Packet-Triggered Subscribers and Policy Control (PTSP)

Published: 2014-06-06

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

Packet-Triggered Subscribers and Policy Control (PTSP)

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:

- C Series

Documentation Conventions

Table 1 on page viii 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.

Documentation Conventions

Table 1 on page viii defines the notice icons used in this guide. Table 3 on page ix defines text conventions used throughout this documentation.

Table 2: 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 3: Text Conventions

Convention	Description	Examples
Bold text like this	• Represents keywords, scripts, and tools in text. • Represents a GUI element that the user selects, clicks, checks, or clears.	• Specify the keyword **exp-msg**. • Run the **install.sh** script. • Use the **pkgadd** tool. • To cancel the configuration, click **Cancel**.
Bold text like this	Represents text that the user must type.	**user@host# set cache-entry-age** *cache-entry-age*

`Fixed-width text like this`	Represents information as displayed on your terminal's screen, such as CLI commands in output displays.	`nic-locators {`
		`  login {`
		`  resolution {`
		`  resolver-name /realms/`
		`  login/A1;`
		`  key-type LoginName;`
		`  value-type SaeId;`
		`  }`

Regular sans serif typeface	• Represents configuration statements. • Indicates SRC CLI commands and options in text. • Represents examples in procedures. • Represents URLs.	• **system ldap server{ stand-alone;** • Use the **request sae modify device failover** command with the **force** option • **user@host# . . .** • http://www.juniper.net/techpubs/software/management/sdx/api-index.html

Table 3: Text Conventions *(continued)*

Italic sans serif typeface	Represents variables in SRC CLI commands.	**user@host# set local-address *local-address***
Angle brackets	In text descriptions, indicate optional keywords or variables.	Another runtime variable is <gfwif>.
Key name	Indicates the name of a key on the keyboard.	Press Enter.
Key names linked with a plus sign (+)	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
Italic typeface	• Emphasizes words. • Identifies book names. • Identifies distinguished names. • Identifies files, directories, and paths in text but not in command examples.	• There are two levels of access: *user* and *privileged*. • *SRC-PE Getting Started Guide.* • *o=Users, o=UMC* • The */etc/default.properties* file.
Backslash	At the end of a line, indicates that the text wraps to the next line.	Plugin.radiusAcct-1.class=\ net.juniper.smgt.sae.plugin\ RadiusTrackingPluginEvent
Words separated by the | symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. (The keyword or variable may be either optional or required.)	diagnostic | line

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

Managing Subscriber-Level Policies on MX Series Routers Overview

The Juniper Networks MX Series Ethernet Services Router supports a feature known as packet-triggered subscribers and policy control (PTSP). This feature allows dynamic policy and profile changes to be applied on a per-subscriber basis. The PTSP in the MX Series router signals the SRC policy manager when a new IP address flow is detected or when an existing flow is idle, and allows the policy manager to dynamically apply new policies associated with the IP address flow.

The SRC software uses the Diameter protocol for communications between the local SRC peer on a Juniper Networks routing platform, such as the MX Series router, and the service activation engine (SAE). The local SRC peer in the MX Series router is known as the *PTSP*.

The PTSP device driver has the following responsibilities:

- Manage the logical connection to the MX Series router Diameter peer (PTSP).
- Receive IP address notifications from the MX Series router and dynamically activate, modify, or deactivate policies for existing subscriber sessions.
- Send subscriber identification information to the MX Series router.
- Push subscriber policy changes to MX Series router.
- Retrieve accounting information for active service sessions.
- Terminate a subscriber session.
- Synchronize the state of a single subscriber session or all sessions.

The PTSP device driver responds to requests from the MX Series router, which signals subscribers logging in and logging out. The driver publishes interface tracking events, performs interface classification to determine any default policies, and initiates SAE subscriber session login and logout processing.

Multiple instances of the device driver for the same device (MX Series router) can be configured in the network. The instances communicate with each other to provide redundancy. Only one driver for a given device is active at the same time.

The SAE activates, modifies and deactivates subscriber policies. The SAE can control only those resources that have been provisioned through the SAE. Therefore, the SAE receives information about only those subscribers (IP address flows) for whom PTSP has requested provisioning from the SAE. Similarly, the SAE can control only the subscriber policies that it has activated.

Related Documentation

- Managing Dynamic Policy Changes on MX Series Routers Using the Diameter Application on page 4
- *Policy Management Overview*
- *Policy Information Model*

Managing Dynamic Policy Changes on MX Series Routers Using the Diameter Application

You can use the policy manager in the SRC software to dynamically manage subscriber level policy changes on MX Series routers. The PTSP device driver in the SRC software and the PTSP in the MX Series router are peers that communicate using a Diameter application. Information about subscriber policy changes is communicated between the PTSP and PTSP device driver using Diameter messages.

The SRC software includes a Diameter server process that forwards AAR, ACR, SRQ, and STR messages from PTSP to the PTSP device driver in the SAE, and that forwards PPR and ASR messages from the PTSP device driver to PTSP. These Diameter messages perform these functions:

- AA-Answer (AAA)—Sent in response to the AAR message for confirmation of the result of QoS provisioning.
- AA-Request (AAR)—Attaches the subscriber to the access network.
- Accounting-Request (ACR)—Provides accounting information.
- Abort-Session-Request (ASR)—Disconnects the subscriber.
- Push-Profile-Request (PPR)—Starts, modifies, or stops a service session.
- Session-Resource-Query (SRQ)—Initiates synchronization.
- Session-Termination-Request (STR)—Detaches the subscriber from the access network.

In the SRC software, you configure the Diameter peer (the MX Series router) and a device type (junos-ptsp) for each device managed by the SAE. The Diameter server process in the SRC software searches all devices of device type *junos-ptsp* for virtual routers that include the local host in their SAE connections. For these devices, the Diameter server process establishes a logical connection with the peers (in this case the MX Series router PTSP) referenced in the device configuration.

Related Documentation

- Managing Subscriber-Level Policies on MX Series Routers Overview on page 3
- Configuring the Diameter Application (SRC CLI) on page 13
- Configuring Diameter Peers (SRC CLI) on page 18

PART 2

Configuration

CHAPTER 2

Summary of PTSP Configuration Tasks

Configuring PTSP to Manage Subscriber-Level Policies

To configure PTSP to manage subscriber-level policies on the MX Series router:

- Configure PTSP on the MX Series router.

