application identification (APPID) services, but we do not recommend specifying the forwarding instance action when you are using these match conditions in PTSP policies. In this situation, some network topologies may route packets in a manner that causes the flow to be dropped. For example, the APPID services might forward some packets on the default routing instance while the PTSP services forward other packets in the same flow to another routing instance.

4. Configure the forwarding instance action with the routing instance name and the unit number.

```
[edit services ptsp forward-rule ptspForward term 5]
user@host# set then forwarding-instance less-effort-ri 144
```

NOTE: When the forwarding instance action is performed on the flow, any postservice filters are not applied to the underlying interface.

Related Documentation

- *APPID Overview*
- *Routing Instances Overview*

CHAPTER 5

Configuration Statements

[edit system services packet-triggered-subscribers] Hierarchy Level

```
system {
  services {
    packet-triggered-subscribers {
      subscriber-packet-idle-timeout subscriber-packet-idle-timeout
      partition partition-name {
        destination-host hostname;
        destination-realm realm;
        diameter-instance instance-name;
      }
      traceoptions {
        file filename <files number> <match regular-expression> <size maximum-file-size>
          <world-readable | no-world-readable>;
        flag flag;
        no-remote-trace;
      }
    }
  }
}
```

Related Documentation

- Configuring the PTSP Application on page 29

application-group-any

Syntax application-group-any;

Hierarchy Level [edit services ptsp rule *rule-name* term *precedence* from]

Release Information Statement introduced in Junos OS Release 10.2.

Description Specify that any application group defined in the database is considered a match.

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

Related Documentation
- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

application-groups

Syntax application-group [*application-group-name*];

Hierarchy Level [edit services ptsp forward-rule *forward-rule-name* term *precedence* from]
[edit services ptsp rule *rule-name* term *precedence* from]

Release Information Statement introduced in Junos OS Release 10.2.

Description Identify one or more application groups defined in the application identification configuration for inclusion as a match condition.

Options ***application-group-name***—Identifier of the application group.

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

Related Documentation
- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

applications (Services PTSP)

Syntax applications [*application-name*];

Hierarchy Level [edit services ptsp forward-rule *forward-rule-name* term *precedence* from]
[edit services ptsp rule *rule-name* term *precedence* from]

Release Information Statement introduced in Junos OS Release 10.2.

Description Identify one or more applications defined in the application identification configuration for inclusion as a match condition.

Options ***application-name***—Identifier of the application.

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

Related Documentation
- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

concurrent-data-sessions

Syntax concurrent-data-sessions *max-session-number*;

Hierarchy Level [edit services service-set *services-set-name* subscriber-profile *profile-name* enable *service-name*]

Release Information Statement introduced in Junos OS Release 11.4.

Description Specify the maximum number of sessions that are concurrently enabled for the named service. The system randomly selects the number of sessions and enables the named service, whereas other sessions are not allotted the named service. This facilitates to increase the limit on the number of resources a service can use.

Options ***max-session-number***—Maximum number of sessions concurrently enabled for the named service.

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

count-type

Syntax count-type (application | rule);

Hierarchy Level [edit services ptsp rule *rule-name*]

Release Information Statement introduced in Junos OS Release 10.2.

Description Specify the statistics aggregation, collection, and reporting style for this rule. Terms and rules cannot mix and match different styles. All service rules attached to a given service set must have the same style.

Options

application—Report statistics in a flat file and aggregate them by application for one of the following:

- An application, where the count action **application** is specified in the term.
- An application group, where the count action **application-group** is specified in the term.
- All application groups, where the count action **application-group-any** is specified in the term.

rule—Aggregate statistics for the service rule. The statistics are reported by Diameter. All count actions in all terms for the rule must specify **rule**.

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

Related Documentation

- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

demux

Syntax demux (destination-address | source-address);

Hierarchy Level [edit services ptsp rule *rule-name*]

Release Information Statement introduced in Junos OS Release 10.2.

Description Specify the IP address used to establish the subscriber context. Subscriber instantiation is always triggered for ingress packets, so this value indicates which IP address in the ingress packets for the flow is used. If the IP address does not correspond to a known subscriber, then a new subscriber context is created. All service rules attached to a given service set must have the same setting.

Options **destination-address**—Use the destination IP address field of the ingress packet header for the flow.

source-address—Use the source IP address field of the ingress packet header for the flow.

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

Related Documentation
- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

destination-host (PTSP)

Syntax destination-host *hostname*;

Hierarchy Level [edit system services packet-triggered-subscribers partition *partition-name*]

Release Information Statement introduced in Junos OS Release 10.2.

Description Configure the host on which the SAE application resides.

Options ***hostname***—Host on which the SAE is installed.

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

Related Documentation
- Configuring the PTSP Partition on page 31

destination-realm (PTSP)

Syntax destination-realm *realm*

Hierarchy Level [edit system services packet-triggered-subscribers partition *partition-name*]

Release Information Statement introduced in Junos OS Release 10.2.

Description Configure the realm in which the SAE host resides.

Options ***realm***—Realm in which the SAE host resides.

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

Related Documentation
- Configuring the PTSP Partition on page 31

diameter-instance (PTSP)

Syntax diameter-instance *instance-name*

Hierarchy Level [edit system services packet-triggered-subscribers partition *partition-name*]

Release Information Statement introduced in Junos OS Release 10.2.

Description Specify the Diameter instance associated with the PTSP partition.

Options ***instance-name***—Name of the Diameter instance. Currently, only **master** is supported.

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

Related Documentation
- Configuring the PTSP Partition on page 31

disable

Syntax disable *service-name*;

Hierarchy Level [edit services service-set *services-set-name* subscriber-profile *profile-name*]

Release Information Statement introduced in Junos OS Release 11.4.

Description Disable the service name of the subscriber profile.

Options ***service-name***—Name of the disabled service.

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

enable

Syntax

```
enable service-name {
  concurrent-data-sessions max-session-number;
}
```

Hierarchy Level [edit services service-set *services-set-name* subscriber-profile *profile-name*]

Release Information Statement introduced in Junos OS Release 11.4.

Description Enable the service name for the subscriber profile.

Options ***service-name***—Name of the enabled service.

The remaining statements are explained separately.

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

exceed-action

Syntax

```
exceed-action {
  drop;
  syslog;
}
```

Hierarchy Level [edit services service-set *services-set-name* subscriber-profile *profile-name*
max-data-sessions-per-subscriber]

Release Information Statement introduced in Junos OS Release 11.4.

Description Specify the action if the maximum data sessions per subscriber exceed the maximum limit. You must also specify the drop rate of the packets for **drop** and system log details for **syslog**.