  See "Configuring PTSP on the MX Series Router" on page 11.

- Configure the Diameter application.

  See "Configuring the Diameter Application (SRC CLI)" on page 13

- Configure the Diameter peers.

  See "Configuring Diameter Peers (SRC CLI)" on page 18.

- Configure the SAE to manage PTSP on the MX Series router.

  See "Adding an MX Series Router as a PTSP Network Device (SRC CLI)" on page 21.

- Configure the SAE to obtain attachment session information from the SSR database.

  See "Configuring the SAE to Obtain Information About Subscribers (SRC CLI)" on page 23.

- Configure the PTSP device driver.

  See "Configuring the PTSP Device Driver (SRC CLI)" on page 27.

- Configure the session storage parameters for the PSTP device driver.

  See "Configuring the PTSP Device Driver Session Store (SRC CLI)" on page 28

- Configure the PTSP policies.

  See "Configuring PTSP Policies (SRC CLI)" on page 33.

CHAPTER 3

Configuration Tasks for the MX Series Router

Configuring PTSP on the MX Series Router

Tasks to set up PTSP on the Juniper Networks routing platform are:

- Configure the Multiservices DPC for PTSP.
- Configure the Diameter application to download dynamic PTSP policies.
- Configure any static PTSP policies.

Related Documentation

- For more information about running PTSP on the MX Series router, see the *Junos OS Subscriber Management and Services Library*.
- Configuring PTSP to Manage Subscriber-Level Policies on page 9

CHAPTER 4

Configuration Tasks for the Diameter Application

Configuring the Diameter Application (SRC CLI)

You can configure the properties of the application, client, server, and logging destination of the SRC Diameter application.

Perform the following tasks to configure these properties:

Configuring the Diameter Application Properties

The SRC software supports Diameter application properties such as Juniper Networks Session Resource Control (JSRC), Packet-Triggered Subscribers and Policy Control (PTSP), and GX-Plus. JSRC and PTSP communicates with the Service Activation Engine (SAE) (remote SRC peer), whereas GX-Plus communicates with the Policy and Charging Rules Function (PCRF).

Use the following configuration statements to configure the properties for the Diameter application:

```
system diameter {
    java-heap-size java-heap-size;
    java-new-size java-new-size;
    java-garbage-collection-options java-garbage-collection-options;
    protocol [(tcp | sctp)...];
    local-address [local-address...];
    port port;
    origin-host origin-host;
    origin-realm origin-realm;
    diameter-server-timeout diameter-server-timeout;
```

```
    active-peers;
    debug-mode;
    load-balancing-mode (failover | round-robin);
    transaction-processing-log (log-no-messages | log-severe-messages |
      log-normal-messages | log-debug-messages);
    packet-trace-log (log-no-messages | log-severe-messages | log-normal-messages |
      log-debug-messages);
    peer-state-machine-log (log-no-messages | log-severe-messages | log-normal-messages
      | log-debug-messages);
    configuration-log (log-no-messages | log-severe-messages | log-normal-messages |
      log-debug-messages);
}
```

To configure the Diameter application:

1. From configuration mode, access the statement for the Diameter application.

   ```
   user@host# edit system diameter
   ```

   

   NOTE: The java-* options have default values that should not be changed unless directed by Juniper Networks Technical Assistance Center (JTAC).

2. If you encounter problems caused by lack of memory, change the maximum memory size available to the Java Runtime Environment (JRE).

   ```
   [edit system diameter]
   user@host# set java-heap-size java-heap-size
   ```

3. Configure the amount of space available to the JRE when the Diameter server starts.

   ```
   [edit system diameter]
   user@host# set java-new-size java-new-size
   ```

4. Configure the garbage collection functionality of the Java Virtual Machine.

   ```
   [edit system diameter]
   user@host# set java-garbage-collection-options java-garbage-collection-options
   ```

5. Specify the protocol for the transport connection.

   ```
   [edit system diameter]
   user@host# set protocol [(tcp | sctp)...]
   ```

6. (Optional) Specify the local IP addresses that remote peers can use to reach this server.

   ```
   [edit system diameter]
   user@host# set local-address [local-address...]
   ```

7. (Optional) Specify the port for the server.

   ```
   [edit system diameter]
   user@host# set port  port
   ```

8. (Optional) Specify the fully qualified domain name (FQDN) used to identify this host to its Diameter peers.

   ```
   [edit system diameter]
   user@host# set origin-host origin-host
   ```

9. (Optional) Specify the realm used to identify this host to its Diameter peers.

   ```
   [edit system diameter]
   user@host# set origin-realm origin-realm
   ```

   The Diameter realm should be configured to the domain name of the origin host. For example, if the FQDN of the host is host.juniper.net, then the realm should be juniper.net. For PTSP, realm-based Diameter routing is not used.

10. (Optional) Configure the timeout value until which the Diameter server holds unsolicited requests such as Point to Point Protocol (PPP) and Abort Session Request (ASR), and waits for a matching response such as Push Profile Answer (PPA) and Abort Session Answer (ASA). The server discards the responses received after the specified time. The value range is 1–65,565 seconds. The preferred value is 10–30 seconds. By default, the value is set to 25 seconds .

    ```
    [edit system diameter]
    user@host# set diameter-server-timeout diameter-server-timeout
    ```

    NOTE: **diameter-server-timeout** and **reply-timeout** under the **[edit shared sae group configuration driver]** hierarchy should be configured with the same value.

11. (Optional) Specify whether the peer connection is in active mode.

    ```
    [edit system diameter]
    user@host# set active-peers
    ```

    NOTE: Active mode means that the SRC software actively tries to connect to the peer. Make sure the peer you are connecting to supports active peers. The MX Series router does not support active peers. The SRC software can still be configured, but the connection attempts will not work.

12. (Optional) Specify whether the peer connection is in debug mode.

    ```
    [edit system diameter]
    user@host# set debug-mode
    ```

13. (Optional) Configure the load-balancing mode for peer selection when forwarding a request message.

    ```
    [edit system diameter]
    user@host# set load-balancing-mode (failover | round-robin)
    ```

14. (Optional) Configure the log level for the transaction processing log.

    [edit system diameter]
    user@host# **set transaction-processing-log *log-level***

    where ***log-level*** is one of the following:

    - **log-no-messages**—Do not log any messages.
    - **log-severe-messages**—Log only severe messages.
    - **log-normal-messages**—Log only normal messages.
    - **log-debug-messages**—Log only debug messages.