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

forward-rule (Configuring)

Syntax

```
forward-rule forward-rule-name {
  term precedence {
    from {
      application-groups [ application-group-name ];
      applications [ application-name ];
      local-address address <except>;
      local-address-range low low-value high high-value <except >;
      local-prefix-list prefix-list-name <except >;
    }
    then {
      forwarding-instance forwarding-instance;
      unit-number unit-number;
    }
  }
}
```

Hierarchy Level [edit services ptsp]

Release Information Statement introduced in Junos OS Release 10.2.
IPv6 support introduced in Junos OS Release 12.2

Description Specify the forwarding instance for a specific subscriber or set of subscribers based on the IP address, network, or prefix list. The rule match is applied on the input side.

Options *forward-rule-name*—Identifier for the collection of terms that constitute this rule.

The remaining statements are explained separately.

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

Related Documentation

- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

forward-rule (Including in Rule)

Syntax forward-rule *forward-rule-name*;

Hierarchy Level [edit services ptsp rule *rule-name*]

Release Information Statement introduced in Junos OS Release 10.2.

Description Identify the forwarding instance for inclusion in a rule.

Options ***forward-rule-name***—Identifier for the forward rule that specifies the forwarding instance.

The remaining statements are explained separately.

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

Related Documentation

- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

from (Forward Rule)

Syntax

```
from {
  application-groups [ application-group-name ];
  applications [ application-name ];
  local-address address <except >;
  local-address-range low low-value high high-value <except >;
  local-prefix-list prefix-list-name <except >;
}
```

Hierarchy Level [edit services ptsp forward-rule *forward-rule-name* term *precedence*]

Release Information Statement introduced in Junos OS Release 10.2.

Description Specify match conditions for the PTSP term.

Options For information on match conditions, see the description of firewall filter match conditions in the *Routing Policy Feature Guide for Routing Devices*.

The remaining statements are explained separately.

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

Related Documentation

- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

from (Rule)

Syntax

```
from {
  application-group-any;
  application-groups [ application-group-name ];
  applications [ application-name ];
  local-port-range low low-value high high-value;
  local-ports [ value-list ];
  protocol protocol-number;
  remote-address address <except >;
  remote-address-range low low-value high high-value <except >;
  remote-port-range low low-value high high-value;
  remote-ports [ value-list ];
  remote-prefix-list prefix-list-name <except >;
}
```

Hierarchy Level [edit services ptsp rule *rule-name* term *precedence*]

Release Information Statement introduced in Junos OS Release 10.2.

Description Specify match conditions for the PTSP term.

Options For information on match conditions, see the description of firewall filter match conditions in the *Routing Policy Feature Guide for Routing Devices*.

The remaining statements are explained separately.

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

Related Documentation

- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

limit

Syntax limit *max-sub-sessions*;

Hierarchy Level [edit services service-set *services-set-name* subscriber-profile *profile-name* max-data-sessions-per-subscriber]

Release Information Statement introduced in Junos OS Release 11.4.

Description Specify the limit for the maximum number of subscriber sessions.

Options ***max-sub-sessions***—Maximum number of subscriber sessions.

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

local-address

Syntax local-address (*address* | any-unicast) <except>;

Hierarchy Level [edit services ptsp forward-rule *forward-rule-name* term *precedence* from]

Release Information Statement introduced in Junos OS Release 10.2.
IPv6 support introduced in Junos OS Release 12.2

Description Specify the address for rule matching. Local address values are matched against a source or destination IP address for the flow depending on the configured value for the **demux** statement. If you do not specify an address, then any local address matches this term. If you do not specify a prefix value, then a host mask is the default.

Options ***address***—IPv4 or IPv6 address or prefix value.

any-unicast—Match all unicast addresses.

except—(Optional) Exclude the specified address, prefix, or unicast packets from rule matching.

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

Related Documentation

- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*
- demux on page 46

local-address-range

Syntax local-address-range low *low-value* high *high-value* <except>;

Hierarchy Level [edit services ptsp forward-rule *forward-rule-name* term *precedence* from]

Release Information Statement introduced in Junos OS Release 10.2.
IPv6 support introduced in Junos OS Release 12.2

Description Specify the address range for rule matching. Local address values are matched against a source or destination IP address for the flow depending on the configured value for the **demux** statement. If you do not specify an address, then any local address matches this term.

Options ***low-value***—Lower boundary for the IPv4 or IPv6 address range.

high-value—Upper boundary for the IPv4 or IPv6 address range.

except—(Optional) Exclude the specified address range from rule matching.

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

Related Documentation

- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*
- demux on page 46

local-port-range

Syntax local-port-range low *low-value* high *high-value*;

Hierarchy Level [edit services ptsp rule *rule-name* term *precedence* from]

Release Information Statement introduced in Junos OS Release 10.2.

Description Specify the port range for rule matching.

Options ***low-value***—Lower boundary for the port range.

high-value—Upper boundary for the port range.

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

Related Documentation

- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

local-ports

Syntax local-ports [*port-numbers*];

Hierarchy Level [edit services ptsp rule *rule-name* term *precedence* from]

Release Information Statement introduced in Junos OS Release 10.2.

Description Identify one or more ports for inclusion as a match condition.

Options ***port-numbers***—Port number.

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

Related Documentation
- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

local-prefix-list

Syntax local-prefix-list *prefix-list-name* <except>;

Hierarchy Level [edit services ptsp forward-rule *forward-rule-name* term *precedence* from]

Release Information Statement introduced in Junos OS Release 10.2.
IPv6 support introduced in Junos OS Release 12.2

Description Specify the prefix list for rule matching. You configure the prefix list by including the **prefix-list** statement at the **[edit policy-options]** hierarchy level.

Options ***prefix-list-name***—Prefix list.

except—(Optional) Exclude the specified prefix list from rule matching.

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

Related Documentation
- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

match-direction (Services PTSP)

Syntax match-direction (input | input-output | output);

Hierarchy Level [edit services ptsp rule *rule-name*]

Release Information Statement introduced in Junos OS Release 10.2.

Description Specify the direction in which the rule match is applied.

Options **input**—Apply the rule match on the input side of the interface.

input-output—Apply the rule match bidirectionally.

output—Apply the rule match on the output side of the interface.

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

Related Documentation

- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

max-data-sessions-per-subscriber

Syntax

```
max-data-sessions-per-subscriber {
  limit max-sub-sessions;
  exceed-action {
    drop;
    syslog;
  }
}
```

Hierarchy Level [edit services service-set *services-set-name* subscriber-profile *profile-name*]

Release Information Statement introduced in Junos OS Release 11.4.

Description Specify the maximum number of sessions that are concurrently enabled for the named service. The system randomly selects a number of sessions and enables the named service for them. To limit the service's use of resources, other sessions cannot access these named services.

Options The remaining statements are explained separately.

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

packet-triggered-subscribers

Syntax

```
packet-triggered-subscribers {
  partition partition-name {
    destination-host hostname;
    destination-realm realm;
    diameter-instance instance-name;
  }
  traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag <disable>;
    no-remote-trace;
  }
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced in Junos OS Release 10.2.

Description Configure PTSP to interact with an SAE in an SRC environment to provision packet-triggered subscribers.

The remaining statements are explained separately.

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

Related Documentation

- Configuring the PTSP Partition on page 31

packet-triggered-subscribers-partition

Syntax packet-triggered-subscribers-partition *partition-name*;

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 10.2.

Description Specify the PTSP partition to associate with the logical system and routing instance.

Options *partition-name*—Name of the PTSP partition that you want PTSP to use. The name is defined with the **partition** statement at the **[edit system services packet-triggered-subscribers]** hierarchy level.

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

Related Documentation

- Assigning the PTSP Partition on page 32

partition (PTSP)

Syntax

```
partition partition-name {
  destination-host hostname;
  destination-realm realm;
  diameter-instance instance-name;
}
```

Hierarchy Level [edit system services packet-triggered-subscribers]

Release Information Statement introduced in Junos OS Release 10.2.

Description Configure a PTSP partition.

Options ***partition-name***—Name of the PTSP partition.

The remaining statements are explained separately.

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

Related Documentation

- Configuring the PTSP Partition on page 31

protocol

Syntax protocol *protocol-number*;

Hierarchy Level [edit services ptsp rule *rule-name* term *precedence* from]

Release Information Statement introduced in Junos OS Release 10.2.

Description Identify the protocol for inclusion as a match condition.

Options ***protocol-number***—Protocol number.

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

Related Documentation

- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

remote-address

Syntax remote-address (*address* | any-unicast) <except>;

Hierarchy Level [edit services ptsp rule *rule-name* term *precedence* from]

Release Information Statement introduced in Junos OS Release 10.2.
IPv6 support introduced in Junos OS Release 12.2

Description Specify the address for rule matching. Remote address values are matched against a destination or source IP address for the flow depending on the configured value for the **demux** statement. If you do not specify an address, then any remote address matches this term. If you do not specify a prefix value, then a host mask is the default.

Options ***address***—IPv4 or IPv6 address or prefix value.

any-unicast—Match all unicast addresses.

except—(Optional) Exclude the specified address, prefix, or unicast packets from rule matching.

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

Related Documentation

- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*
- demux on page 46

remote-address-range

Syntax remote-address-range low *low-value* high *high-value* <except>;

Hierarchy Level [edit services ptsp rule *rule-name* term *precedence* from]

Release Information Statement introduced in Junos OS Release 10.2.
IPv6 support introduced in Junos OS Release 12.2

Description Specify the address range for rule matching. Remote address values are matched against a destination or source IP address for the flow depending on the configured value for the **demux** statement. If you do not specify an address, then any remote address matches this term.

Options ***low-value***—Lower boundary for the IPv4 or IPv6 address range.

high-value—Upper boundary for the IPv4 or IPv6 address range.

except—(Optional) Exclude the specified address range from rule matching.

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

Related Documentation

- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*
- demux on page 46

remote-port-range

Syntax remote-port-range low *low-value* high *high-value*;

Hierarchy Level [edit services ptsp rule *rule-name* term *precedence* from]

Release Information Statement introduced in Junos OS Release 10.2.

Description Specify the port range for rule matching.

Options ***low-value***—Lower boundary for the port range.

high-value—Upper boundary for the port range.

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

Related Documentation

- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

remote-ports

Syntax remote-ports [*port-numbers*];

Hierarchy Level [edit services ptsp rule *rule-name* term *precedence* from]

Release Information Statement introduced in Junos OS Release 10.2.

Description Identify one or more ports for inclusion as a match condition.

Options ***port-numbers***—Port number.

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

Related Documentation
- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

remote-prefix-list

Syntax remote-prefix-list *prefix-list-name* <except>;

Hierarchy Level [edit services ptsp rule *rule-name* term *precedence* from]

Release Information Statement introduced in Junos OS Release 10.2.
IPv6 support introduced in Junos OS Release 12.2

Description Specify the prefix list for rule matching. You configure the prefix list by including the **prefix-list** statement at the **[edit policy-options]** hierarchy level.

Options ***prefix-list-name***—Prefix list.

except—(Optional) Exclude the specified prefix list from rule matching.

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

Related Documentation
- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

rule (Configuring)

Syntax

```
rule rule-name {
  count-type (application | rule);
  demux (destination-address | source-address);
  forward-rule forward-rule-name;
  match-direction (input | input-output | output);
  term precedence {
    from {
      application-group-any;
      application-groups [ application-group-name ];
      applications [ application-name ];
      local-port-range low low-value high high-value;
      local-ports [ value-list ];
      protocol protocol-number;
      remote-address address <except>;
      remote-address-range low low-value high high-value <except>;
      remote-ports [ value-list ];
      remote-port-range low low-value high high-value;
      remote-prefix-list prefix-list-name <except>;
    }
    then {
      (accept | discard);
      count (application | application-group | application-group-any | rule | none);
      forwarding-class forwarding-class;
      police policer-name;
    }
  }
}
```

Hierarchy Level [edit services ptsp]

Release Information Statement introduced in Junos OS Release 10.2.

Description Specify the rule the router uses when applying this service.

Options ***rule-name***—Identifier for the collection of terms that constitute this rule.

The remaining statements are explained separately.

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

Related Documentation

- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

rule (Including in Rule Set)

Syntax rule *rule-name*;

Hierarchy Level [edit services ptsp rule-set *rule-set-name*]

Release Information Statement introduced in Junos OS Release 10.2.

Description Specify the rule the router uses when applying this service.

Options ***rule-name***—Identifier for the collection of terms that constitute this rule.

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

Related Documentation
- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

rule-set (Services PTSP)

Syntax
```
rule-set rule-set-name {
  [rule rule-names ];
}
```

Hierarchy Level [edit services ptsp]

Release Information Statement introduced in Junos OS Release 10.2.

Description Specify the rule set the router uses when applying this service.

Options ***rule-set-name***—Identifier for the collection of rules that constitute this rule set.

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

Related Documentation
- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

services (PTSP)

Syntax services ptsp { ... }

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 10.2.

Description Define the services to be applied to traffic.

Options **ptsp**—Identify the values configured for PTSP matching rules.

The statements are explained separately.

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

Related Documentation

- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

subscriber-identification (PTSP)

Syntax subscriber-identification *subscriber-identification*

Hierarchy Level [edit system services packet-triggered-subscribers partition radius *radius-partition-name*]

Release Information Statement introduced in Junos OS Release 11.3.

Description Configure the subscriber identification to be used in a PTSP partition. You can configure the subscriber identification only in a RADIUS partition.

Options ***subscriber-identification***—String of user-defined characters or a RADIUS attribute type that is supported by the PTSP application. To enable subscriber identification for the specified RADIUS attribute, you may configure the following RADIUS attributes:

- $attribute-1$—User-Name
- $attribute-4$—NAS-IP-Address
- $attribute-5$—NAS-Port
- $attribute-8$—Framed-IP-Address
- $attribute-32$—NAS-Identifier
- $attribute-87$—NAS-Port-ID

When configuring subscriber identification, you must precede the "$" with a slash (\) to enable the CLI interface to process and store the variable correctly.

NOTE: The IP address is formatted in dotted decimal notation—for example, 192.168.1.1. All the other numeric values are converted to a string of characters.

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

Related Documentation

- Configuring the PTSP Partition on page 31

subscriber-packet-idle-timeout

Syntax subscriber-packet-idle-timeout *subscriber-packet-idle-timeout*;

Hierarchy Level [edit system services packet-triggered-subscribers]

Description The subscriber packet idle timeout for packet triggered subscribers.

Options ***subscriber-packet-idle-timeout***—Maximum idle time.

Range: 15 through 1440 minutes.

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

Related Documentation

- Packet-Triggered Subscribers Services Overview on page 20

subscriber-profile

Syntax