15. (Optional) Configure the log level for the packet tracing log.

    [edit system diameter]
    user@host# **set packet-trace-log *log-level***

    where ***log-level*** is one of the following:

    - **log-no-messages**—Do not log any messages.
    - **log-severe-messages**—Log only severe messages.
    - **log-normal-messages**—Log only normal messages.
    - **log-debug-messages**—Log only debug messages.

16. (Optional) Configure the log level for the peer state machine log.

    [edit system diameter]
    user@host# **set peer-state-machine-log *log-level***

    where ***log-level*** is one of the following:

    - **log-no-messages**—Do not log any messages.
    - **log-severe-messages**—Log only severe messages.
    - **log-normal-messages**—Log only normal messages.
    - **log-debug-messages**—Log only debug messages.

17. (Optional) Configure the log level for the configuration log.

    [edit system diameter]
    user@host# **set configuration-log *log-level***

    where ***log-level*** is one of the following:

    - **log-no-messages**—Do not log any messages.
    - **log-severe-messages**—Log only severe messages.
    - **log-normal-messages**—Log only normal messages.
    - **log-debug-messages**—Log only debug messages.

Configuring the Diameter Client Properties

This procedure configures the client-side adapter of the SRC Diameter server, which handles client connections. Configuration should be necessary only if you encounter performance problems.

Use the following statements to configure the properties for the Diameter client:

```
system diameter client {
    threads threads;
    keep-alive-time keep-alive-time;
}
```

To configure the Diameter client properties:

1. From configuration mode, access the statement for the Diameter client.

   ```
   user@host# edit system diameter client
   ```

2. (Optional) Specify the number of threads to use.

   ```
   [edit system diameter client]
   user@host# set threads   threads
   ```

3. (Optional) Specify the time to wait for new commands.

   ```
   [edit system diameter client]
   user@host# set keep-alive-time keep-alive-time
   ```

Configuring the Diameter Server Properties

Use the following statements to configure the properties for the Diameter server:

```
system diameter server {
    threads threads;
    keep-alive-time keep-alive-time;
}
```

To configure the Diameter server properties:

1. From configuration mode, access the statement for the Diameter server.

   ```
   user@host# edit system diameter server
   ```

2. (Optional) Specify the minimum number of threads to use.

   ```
   [edit system diameter server]
   user@host# set threads   threads
   ```

3. (Optional) Specify the time to wait for new commands.

   ```
   [edit system diameter server]
   user@host# set keep-alive-time keep-alive-time
   ```

Configuring Logging Destinations

Use the following configuration statements to configure logging destinations for Diameter:

```
system diameter logger name ...

system diameter logger name file {
  filter filter;
  filename filename;
  rollover-filename rollover-filename;
  maximum-file-size maximum-file-size;
}
```

To configure logging destinations to store log messages in a file:

1. From configuration mode, access the statement that configures the name and type of logging destination.

   ```
   user@host# edit system diameter logger name file
   ```

2. Specify the properties for the logging destination.

   ```
   [edit system diameter logger name file]
   user@host# set ?
   ```

   For more information about configuring properties for the logging destination, see *Configuring Logging Destinations to Store Messages in a File (SRC CLI)*.

Related Documentation

- *SRC CLI Commands to Monitor the SRC Diameter Server*
- To manage services for JSRC peers on MX Series routers, see *Managing Services on MX Series Routers Using the Diameter Application*.
- To manage policies for PTSP peers on MX Series routers, see Configuring PTSP to Manage Subscriber-Level Policies on page 9.

Configuring Diameter Peers (SRC CLI)

Use the following configuration statements to configure the Diameter peers:

```
shared network diameter peer name {
  protocol [(tcp | sctp)...];
  address [address...];
  enforce-source-address;
  local-address local-address;
  connect-timeout connect-timeout;
  watchdog-timeout watchdog-timeout;
  state-machine-timeout state-machine-timeout;
  reconnect-timeout reconnect-timeout;
  port port;
  origin-host origin-host;
  incoming-queue-limit incoming-queue-limit;
  active-peer;
}
```

To configure the Diameter peer:

1. From configuration mode, access the statements for the peer.

   user@host# **edit shared network diameter peer** ***name***

   The peer name must be unique.

2. Specify the protocol for the transport connection.

   [edit shared network diameter peer ***name***]
   user@host# **set protocol** [**(tcp | sctp)**...]

3. Specify the addresses of the remote peer. If SCTP is the transport protocol, you can specify multiple addresses. If TCP is the transport protocol, you can specify only a single address.

   [edit shared network diameter peer ***name***]
   user@host# **set address** [***address***...]

4. (Optional) Specify whether the remote peer must connect from one of the IP addresses listed by the **address** option.

   [edit shared network diameter peer ***name***]
   user@host# **set enforce-source-address**

5. (Optional) Specify the local address of the peer.

   [edit shared network diameter peer ***name***]
   user@host# **set local-address** ***local-address***

6. (Optional) Specify the maximum amount of time allowed for the Diameter peer to respond to a connection request.

   [edit shared network diameter peer ***name***]
   user@host# **set connect-timeout** ***connect-timeout***

7. (Optional) Specify the watchdog timeout used for the connection to the remote peer.

   [edit shared network diameter peer ***name***]
   user@host# **set watchdog-timeout** ***watchdog-timeout***

8. (Optional) Specify the Diameter state machine timeout.

   [edit shared network diameter peer ***name***]
   user@host# **set state-machine-timeout** ***state-machine-timeout***

9. (Optional) Specify the time interval between connection attempts when the peer is in the disconnected state.

   [edit shared network diameter peer ***name***]
   user@host# **set reconnect-timeout** ***reconnect-timeout***

10. (Optional) Specify the port for the client.


```
[edit shared network diameter peer name]
user@host# set port port
```

11. (Optional) Specify the identifier for the endpoint that the peer presents during connection establishment.

```
[edit shared network diameter peer name]
user@host# set origin-host origin-host
```

12. (Optional) Specify the number of messages allowed on the incoming message queue for a peer.

```
[edit shared network diameter peer name]
user@host# set incoming-queue-limit incoming-queue-limit
```

13. (Optional) Specify whether the peer connection is in active mode.

```
[edit shared network diameter peer name]
user@host# set active-peer
```

NOTE: Active mode means that the SRC software actively tries to connect to the peer. Make sure the peer you are connecting to supports active peers. The MX Series router does not support active peers. The SRC software can still be configured, but the connection attempts will not work.

Related Documentation

- Configuring the Diameter Application (SRC CLI) on page 13
- *Viewing SRC Diameter Server State (SRC CLI)*

CHAPTER 5

Configuration Tasks for the SAE

Adding an MX Series Router as a PTSP Network Device (SRC CLI)

You can configure the service activation engine (SAE) to manage a packet-triggered subscribers and policy control (PTSP) network device on an MX Series router.

Use the following configuration statements to configure the network device:

```
shared network device name {
    device-type (junose | junos-ise | junos-ptsp | junos | pcmm | thirdparty);
    origin-host origin-host;
    peers [peers...];
}
shared network device name virtual-router name {
    sae-connection [sae-connection...];
    user-tracking-plug-in user-tracking-plug-in ...];
    authentication-plug-in [authentication-plug-in...];
    vpn-id vpn-id;
}
```

To configure an MX Series router as a PTSP network device so that the router can be managed by the SAE:

1. From configuration mode, access the statements that configure network devices. You must specify the name of a device with lowercase characters. This sample procedure uses mx-name as the name of the router.

   ```
   user@host# edit shared network device mx-name
   ```

2. Set the type of device to junos-ptsp.

   ```
   [edit shared network device mx-name]
   user@host# set device-type junos-ptsp
   ```

3. (Optional) Specify the origin host name of the MX Series router. This example procedure uses mx-origin-host as the origin host name. The active SAE registers events

from the router based on the configured origin host attribute (mx-origin-host in the example). If the origin host is not configured, SAE uses the device name (mx-name in the example) instead.

```
user@host# edit shared network origin-host mx-origin-host
```

4. Specify the configured peers associated with the device. See "Configuring Diameter Peers (SRC CLI)" on page 18.

```
[edit shared network device mx-name]
user@host# set peers [peers...]
```

Note that MX Series routers support only a single peer connection.

5. From configuration mode, access the statements for virtual routers. The name you specify must match the PTSP partition configured on the MX Series router, which is configured within the logical system:routing instance context. This sample procedure uses the name * for the virtual router.

```
[edit shared network device mx-name]
user@host# edit virtual-router *
```

where * matches any PTSP partition. You can also specify that the PTSP partition be configured in a logical system or in a logical system and routing instance. By default, logical system **default** and routing instance **master** are used.

6. Specify the SAEs that can manage this router.

```
[edit shared network device mx-name virtual-router default]
user@host# set sae-connection [sae-connection...]
```

7. (Optional) Specify a single tracking plug-in or a list of tracking plug-ins used to track subscriber sessions associated with this virtual router.

```
[edit shared network device mx-name virtual-router default]
user@host#  set user-tracking-plug-in  [ user-tracking-plug-in  ...]
```

Set the **user-tracking-plug-in** option to the name of the configuration plug-in you configured with the **edit shared sae configuration plug-ins name** *name* **ssr-writer** statement.

8. (Optional) Specify the plug-ins that authenticate subscribers who log in through this virtual router.

```
[edit shared network device mx-name virtual-router default]
user@host# set authentication-plug-in [authentication-plug-in...]
```

9. (Optional) Specify the VPN identifier used by this virtual router. You can specify VRF instead of a string to use the VRF instance reported by the device as the VPN identifier. In this case, the VPN identifier is the name of the routing instance.

```
[edit shared network device mx-name virtual-router default]
user@host# set vpn-id (vpn-id | VRF)
```

10. (Optional) Verify your configuration.


```
[edit shared network device mx-name]
user@host# show

device-type junos-ptsp;
interface-classifier {
  rule rule-1 {
    condition {
      interfaceName=*;
    }
    target /lib/default;
  }
}
origin-host bng-srcmx480b;
peers bng-srcmx480b;
virtual-router * {
  authentication-plug-in ldap-auth;
  sae-connection 10.212.10.2;
  user-tracking-plug-in fileAuth;
  vpn-id 123;
}
```

Related Documentation

- Configuring Diameter Peers (SRC CLI) on page 18
- *Adding Devices Running Junos OS and Virtual Routers (SRC CLI)*
- *Adding Objects for Network Devices (SRC CLI)*
- *Configuring the SAE to Manage Devices Running Junos OS (SRC CLI)*
- Configuring the SAE to Obtain Information About Subscribers (SRC CLI) on page 23
- Configuring the PTSP Device Driver (SRC CLI) on page 27

Configuring the SAE to Obtain Information About Subscribers (SRC CLI)

You can configure the SAE to obtain information about dynamic subscribers from the MX Series routers that support PTSP by making attachment session information available to the SAE. Tasks to configure the SAE for this purpose are:

- Obtaining Subscriber Session Information from the SSR Database on page 23
- Configuring Event Publishers on page 24

Obtaining Subscriber Session Information from the SSR Database

You can obtain subscriber information from the Session State Registrar (SSR) database. The SSR reader plug-in obtains information about attachment sessions from the SSR to set the values for the plug-in attributes. The SSR reader authentication plug-in can be used by a specific virtual router or for all virtual routers.

Use the following configuration statements to set up an SSR reader plug-in:

```
shared sae configuration plug-ins name name ssr-reader {
  read-attributes [read-attributes...];
}
```

To configure the SSR reader plug-in:

1. From configuration mode, access the SSR reader plug-in configuration.

   user@host# edit shared sae configuration plug-ins name *name* ssr-reader

2. (Optional) Specify the plug-in attribute whose value is set from the SSR subscriber sessions table.

   [edit shared sae configuration plug-ins name *name* ssr-reader]
   user@host# set read-attributes *[read-attributes...]*

Configuring Event Publishers

You can configure the event publisher to use the SSR reader authentication plug-in.

To configure the global or default event publisher for PTSP:

1. From configuration mode, access the statement that configures the event publisher.

   user@host# edit shared sae configuration plug-ins event-publishers

2. (Optional) Specify the plug-ins that authenticate subscribers who are assigned to a virtual router that does not specify an authentication plug-in.

   [edit shared sae configuration plug-ins event-publishers]
   user@host# set default-vr-authentication *[default-vr-authentication...]*

3. (Optional) Specify the plug-ins that authenticate subscribers who log in through a specific type of device (for example, junos-ptsp).