```
subscriber-profile profile-name {
  enable service-name {
    concurrent-data-sessions max-session-number;
  }
  disable service-name;
  max-data-sessions-per-subscriber {
    limit max-sub-sessions;
    exceed-action {
      drop;
      syslog;
    }
  }
}
```

Hierarchy Level [edit services service-set *services-set-name*]

Release Information Statement introduced in Junos OS Release 11.4.

Description Specify the subscriber profile name. A subscriber profile specifies which services should be enabled and which services should be disabled for traffic belonging to a subscriber bound to a particular subscriber profile. A subscriber is bound to a minimum of one subscriber profile at any given time.

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

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

term (Forward Rule)

Syntax

```
term precedence {
  from {
    application-groups [ application-group-name ];
    applications [ application-name ];
    local-address address <except>;
    local-address-range low low-value high high-value <except>;
    local-prefix-list prefix-list-name <except>;
  }
  then {
    forwarding-instance forwarding-instance;
    unit-number unit-number;
  }
}
```

Hierarchy Level [edit services ptsp forward-rule *forward-rule-name*]

Release Information Statement introduced in Junos OS Release 10.2.

Description Define the term properties for the forward rule.

Options ***precedence***—Precedence value for this term in relation to other terms. Term with lowest precedence is evaluated first.

The remaining statements are explained separately.

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

Related Documentation

- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

term (Rule)

Syntax

```
term precedence {
  from {
    application-group-any;
    application-groups [ application-group-name ];
    applications [ application-name ];
    local-port-range low low-value high high-value;
    local-ports [ value-list ];
    protocol protocol-number;
    remote-address address <except>;
    remote-address-range low low-value high high-value <except>;
    remote-port-range low low-value high high-value;
    remote-ports [ value-list ];
    remote-prefix-list prefix-list-name <except>;
  }
  then {
    (accept | discard);
    count (application | application-group | application-group-any | rule);
    forwarding-class forwarding-class;
    police policer-name;
  }
}
```

Hierarchy Level [edit services ptsp rule *rule-name*]

Release Information Statement introduced in Junos OS Release 10.2.

Description Define the term properties for the PTSP rule.

Options ***precedence***—Precedence value for this term in relation to other terms. Term with lowest precedence is evaluated first.

The remaining statements are explained separately.

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

Related Documentation

- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

then (Forward Rule)

Syntax

```
then {
  forwarding-instance forwarding-instance;
  unit-number unit-number;
}
```

Hierarchy Level [edit services ptsp forward-rule *forward-rule-name* term *precedence*]

Release Information Statement introduced in Junos OS Release 10.2.

Description Define the term actions for the forward rule.

Options

forwarding-instance—Identifier for the forwarding instance for packet flows accepted under this policy.

unit-number—Unit number associated with the forwarding instance.

Required Privilege Level

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

Related Documentation

- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

then (Rule)

Syntax

```
then {
  (accept | discard);
  count (application | application-group | application-group-any | rule);
  forwarding-class forwarding-class;
  police policer-name;
}
```

Hierarchy Level [edit services ptsp rule *rule-name* term *precedence*]

Release Information Statement introduced in Junos OS Release 10.2.

Description Define the term actions. You can configure the router to accept or discard the targeted traffic. The action modifiers (count and forwarding-class) are optional.

Options You can configure one of the following actions:

- **accept**—Accept the packets and all subsequent packets in flows that match the rules.
- **discard**—Discard the packet and all subsequent packets in flows that match the rules.

When you select **accept** as the action, you can optionally configure one or both of the following action modifiers. No action modifiers are allowed with the **discard** action.

- **count (application | application-group | application-group-any | rule | none)**—For all accepted packets that match the rules, record a packet count using PTSP statistics practices. You can specify one of the following options; there is no default setting:
  - **application**—Count the application that matched in the **from** clause.
  - **application-group**—Count the application group that matched in the **from** clause.
  - **application-group-any**—Count all application groups that match **from application-group-any** under the **any** group name.
  - **rule**—Count the rule that matched in the **from** clause.
  - **none**—Same as not specifying **count** as an action.
- **forwarding-class *forwarding-class***—Specify the forwarding class name for outgoing packets.

When you include a policer, the only allowed action is **discard**. For more information on policers, see the *Routing Policy Feature Guide for Routing Devices*.

- **police *policer-name***—Apply rate-limiting properties to the traffic as configured at the **[edit firewall policer *policer-name*]** hierarchy level. This configuration allows bit-rate and burst-size attributes to be applied to the traffic that are not supported by PTSP rules.

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

Related Documentation

- Configuring Static PTSP Rules on page 35 in *Junos OS Subscriber Management and Services Library*

PART 3

Administration

CHAPTER 6

Monitoring Packet-Triggered Subscribers

Verifying and Managing PTSP Configuration

Purpose Display and clear information about packet-triggered subscribers and PTSP services.

Action

- To display bandwidth information about subscribers:

  user@host> show services subscriber bandwidth

- To display information about the active dynamic policies applied to a subscriber:

  user@host> show services subscriber dynamic-policies client-id *client-id*

- To display information about the data flows associated with a subscriber:

  user@host> show services subscriber flows client-id *client-id*

- To display information about the active packet-triggered subscriber sessions on the router:

  user@host> show services subscriber sessions

- To display information about the data traffic statistics for the packet-triggered subscriber:

  user@host> show services subscriber statistics client-id *client-id*

- To clear the active packet-triggered subscriber session on the router and log out the subscriber:

  user@host> clear services subscriber sessions client-id *client-id*

Related Documentation

- CLI Explorer

CHAPTER 7

Monitoring Commands

- clear services subscriber sessions
- clear request services subscribers
- set request services subscribers
- show services subscriber bandwidth
- show services subscriber dynamic-policies
- show services subscriber flows
- show services subscriber sessions
- show services subscriber statistics

clear services subscriber sessions

Syntax **clear services subscriber sessions client-id *client-id***

Release Information Command introduced in Junos OS Release 10.2.

Description Clear the packet-triggered subscriber sessions on the router to log out the subscribers.

Options **client-id *client-id***—Logs out the packet-triggered subscriber with this client ID. The client ID is a generated identifier assigned to each packet-triggered subscriber known to the router.

Required Privilege Level clear

Related Documentation
- show services subscriber sessions on page 86

List of Sample Output clear services subscriber sessions on page 76

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

Sample Output

clear services subscriber sessions