   [edit shared sae configuration plug-ins event-publishers]
   user@host# set device-type-authentication junos-ptsp *[plug-ins...]*

To specify the plug-ins that authenticate subscribers who log in through a specific virtual router, set the **authentication-plug-in** option when you are adding the virtual router for the network device. See "Adding an MX Series Router as a PTSP Network Device (SRC CLI)" on page 21.

Related Documentation

- Adding an MX Series Router as a PTSP Network Device (SRC CLI) on page 21
- *Configuring Global and Default Retailer Event Publishers (SRC CLI)*
- *SSR Database Schema*
- *Making Modifications to the SSR Database Schema Overview*

Configuring the SAE to Write Information About Subscribers to the SSR Database (SRC CLI)

When you use an SRC-managed device—for example, an E Series Broadband Services Router as the access node in a PTSP application—you can configure the SAE to write information about dynamic subscribers directly to the SSR database. To do this, you need to configure the SSR writer and specify the mapping between access subscriber session attributes and the SAE plug-in attributes used to identify service node subscriber sessions.

NOTE: Before you configure the SSR writer, we recommend that you configure the mapping between the SAE plug-in attributes and the SSR subscriber sessions table. The subscriber sessions table schema requires the user IP address and VPN ID; see *SSR Database Schema*.

Use the following statements to configure the mapping between access subscriber session attributes and the SAE plug-in attributes:

```
shared sae configuration plug-ins name name ssr-writer {
}
shared sae configuration plug-ins name name ssr-writer plugin-attributes id {
   access-plugin-attribute access-plugin-attribute;
   literal literal;
}
```

To configure the mapping between access subscriber session attributes and the SAE plug-in attributes:

1. From configuration mode, access the statement that configures the SSR writer plug-in and specify a name for the plug-in configuration. For example, to configure a plug-in configuration called pc1:

   ```
   [edit]
   user@host# edit shared sae configuration plug-ins name pc1 ssr-writer
   ```

   The name you specify for the configuration plug-in must be specified for the **user-tracking-plug-in** option under the **edit shared network device *name* virtual-router *name*** statement.

2. Specify the name of an SAE plug-in attribute to be mapped to the access session attribute, or literal. For example, to specify the login-name SAE plugin attribute:

   ```
   [edit shared sae configuration plug-ins name pc1 ssr-writer]
   user@host# edit plugin-attributes login-name
   ```

3. Specify the name of either an access plug-in attribute or a literal to be mapped to the SAE plug-in attribute.

   - To specify an access plug-in attribute—for example, login-name:

     ```
     [edit shared sae configuration plug-ins name pc1 ssr-writer plugin-attributes
       login-name]
     user@host# set access-plugin-attributes login-name
     ```

   - To specify a literal—for example, xyz-name:

     ```
     [edit shared sae configuration plug-ins name pc1 ssr-writer plugin-attributes
       login-name]
     user@host# set literal xyz-name
     ```

Related Documentation

- *Configuring the Fields in the Subscriber Sessions Table (SRC CLI)*

- *SSR Database Schema*
- *Modifying Attribute Mapping in an Active SSR Cluster (SRC CLI)*
- *Modifying the SSR Database Schema in an Active Cluster (SRC CLI)*

CHAPTER 6

Configuration Tasks for the PTSP Device Driver

Configuring the PTSP Device Driver (SRC CLI)

In most cases, all attributes have reasonable defaults and should not require configuration. The configuration should be changed only by advanced users wishing to tune the performance.

Use the following configuration statements to configure the PTSP device driver for MX Series routers:

```
shared sae configuration driver junos-ptsp {
    sae-community-manager  sae-community-manager;
    cached-driver-expiration cached-driver-expiration;
    keep-alive-timeout keep-alive-timeout;
    registry-retry-interval registry-retry-interval;
    reply-timeout reply-timeout;
    sequential-message-timeout  sequential-message-timeout;
    thread-pool-size  thread-pool-size;
    thread-idle-timeout thread-idle-timeout;
}
```

To configure the device driver:

1. From configuration mode, access the statements for the device driver.

   ```
   user@host# edit shared sae configuration driver junos-ptsp
   ```

2. Specify the name of the community manager.

   ```
   [edit shared sae configuration driver junos-ptsp]
   user@host# set sae-community-manager sae-community-manager
   ```

3. (Optional) Specify the minimum amount of time to keep the state of a device driver after its Diameter connection is closed.

   ```
   [edit shared sae configuration driver junos-ptsp]
   user@host# set cached-driver-expiration cached-driver-expiration
   ```

4. (Optional) Specify the keepalive timeout before the registry to a Diameter server expires.

   ```
   [edit shared sae configuration driver junos-ptsp]
   user@host# set keep-alive-timeout keep-alive-timeout
   ```

5. (Optional) Specify the interval between retrying a failed registry to a Diameter server.

   ```
   [edit shared sae configuration driver junos-ptsp]
   user@host# set registry-retry-interval registry-retry-interval
   ```

6. (Optional) Specify the length of time before a request sent to a Diameter server expires.

   ```
   [edit shared sae configuration driver junos-ptsp]
   user@host# set reply-timeout reply-timeout
   ```

7. (Optional) Specify the length of time before an expected message expires.

   ```
   [edit shared sae configuration driver junos-ptsp]
   user@host# set sequential-message-timeout sequential-message-timeout
   ```

8. (Optional) Specify the number of working threads that process requests.

   ```
   [edit shared sae configuration driver junos-ptsp]
   user@host# set thread-pool-size thread-pool-size
   ```

9. (Optional) Specify the length of time for stopping working threads after they become idle.

   ```
   [edit shared sae configuration driver junos-ptsp]
   user@host# set thread-idle-timeout thread-idle-timeout
   ```

10. (Optional) Configure the session store parameters for the device driver.

    From configuration mode, access the statement that configures the session store for the device driver.

    ```
    user@host# edit shared sae configuration driver junos-ptsp session-store
    ```

    For more information about configuring session store parameters, see *Configuring the Session Store Feature (SRC CLI)*.

Related Documentation

- *Configuring the SAE to Manage Devices Running Junos OS (SRC CLI)*
- Configuring the PTSP Device Driver Session Store (SRC CLI) on page 28

Configuring the PTSP Device Driver Session Store (SRC CLI)

In most cases, all attributes have reasonable defaults and should not require configuration. The configuration should be changed only by advanced users wishing to tune the performance.

Use the following configuration statements to configure the PTSP device driver session storage configuration:

```
shared sae configuration driver junos-ptsp session-store {
  maximum-queue-age maximum-queue-age;
```

```
    maximum-queued-operations maximum-queued-operations;
    maximum-queue-size maximum-queue-size;
    maximum-file-size maximum-file-size;
    minimum-disk-space-usage minimum-disk-space-usage;
    rotation-batch-size rotation-batch-size;
    maximum-session-size maximum-session-size;
    disk-load-buffer-size disk-load-buffer-size;
    network-buffer-size network-buffer-size;
    retry-interval retry-interval;
    communications-timeout communications-timeout;
    load-timeout load-timeout;
    idle-timeout idle-timeout;
    maximum-backlog-ratio maximum-backlog-ratio;
    minimum-backlog minimum-backlog;
}
```

To configure the PTSP device driver session storage:

1. From configuration mode, access the statements for the driver session storage.

   ```
   user@host# edit shared sae configuration driver junos-ptsp session-store
   ```

2. (Optional) Specify the maximum age that a queue of buffered store operations (such as adding a session to the store or removing a session from the store) can reach before the queue is written to a session store file.

   ```
   [edit shared sae configuration driver junos-ptsp session-store]
   user@host# set maximum-queue-age maximum-queue-age
   ```

   Enter a value for the number of milliseconds in the range 0–2147483647. A value of –1 indicates that there is no limit. A value of 0 causes the session store to write each store operation to a session store file immediately.

3. (Optional) Specify the number of buffered store operations that are queued before the queue is written to a session store file.

   ```
   [edit shared sae configuration driver junos-ptsp session-store]
   user@host# set maximum-queued-operations maximum-queued-operations
   ```

   Enter an integer in the range 0–2147483647. A value of –1 indicates that there is no limit. A value of 0 causes the session store to write each store operation to a session store file immediately.

4. (Optional) Specify the maximum size that a queue of buffered store operations can reach before the queue is written to a session store file.

   ```
   [edit shared sae configuration driver junos-ptsp session-store]
   user@host# set maximum-queue-size maximum-queue-size
   ```

   Enter the number of bytes in the range 0–2147483647.

5. (Optional) Specify the maximum size of session store files. When a file reaches this size, a new file is created.

   ```
   [edit shared sae configuration driver junos-ptsp session-store]
   user@host# set maximum-file-size maximum-file-size
   ```

   Enter the number of bytes in the range 0–2147483647.

6. (Optional) Specify the percentage of space in all session store files that is used by live sessions. When the space in the session store files that is used by live sessions decreases to this percentage, the oldest session store file is compacted and appended to the newest session store file, and then the oldest session store file is deleted.

   ```
   [edit shared sae configuration driver junos-ptsp session-store]
   user@host# set minimum-disk-space-usage minimum-disk-space-usage
   ```

   Enter a percentage of disk space in the range 1–100. We recommend a range of 30-50.

7. (Optional) Specify when the oldest session store file is rotated. The value specifies the number of sessions that are rotated from the oldest file to the newest file at the same time. While a set of sessions is rotated, no other session store activity can take place

   ```
   [edit shared sae configuration driver junos-ptsp session-store]
   user@host# set rotation-batch-size rotation-batch-size
   ```

   Enter an integer in the range 0–2147483647.

8. (Optional) Specify the maximum size of a single subscriber or service session. Use this parameter to reserve memory for an internal buffer.

   ```
   [edit shared sae configuration driver junos-ptsp session-store]
   user@host# set maximum-session-size maximum-session-size
   ```

   Enter the number of bytes in the range 0–2147483647.

9. (Optional) Specify the size of the buffer that is used to load all of a session store's files from disk at startup.

   ```
   [edit shared sae configuration driver junos-ptsp session-store]
   user@host# set disk-load-buffer-size disk-load-buffer-size
   ```

   Enter the number of bytes in the range 0–2147483647.

10. (Optional) Specify the size of the buffer that holds messages or message segments that are waiting to be sent to passive session stores.

    ```
    [edit shared sae configuration driver junos-ptsp session-store]
    user@host# set network-buffer-size network-buffer-size
    ```

    The number of bytes entered must be larger than or equal to 21 plus *maximum-session-size* and less than 2147483647.

11. (Optional) Specify the time interval to be allowed between attempts by the active session store to connect to missing passive session stores.

    ```
    [edit shared sae configuration driver junos-ptsp session-store]
    user@host# set retry-interval retry-interval
    ```

    Enter the number of milliseconds in the range 0–2147483647.

12. (Optional) Specify the amount of time in milliseconds that a session store should wait before closing when it is blocked from reading or writing a message. This timeout does not apply when a session store is waiting for a remote session store to load its state from disk.

    ```
    [edit shared sae configuration driver junos-ptsp session-store]
    user@host# set communications-timeout communications-timeout
    ```


Enter the number of milliseconds. (A nonpositive number means wait forever. This is not recommended.)

13. (Optional) Specify the amount of time in milliseconds that an active session store should wait for a passive session store or a passive session store waits for an active session store to load its data from disk before it closes the connection to the session store.

    ```
    [edit shared sae configuration driver junos-ptsp session-store]
    user@host# set load-timeout load-timeout
    ```

    Enter the number of milliseconds. (A nonpositive number means wait forever. This is not recommended.)

14. (Optional) Specify the amount of time that a passive session store waits for activity from the active session store before it closes the connection to the active session store. This timeout applies after the session store startup and initial update processes are complete.

    ```
    [edit shared sae configuration driver junos-ptsp session-store]
    user@host# set idle-timeout idle-timeout
    ```

    Enter the number of milliseconds in the range 0–2147483647.

15. (Optional) Specify the maximum backlog ratio. Along with the minimum backlog size, this ratio specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

    If the backlog of unsent operations (in bytes) divided by the total size (in bytes) of all live store operations is greater than this number, the connection is closed.

    ```
    [edit shared sae configuration driver junos-ptsp session-store]
    user@host# set maximum-backlog-ratio maximum-backlog-ratio
    ```

    Enter a floating point number.

16. (Optional) Specify the size of the minimum backlog. Along with the maximum backlog ratio, this number specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent to the passive session store. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened. If the maximum backlog ratio is met, the active session store does not close the connection unless the backlog of messages (in bytes) is greater than this number.

    ```
    [edit shared sae configuration driver junos-ptsp session-store]
    user@host# set minimum-backlog minimum-backlog
    ```

    Enter the number of bytes in the range 0–2147483647.