```
user@host> clear services subscriber sessions client-id 1
Initiated logout request for 1 subscriber session(s)
```

clear request services subscribers

Syntax **request services subscribers clear subscriber-profile *profile* client-id *client-id***

Release Information Command introduced in Junos OS Release 11.4.

Description Clear the subscriber profile associated with the given subscriber.

Options ***profile***—Name of the subscriber profile to clear the active subscriber profile for the given subscriber.

client-id—Client session ID assigned to the subscriber.

Required Privilege Level clear

List of Sample Output request services subscriber clear subscriber-profile tc_act_prof client-id on page 77

Sample Output

request services subscriber clear subscriber-profile tc_act_prof client-id

```
user@host>request services subscriber clear subscriber-profile tc_act_prof client-id
2533274790395909 | display xml
rpc-reply xmlns:junos="http://xml.juniper.net/junos/11.1I0/junos"
    packet-triggered-subscribers-information
xmlns="http://xml.juniper.net/junos/11.1I0/junos-packet-triggered-subscribers"
        service-subscribers-request-result junos:style="success"
        /service-subscribers-request-result
    /packet-triggered-subscribers-information
    cli
        banner/banner
    /cli
/rpc-reply
```

set request services subscribers

Syntax **request services subscribers set subscriber-profile *profile* client-id *client-id***

Release Information Command introduced in Junos OS Release 11.4.

Description Set the subscriber profile associated with the given subscriber.

Options ***profile***—Name of the subscriber profile to create or override the currently active subscriber profile for the given subscriber.

client-id—Client session ID assigned to the subscriber.

Required Privilege Level view

List of Sample Output request services subscriber set subscriber-profile tc_act_prof client-id on page 78

Sample Output

request services subscriber set subscriber-profile tc_act_prof client-id

```
user@host> request services subscriber set subscriber-profile tc_act_prof client-id
2533274790395909 | display xml
rpc-reply xmlns:junos="http://xml.juniper.net/junos/11.1I0/junos"
    packet-triggered-subscribers-information
xmlns="http://xml.juniper.net/junos/11.1I0/junos-packet-triggered-subscribers"
        service-subscribers-request-result junos:style="success"
        /service-subscribers-request-result
    /packet-triggered-subscribers-information
    cli
        banner/banner
    /cli
/rpc-reply
```

show services subscriber bandwidth

Syntax

show services subscriber bandwidth
<client-id *client-id*>
<interface *interface-name*> <top-talkers *top-talkers*>
<ip-address *ip-address*>
<service-interface *interface-name*> <top-talkers *top-talkers*>

Release Information

Command introduced in Junos OS Release 10.2.

Description

Display bandwidth information about subscribers with the specified criteria. The bandwidth is computed at fixed intervals on the MS-DPC and only the last interval is used for comparison.

Options

client-id *client-id*—(Optional) Displays bandwidth information for the subscriber with this client ID. The client ID is a generated identifier assigned to each packet-triggered subscriber known to the router.

interface *interface-name*—(Optional) Displays bandwidth information for the subscriber with this underlying interface name.

ip-address *ip-address*—(Optional) Displays bandwidth information for the subscriber with this IPv4 address.

service-interface *interface-name*—(Optional) Displays bandwidth information for the subscriber with this service interface name.

top-talkers *number-top-talkers*—(Optional) Displays bandwidth information for the specified number of subscribers using the most bandwidth based on the input-bps or output-bps values for the interface or service interface.

Required Privilege Level

view

List of Sample Output

show services subscriber bandwidth client-id on page 80

Output Fields

Table 10 on page 79 lists the output fields for the **show services subscriber bandwidth** command. Output fields are listed in the approximate order in which they appear.

Table 10: show services subscriber bandwidth Output Fields

Field Name	Field Description
client-id	Client identifier.
input-bps	Ingress bandwidth in bytes per second.
output-bps	Egress bandwidth in bytes per second.
input-pps	Ingress bandwidth in packets per second.
output-pps	Egress bandwidth in packets per second.

Sample Output

show services subscriber bandwidth client-id

```
user@host> show services subscriber bandwidth client-id 1
client-id   input-bps   output-bps   input-pps    output-pps
1           20          20           1000         1000
```

show services subscriber dynamic-policies

Syntax **show services subscriber dynamic-policies client-id *client-id***

Release Information Command introduced in Junos OS Release 10.2.

Description Display information about the active dynamic policies applied to the specified subscriber.

Options **client-id *client-id***—Displays information about the active dynamic policies applied to the subscriber with this client ID. The client ID is a generated identifier assigned to each packet-triggered subscriber known to the router.

Required Privilege Level view

List of Sample Output show services subscriber dynamic-policies client-id on page 82

Output Fields Table 11 on page 81 lists the output fields for the **show services subscriber dynamic-policies** command. Output fields are listed in the approximate order in which they appear.

Table 11: show services subscriber dynamic-policies Output Fields

Field Name	Field Description
Subscriber session	Client identifier.
Policy name	Dynamic policy identifier.
rpr	Rule precedence for the dynamic policy.
d	Direction of the dynamic policy.
Template	Service rule associated with the dynamic policy.
tpr	Term precedence.
ra	Remote address.
rm	Remote address mask.
lpl	Lower boundary for the local port range.
lph	Upper boundary for the local port range.
rpl	Lower boundary for the remote port range.
rph	Upper boundary for the remote port range.
p	Protocol.
a-f	Action.

Table 11: show services subscriber dynamic-policies Output Fields *(continued)*

Field Name	Field Description
a-s	Type of statistics collection and aggregation.
a-fc	Forwarding class.
a-p-i	Policer instance.
a-p-bw	Policer bandwidth.
a-p-mbs	Policer maximum burst size.
a-fu	Unit number for forwarding instance.
anl	Application names.
agl	Application group name.

Sample Output

show services subscriber dynamic-policies client-id