Related Documentation

- Configuring PTSP Policies (SRC CLI) on page 33
- Managing Subscriber-Level Policies on MX Series Routers Overview on page 3

CHAPTER 7

Configuration Tasks for PTSP Policies

Configuring PTSP Policies (SRC CLI)

The role of the policy list for the PTSP device driver must be set to *junos-ptsp*. The policy list must be configured to contain the rule of type *ptsp-service-rule*. A ptsp-service-rule object can contain one or more traffic-conditions and any number of actions (filter, policer-ref, forwarding-class, forwarding-instance). Each traffic-condition is translated to the PTSP policy template using the same action variables defined in the policy rule.

Before you configure PTSP policies, review the information about configuring and managing policies:

- *Policy Management Overview*
- *Policy Information Model*
- *Before You Configure SRC Policies*
- *Enabling the Policy Configuration on the SRC CLI*

To configure PTSP policies:

1. Create a policy group.

   See "Configuring Policy Groups (SRC CLI)" on page 35.

2. Configure the policy list and set the **role** of the list to **junos-ptsp** and the **applicability** to **both**.

   See "Configuring PTSP Policy Lists (SRC CLI)" on page 36.

3. Configure the PTSP policer instance.

See "Configuring the PTSP Policer Instance (SRC CLI)" on page 34.

4. Configure the PTSP policy rule and set the rule **type** to **ptsp-service-rule** or **ptsp-subscriber-profile**.

   See "Configuring PTSP Policy Rules (SRC CLI)" on page 37.

5. Configure the PTSP classify-traffic conditions.

   See "Configuring PTSP Classify-Traffic Conditions (SRC CLI)" on page 40.

6. Configure the PTSP actions.

   See "Configuring PTSP Actions" on page 51.

Related Documentation

- *Policy Components*
- Configuration Statements for PTSP Policies (SRC CLI) on page 61

Configuring the PTSP Policer Instance (SRC CLI)

Optionally, configure one or more policer instances that can be referenced by one or more PTSP policer-ref actions. The policer instance can be shared by different service rules inside the same policy list. If the policer instance is shared, all packets matching any of the service rules are policed together.

NOTE: You need to configure a policer instance only if a policy rule references the policer.

NOTE: For PTSP you must:

- Set the role of the policy list to junos-ptsp
- Set the policy list rule type to ptsp-service-rule
- Set the policy list applicability option to both
- Create a policer instance.

Use the following configuration statements to configure the policer instance:

```
policies group name list name policer name {
    bandwidth bandwidth;
    max-burst-size max-burst-size;
}
```

To configure a policer instance:

1. (Optional) From configuration mode, create a policer instance. In this example the policer instance is called policer1.

   user@host# edit policies group name list name policer policer1

2. (Optional) Specify the bandwidth for the policer instance.

   ```
   [edit policies group name list name policer policer1]

   user@host# set bandwidth bandwidth
   ```

   Enter an integer between 8000–40000000000 bits per second.

3. (Optional) Specify the maximum burst size for the policer instance.

   ```
   [edit policies group name list name policer policer1]
   user@host# set max-burst-size max-burst-size
   ```

   Enter an integer between 1500–100000000000 octets.

Related Documentation

- Configuring PTSP Policies (SRC CLI) on page 33
- Configuring PTSP Actions on page 51
- Configuring PTSP Policy Lists (SRC CLI) on page 36
- Configuring PTSP Policy Rules (SRC CLI) on page 37
- Configuring PTSP Classify-Traffic Conditions (SRC CLI) on page 40

Configuring Policy Groups (SRC CLI)

Policy groups hold policy lists. You can create policy groups within policy folders. Use the following configuration statement to create a policy group:

```
policies group name {
  description description ;
}
```

To create a policy group:

1. From configuration mode, enter the **edit policies group** statement. For example, to create a folder called dhcp-default:

   ```
   user@host# edit policies group dhcp-default
   ```

2. (Optional) Enter a description for the policy group.

   ```
   [edit policies group dhcp-default]
   user@host# set description description
   ```

3. (Optional) Verify your policy group configuration.

   ```
   [edit policies group dhcp-default]
   user@host#show
   description "Default policy for JunosE routers";
   ```

Related Documentation

- *Before You Configure SRC Policies*
- *Configuring Policy Folders (SRC CLI)*
- *Enabling the Policy Configuration on the SRC CLI*

- *Configuring Policy Groups (C-Web Interface)*
- *Example: Creating Access Policies for Subscribers*

Configuring PTSP Policy Lists (SRC CLI)

NOTE: For PTSP you must:

- Set the role of the policy list to **junos-ptsp**
- Set the policy list rule type to **ptsp-service-rule**
- Set the policy list **applicability** option to **both**
- Create a policer instance.

Use the following configuration statements to PTSP policy lists:

```
policies group name list name {
    role [(junos | junose-ipv4 | junose-ipv6 | junose-l2tp | pcmm | aaa | junos-ise | junos-ptsp)];
    applicability [(input | output | both | secondary-input)];
    description description;
}
```

To configure policy lists:

1. From configuration mode, create a policy list. For example, to create a policy list called list1 within a policy group called group1:

   ```
   user@host# edit policies group group1 list list1
   ```

2. Specify the role of the policy list. For PTSP the role must be set to **junos-ptsp**.

   ```
   [edit policies group group1 list list1]
   user@host# set role junos-ptsp
   ```

3. Specify where the policy is applied on the device. For PTSP the **applicability** option must be set to **both**.

   ```
   [edit policies group group1 list list1]
   user@host# set applicability both
   ```

Related Documentation

- *Policy Management Overview*
- Configuring PTSP Policies (SRC CLI) on page 33
- Configuring PTSP Policy Rules (SRC CLI) on page 37
- Configuring the PTSP Policer Instance (SRC CLI) on page 34

Configuring PTSP Policy Rules (SRC CLI)

NOTE: For PTSP you must:

- Set the role of the policy list to **junos-ptsp**
- Set the policy list rule type to **ptsp-service-rule**
- Set the policy list **applicability** option to **both**
- Create a policer instance.