```
user@host> show services subscriber dynamic-policies client-id 1
Subscriber session 1 policy
  Policy name: 1311465998724890695
  rpr: 200
  d: input-output
    Template: __svc_rule__
    tpr: 100
    ra: 0.0.0.0
    rm: 0
    lpl: 0
    lph: 65535
    rpl: 0
    rph: 65535
    p: 0
    a-f: accept forwarding-class
    a-s:
    a-fc: assured-forwarding
    a-p-i: 0
    a-p-bw: 0
    a-p-mbs: 0
    a-fu: 0
    anl: junos:http
    agl: junos:web
    Template: __svc_rule__
    tpr: 100
    ra: 10.10.10.0
    rm: 0
    lpl: 0
    lph: 65535
    rpl: 0
```

```
rph: 65535
p: 0
a-f: accept
a-s:
a-fc:
a-p-i: 0
a-p-bw: 0
a-p-mbs: 0
a-fu: 0
anl:
agl:
```

show services subscriber flows

Syntax **show services subscriber flows client-id *client-id***

Release Information Command introduced in Junos OS Release 10.2.
Offload status for flows using Juniper Forwarding Mechanism (JFM) added in Junos OS Release 12.1.

Description Display information about the data flows associated with the specified subscriber. Offloading using JFM is supported only on MX Series routers with Modular Port Concentrators (MPCs) for the packet-triggered subscribers and policy control (PTSP) plug-in.

Options **client-id *client-id***—Displays information about the data flows associated with the subscriber identified by this client ID. The client ID is a generated identifier assigned to each packet-triggered subscriber known to the router.

Required Privilege Level view

List of Sample Output show services subscriber flows client-id on page 85
show services subscriber flows client-id for offloading using JFM on page 85

Output Fields Table 12 on page 84 lists the output fields for the **show services subscriber flows** command. Output fields are listed in the approximate order in which they appear.

Table 12: show services subscriber flows Output Fields

Field Name	Field Description
Subscriber session	Client identifier.
Number of data flows	Number of data sessions associated with this subscriber.
Data flow high-water-mark	High water mark number of concurrent data sessions for this subscriber. This value is never reset during the login session.
5-tuple	5 tuple information for each flow.
Application-ID	Application ID for each flow.
Policy-name	Service rule name for each flow.
Dir	Direction of each flow.
Packets	Information about counter statistics for each flow.
Bytes	Information about counter statistics for each flow.

Table 12: show services subscriber flows Output Fields *(continued)*

Field Name	Field Description
Off	The status of offload to Packet Forwarding Engine using JFM. The various options are: • Not Offloaded (-) • Offload requested but not completed (R) • Offload requested and completed (O)
Action	Action of the service rule for each flow.

Sample Output

show services subscriber flows client-id

```
user@host> show services subscriber flows client-id 1
Subscriber session 1
Number of data flows: 1
Data flows high-water-mark: 8180
5-tuple                                  Application-ID    Policy-name      Dir
80.1.1.2:45287->90.2.255.2:80,6           junos:http        ptsp-appl/23     I
Packets     Bytes       Action
6           511         C-T
```

show services subscriber flows client-id for offloading using JFM

```
user@host> show services subscriber flows client-id 1
5-tuple                          Application-ID   Policy-name   Dir   Packets
Bytes Off Action
80.1.1.2:45288->90.2.255.2:80,6   junos:http       ptsp-appl/23  I     12
1511  -    C-T
80.1.1.2:45287->90.2.255.2:80,6   junos:http       ptsp-appl/23  I     6
511   R    C-T
80.1.1.2:45287->91.4.2.200:80,6   junos:http       ptsp-appl/23  I     645
5329  O    C-T
```

show services subscriber sessions

Syntax

show services subscriber sessions
<brief | detail | summary>
<client-id *client-id*>
<interface *interface-name*>
<ip-address *ip-address*>
<routing-instance *routing-instance-name*>
<service-interface *interface-name*>
<user-id *user-id*>

Release Information

Command introduced in Junos OS Release 10.2.

Description

Display information about the active packet-triggered subscriber sessions on the router.

Options

brief | detail | summary—(Optional) Display the specified level of output. The default level is brief.

client-id *client-id*—(Optional) Displays information about the active packet-triggered subscriber sessions for this client ID. The client ID is a generated identifier assigned to each packet-triggered subscriber known to the router.

interface *interface-name*—(Optional) Displays information about the active packet-triggered subscriber sessions for the subscriber with this underlying interface name.

ip-address *ip-address*—(Optional) Displays information about the active packet-triggered subscriber sessions for the subscriber with this IP address.

routing-instance *routing-instance-name*—(Optional) Displays information about the active packet-triggered subscriber sessions for the subscriber on this routing instance.

service-interface *interface-name*—(Optional) Displays information about the active packet-triggered subscriber sessions for the subscriber with this service interface name.

user-id *user-id*—(Optional) Displays information about the active packet-triggered subscriber sessions with this user ID.

Required Privilege Level

view

Related Documentation

- clear services subscriber sessions on page 76

List of Sample Output

show services subscriber sessions client-id summary on page 87
show services subscriber sessions client-id on page 87
show services subscriber sessions client-id detail on page 87
show services subscriber sessions detail on page 87

Output Fields

Table 13 on page 87 lists the output fields for the **show services subscriber sessions** command. Output fields are listed in the approximate order in which they appear.

Table 13: show services subscriber sessions Output Fields

Field Name	Field Description
Client-ID	Client identifier.
IP-address	IPv4 address.
Underlying-interface	Interface where services are applied.
User-name	Subscriber identifier.
Service interface name	Location of the MS-DPC on which the subscriber is instantiated.
Routing instance	Routing instance on which the subscriber is instantiated.
State	State of the subscriber.

Sample Output

show services subscriber sessions client-id summary

```
user@host> show services subscriber sessions client-id 1 summary
1
```

show services subscriber sessions client-id

```
user@host> show services subscriber sessions client-id 1
Client-ID            IP-address      Underlying-interface User-name
1                    80.1.1.2        ge-1/3/2.1           ip80.1.1.2@default
```

show services subscriber sessions client-id detail

```
user@host> show services subscriber sessions client-id 1 detail
Subscriber session 1
  User name: ip80.1.1.2@default
  Interface name: ge-1/3/2.1
  User IP address: 80.1.1.2
  Service interface name: ms-2/0/0
  Routing instance: default
  State: logged in
  Login time: Tue Dec 29 19:56:07 2009
  1 service session(s) instantiated:
  Service session 1323423760868442114 => State: activated
```

show services subscriber sessions detail

```
user@host>show services subscriber sessions detail
Subscriber session 4503599627370515
  User name: 00a0.c9b2.551e@kanlab.jnpr.net<6.6.0.11>:glacier:ge-1/0/6.0[:0-0]
  Interface name: ge-1/0/3.8
  User IP address: 6.6.0.11
```

```
Service interface name: ms-4/0/0
Partition name: radius-p1
State: logged in
Subscriber profile: enable_HCM_only
Login time: Mon Oct  4 14:32:51 2010
1 service session(s) instantiated:
Service session radius => State: activated
```

show services subscriber statistics

Syntax **show services subscriber statistics client-id *client-id***

Release Information Command introduced in Junos OS Release 10.2.

Description Display information about the data traffic statistics for the specified packet-triggered subscriber and for each service rule attached to that subscriber.

Options **client-id *client-id***—Displays information about the data traffic statistics associated with the subscriber identified by this client ID. The client ID is a generated identifier assigned to each packet-triggered subscriber known to the router.

Required Privilege Level view

List of Sample Output show services subscriber statistics client-id by rule on page 89
show services subscriber statistics client-id by application on page 89

Output Fields Table 14 on page 89 lists the output fields for the **show services subscriber statistics** command. Output fields are listed in the approximate order in which they appear.

Table 14: show services subscriber statistics Output Fields

Field Name	Field Description
Aggregation-level	Type of statistics collected — subscriber and service rule or application.
Name/Id	Identifier for Aggregation-level field.
Packets-in	Number of ingress packets.
Packets-out	Number of egress packets.
Bytes-in	Number of ingress bytes.
Bytes-out	Number of egress bytes.

Sample Output

show services
subscriber statistics client-id by rule

```
user@host> show services subscriber statistics client-id 1
Aggregation-level Name/Id    Packets-in  Packets-out  Bytes-in  Bytes-out
subscriber        1          5           5            1000      1000
dynamic rule      ptsp-rule  5           5            1000      1000
```

Sample Output

show services

subscriber statistics client-id by application

```
user@host> show services subscriber statistics client-id 1
Aggregation-level Name/Id    Packets-in  Packets-out  Bytes-in   Bytes-out
subscriber        1          4358118     3630087      371167451  3301658453
application group any        4358118     3631768      371167451  3304179953
```

PART 4

Troubleshooting

CHAPTER 8

Acquiring Troubleshooting Information

Tracing Packet-Triggered Subscriber Operations

Packet-triggered subscriber tracing operations track packet-triggered subscriber operations and record them in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

All log files are located in the **/var/log** directory. You cannot change the directory (**/var/log**) in which trace files are located. When the trace file reaches its maximum size, a **.0** is appended to the filename, then a new file is created with a **.1**, and finally a **.2**. When the maximum number of trace files is reached, the oldest trace file is overwritten.

To configure packet-triggered subscriber tracing operations:

1. Specify that you want to configure tracing options.

   ```
   [edit system services packet-triggered-subscribers]
   user@host# edit traceoptions
   ```

2. (Optional) Configure the name for the file used for the trace output.
3. (Optional) Configure the number and size of the log files.
4. (Optional) Configure flags to filter the operations to be logged.

The packet-triggered subscriber traceoptions operations are described in the following sections:

Configuring the Packet-Triggered Subscribers Trace Log Filename

By default, the name of the file that records trace output for packet-triggered subscribers is **jptspd**. You can specify a different name with the **file** option.

To configure the filename for packet-triggered subscribers tracing operations:

- Specify the name of the file used for the trace output.

```
[edit system services packet-triggered-subscribers traceoptions]
user@host# set file ptsp-subs_1
```

Configuring the Size of Packet-Triggered Subscribers Log Files

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format ***.number*.gz**. The newest archived file is **.0.gz** and the oldest archived file is ***.(maximum number)-1*.gz**. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, ***filename***, reaches 2 MB, ***filename*** is compressed and renamed ***filename*.0.gz**, and a new file called ***filename*** is created. When the new ***filename*** reaches 2 MB, ***filename*.0.gz** is renamed ***filename*.1.gz** and ***filename*** is compressed and renamed ***filename*.0.gz**. This process repeats until there are 20 trace files. Then the oldest file, ***filename*.19.gz**, is simply overwritten when the next oldest file, ***filename*.18.gz** is compressed and renamed to ***filename*.19.gz**.

To configure the size of trace files:

- Specify the name and size of the file used for the trace output.

```
[edit system services packet-triggered-subscribers traceoptions]
user@host# set file ptsp-subs_1 _logfile_1 size 2097152
```

Configuring the Packet-Triggered Subscribers Tracing Flags

To configure the flags for the events to be logged:

- Configure the flags.

```
[edit system services packet-triggered-subscribers traceoptions]
user@host# set flag peer
user@host# set flag session
```

Related Documentation

- Configuring the PTSP Application on page 29

Configuring a Statistics Profile for PTSP

The local policy decision function (L-PDF) enables you to configure properties for statistics output by creating a statistics profile. The statistics profile configures the files to which statistics records are exported and the format that is exported. You configure the statistics profile so that the statistics records are exported to a flat file. Flat files contain statistics that are collected for each subscriber by application or application group. The statistics in a flat file are not transmitted to the external policy manager using Diameter.

To configure a statistics profile for PTSP:

1. Specify that you want to configure a statistics profile.

   ```
   [edit system services local-policy-decision-function]
   user@host# edit statistics
   ```

2. Configure the file properties used for the trace output.
3. Configure the profile properties.
4. Specify the record type.

Tasks to configure a statistics profile for PTSP are:

- Configuring the File Properties for Statistics Data Output on page 95
- Configuring the Profile Properties for Statistics Data Output on page 96
- Configuring the Record Type for Statistics Data on page 96

Configuring the File Properties for Statistics Data Output

You configure a file to which the statistics data output is exported in a specified format.

To configure the file properties:

1. Specify the unique filename for receiving statistics data output.

   ```
   [edit system services local-policy-decision-function statistics]
   user@host# edit file ptsp
   ```

2. (Optional) Specify the maximum number of files that are maintained at one time and the maximum size of each file. If you configure one of these options, you also must set the other option.

   ```
   [edit system services local-policy-decision-function statistics file ptsp]
   user@host# set files 10 size 1g
   ```

3. Specify the interval for transferring files to archive sites.

   ```
   [edit system services local-policy-decision-function statistics file ptsp]
   user@host# set transfer-interval 60
   ```

4. Specify one or more URLs for archiving the files. Archiving can be done by using FTP or SCP.

   ```
   [edit system services local-policy-decision-function statistics file ptsp]
   user@host# set archive-sites "ftp://anonymous@10.227.1.114"
   ```

Configuring the Profile Properties for Statistics Data Output

You can create an AACL statistics profile, which configures the statistics to collect and write to a file in the **/var/stats/aacl** directory.

To configure the profile properties:

1. Specify the name of the profile.

   ```
   [edit system services local-policy-decision-function statistics]
   user@host# edit aacl-statistics-profile ptsp
   ```

2. (Optional) Specify the file in the **/var/stats/aacl** directory in which statistics are collected. Enclose the name within quotation marks.

   ```
   [edit system services local-policy-decision-function statistics aacl-statistics-profile
     ptsp]
   user@host# set file "pstp"
   ```

3. Set the interval for reporting statistics.

   ```
   [edit system services local-policy-decision-function statistics aacl-statistics-profile
     ptsp]
   user@host# set report-interval 5
   ```

4. Set the **interim-active-only** mode for reporting statistics. This mode reports only statistics that have changed in the past report interval.

   ```
   [edit system services local-policy-decision-function statistics aacl-statistics-profile
     ptsp]
   user@host# set record-mode interim-active-only
   ```

5. Specify the statistics to be collected in the log file.

   ```
   [edit system services local-policy-decision-function statistics aacl-statistics-profile
     ptsp]
   user@host# set aacl-fields all-fields
   ```

Configuring the Record Type for Statistics Data

You must configure the interim record type for recording the AACL statistics.

To configure the record type:

- Specify interim as the record type.

  ```
  [edit system services local-policy-decision-function statistics]
  user@host# set record-type interim
  ```

Related Documentation

- Tracing PTSP Operations on page 97
- Configuring PTSP on page 29

Tracing PTSP Operations

Tracing operations track L-PDF operations and record them in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

By default, no events are traced. When you enable the tracing operation, the default tracing behavior is as follows:

1. Important events are logged in a file located in the **/var/log** directory. By default, the router uses the filename, **ptspd**. You can specify a different filename, but you cannot change the directory in which trace files are located.
2. When the trace log file ***filename*** reaches 128 kilobytes (KB), it is compressed and renamed ***filename*.0.gz**. Subsequent events are logged in a new file called ***filename***, until it reaches capacity again. At this point, ***filename*.0.gz** is renamed ***filename*.1.gz** and ***filename*** is compressed and renamed ***filename*.0.gz**. This process repeats until the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

   You can optionally configure the maximum file size to be from 10 KB through 1 gigabyte (GB). You can also specify the number of trace files to be from 2 through 1000. (For more information about how log files are created, see the *Junos OS System Log Messages Reference*.)

To customize trace file settings:

1. Specify that you want to configure tracing options.

   ```
   [edit system services local-policy-decision-function]
   user@host# edit traceoptions
   ```

2. Configure the filename used for the trace output.

   ```
   [edit system services local-policy-decision-function traceoptions]
   user@host# set file lpdfd
   ```

3. (Optional) Configure the maximum number and size of the log files. If you configure one of these options, you also must set the other option.

   ```
   [edit system services local-policy-decision-function traceoptions]
   user@host# set files 10 size 1g
   ```

4. (Optional) Specify flags to filter the operations to be logged. To specify more than one flag, include multiple **flag** statements.

   ```
   [edit system services local-policy-decision-function traceoptions]
   user@host# set flag ptsp-statistics
   ```

   The following table describes the flags that you can include.

Flag	Description
configuration	Trace configuration events

Flag	Description
database	Trace database events
general	Trace general flow
ptsp-statistics	Trace PTSP events
rtsock	Trace routing socket events
statistics	Trace statistics events
subscriber	Trace subscriber events

Related Documentation

- Configuring a Statistics Profile for PTSP on page 95
- Configuring PTSP on page 29

Collecting Subscriber Access Logs Before Contacting Juniper Technical Support

Problem When you experience a subscriber access problem in your network, we recommend that you collect certain logs before you contact Juniper Technical Support. This topic shows you the most useful logs for a variety of network implementations. In addition to the relevant log information, you must also collect standard troubleshooting information and send it to Juniper Technical Support in your request for assistance.

Solution To collect standard troubleshooting information:

- Redirect the command output to a file.

  user@host> **request support information | save rsi-1**

To configure logging to assist Juniper Technical Support:

1. Review the following blocks of statements to determine which apply to your configuration.

```
[edit]
set system syslog archive size 100m files 25
set system auto-configuration traceoptions file filename
set system auto-configuration traceoptions file filename size 100m files 25
set protocols ppp-service traceoptions file filename size 100m files 25
set protocols ppp-service traceoptions level all
set protocols ppp-service traceoptions flag all
set protocols ppp traceoptions file filename size 100m files 25
set protocols ppp traceoptions level all
set protocols ppp traceoptions flag all
set protocols ppp monitor-session all
set interfaces pp0 traceoptions flag all
set demux traceoptions file filename size 100m files 25
set demux traceoptions level all
set demux traceoptions flag all
set system processes dhcp-service traceoptions file filename
set system processes dhcp-service traceoptions file size 100m
set system processes dhcp-service traceoptions file files 25
set system processes dhcp-service traceoptions flag all
set class-of-service traceoptions file filename
set class-of-service traceoptions file size 100m
set class-of-service traceoptions flag all
set class-of-service traceoptions file files 25
set routing-options traceoptions file filename
set routing-options traceoptions file size 100m
set routing-options traceoptions flag all
set routing-options traceoptions file files 25
set interfaces traceoptions file filename
set interfaces traceoptions file size 100m
set interfaces traceoptions flag all
set interfaces traceoptions file files 25
set system processes general-authentication-service traceoptions file filename
set system processes general-authentication-service traceoptions file size 100m
set system processes general-authentication-service traceoptions flag all
set system processes general-authentication-service traceoptions file files 25
```

2. Copy the relevant statements into a text file and modify the log filenames as you want.
3. Copy the statements from the text file and paste them into the CLI on your router to configure logging.
4. Commit the logging configuration to begin collecting information.

NOTE: The maximum file size for DHCP local server and DHCP relay log files is 1 GB. The maximum number of log files for DHCP local server and DHCP relay is 1000.

BEST PRACTICE: Enable these logs only to collect information when troubleshooting specific problems. Enabling these logs during normal operations can result in reduced system performance.

Related Documentation

- *Compressing Troubleshooting Logs from /var/logs to Send to Juniper Technical Support*

CHAPTER 9

Troubleshooting Configuration Statement

traceoptions (PTSP)

Syntax

```
traceoptions {
  file filename <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag <disable>;
  no-remote-trace;
}
```

Hierarchy Level [edit system services packet-triggered-subscribers]

Release Information Statement introduced in Junos OS Release 10.2.

Description Define tracing operations for PTSP.

Options

file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all operations.
- **configuration**—Trace configuration events.
- **general**—Trace general flow.
- **peer**—Trace SRC peer events.
- **pic**—Trace PIC events.
- **rtsock**—Trace routing socket events.
- **session**—Trace session events.

disable—Disable this trace flag.

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: ***size*k** to specify KB, ***size*m** to specify MB, or ***size*g** to specify GB
Range: 10240 through 1073741824
Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

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

Related Documentation
- Tracing Packet-Triggered Subscriber Operations on page 93

PART 5

Index

Index

Symbols

A

B

C

D

E

F

G

J

L