Use the following configuration statements to configure PTSP policy rules:

```
policies group name list name rule name {
  precedence precedence;
  accounting;
  application-accounting application-accounting;
  type [(ptsp-service-rule | ptsp-subscriber-profile | ptsp-template)];
  subscriber-profile subscriber-profile;
}
```

To configure policy rules:

1. From configuration mode, create a policy rule inside a policy list that has already been created and configured. For example, to create a policy rule called rule1 within a policy list called list1:

   user@host# edit policies group group1 list list1 rule rule1

2. (Optional) Specify the order in which the policy manager applies the policy rule. Rules are evaluated from lowest to highest precedence value. Precedence has meaning only if two rules have different classifiers and if those classifiers overlap. If this is the case and a packet is received that satisfies both classifiers, then only the action of the rule with the lower precedence value is performed.

   For PTSP policies, enter an integer in the range 1–254.

   [edit policies group group1 list list1 rule rule1]
   user@host# set precedence *precedence*

3. (Optional) Specify whether accounting data is collected for the actions in the policy rule.

   The value set for the *a-s* variable in the ptsp-service-rule policy template (__svc_rule__) on the MX Series router corresponds to the setting of the **accounting** and **application-accounting** options under the policy rule. If the **accounting** option is set, it corresponds to setting the *a-s* variable to the “rule” value, and statistics are collected on a per subscriber/per rule basis. If the **accounting** option is not set, you can define the value for the **application-accounting** option.

   If you specify that accounting data is collected, the SAE begins collecting accounting information when a service that uses the policy rule is activated. When the service is

deactivated, the SAE sends the accounting records to the RADIUS accounting server or to a plug-in.

When you specify multiple actions for accounting, the SAE adds the accounting data for individual actions together to obtain a summary accounting record for that interface direction.

Accounting is not available for all actions.

```
[edit policies group group1 list list1 rule rule1
user@host# set accounting
```

4. (Optional) Specify application accounting.

   If PTSP application accounting is configured on the MX Series router, this attribute selects how application accounting is collected. Application accounting is maintained in a flat file on the router and is not collected by the SRC software. Application accounting and rule accounting are mutually exclusive.

   ```
   [edit policies group group1 list list1 rule rule1
   user@host# set application-accounting application-accounting
   ```

   The value set for the *a-s* variable in the **ptsp-service-rule** policy template (__svc_rule__) on the MX Series router corresponds to the setting of the **accounting** and **application-accounting** options under the policy rule. If the **accounting** option is not set, you can define one of the following values for the **application-accounting** option:

   - **“application”**—Router maintains one counter per subscriber/application. This value corresponds to setting the *a-s* variable in the **ptsp-service-rule** policy template (__svc_rule__) on the MX Series router to the “app” value, and statistics are collected on a per subscriber/per application basis.
   - **“group”**—Router maintains one counter per subscriber/application group. This value corresponds to setting the *a-s* variable in the **ptsp-service-rule** policy template (__svc_rule__) on the MX Series router to the “group” value, and statistics are collected on a per subscriber/per application-group basis.
   - **“any”**—Router maintains one counter per subscriber. This value corresponds to setting the *a-s* variable in the **ptsp-service-rule** policy template (__svc_rule__) on the MX Series router to the “any” value, and statistics are collected on a per subscriber basis.
   - **“nested-app”**—Router maintains one counter per subscriber/per nested application. This value corresponds to setting the *a-s* variable in the **ptsp-service-rule** policy template (__svc_rule__) on the MX Series router to the “nested-app” value, and statistics are collected on a per subscriber/per nested application basis. Use the *nanl* variable, in the policy template for the router to specify the list of nested application names. Items in the list are separated by commas.
   - A parameter of type applicationAccounting.

NOTE: The values **application**, **group**, **any**, and **nested-app** are literal strings and must be enclosed in double quotation marks (“ ”). To enter them in the SRC CLI, enclose the literal string with double quotation marks (“ ”) within single quotation marks (‘ ’). For example **“nested-app”** is entered as **‘“nested-app”’** in the SRC CLI. Alternatively, you can enclose them in double quotation marks within backslashes. For example, **\“nested-app”**.

5. Specify the type of policy rule.

   ```
   [edit policies group group1 list list1 rule rule1
   user@host# set type type
   ```

   Where ***type*** is one of the following values:

   - **ptsp-service-rule**—Use the predefined policy template called __svc_rule__ on the MX Series router.
   - **ptsp-subscriber-profile**—Use the policy template called __opt__ on the MX Series router. The router running Junos OS allows a service chain to be configured inside service sets, which are attached to the router interfaces. To configure this feature you need to specify a subscriber profile using the **subscriber-profile** option. The subscriber profile indicates which services should be enabled or disabled for the matching traffic flow. All traffic flows passing through the interface receive the same service chain irrespective of the subscriber. Using this option allows you to apply differentiated services to different sets of subscribers. Subscriber profiles must be preconfigured on the router. Only one subscriber profile can be bound to a subscriber at any given time. This option does not support classifiers or accounting.
   - **ptsp-template**—This setting is for future use.

6. (Optional) Specify the name of the subscriber profile to attach to the matching flow. This option is used only when the policy rule type is set to **ptsp-subscriber-profile**.

   ```
   [edit policies group group1 list list1 rule rule1
   user@host# set subscriber-profile subscriber-profile
   ```

   Set the value to one of the following:

   - A literal specifying the name of the subscriber profile. There are no predefined values for the **subscriber-profile** name; you must enter the name of a **subscriber-profile** you previously configured on the router. The name must be enclosed in double quotation marks, and entered in the SRC CLI enclosed within single quotation marks or backslashes. For example, ‘“vod1-profile”’ or \“vod1-profile”\.
   - A parameter of type profileName.

Related Documentation

- *Policy Management Overview*
- Configuring PTSP Policies (SRC CLI) on page 33
- Configuring the PTSP Policer Instance (SRC CLI) on page 34
- Configuring PTSP Actions on page 51

Configuring PTSP Classify-Traffic Conditions (SRC CLI)

Before you configure PTSP classify-traffic conditions, review the following topics:

- *Policy Management Overview*
- *Policy Components*
- *Policy Information Model*

Topics that discuss configuring PTSP classify-traffic conditions include:

Creating PTSP Classify-Traffic Conditions (SRC CLI)

You create classify-traffic conditions within policy rules. Use the following configuration statements to create a classify-traffic condition:

```
policies group name list name rule name traffic-condition name {
    match-direction match-direction;
    description  description;
}
```

To add a classify-traffic condition:

1. From configuration mode, create a classify-traffic condition inside a policy rule that has already been created and configured. For example, to create a traffic-condition called condition1 within policy rule rule1:

   ```
   user@host# edit policies group group1 list list1 rule rule1 traffic-condition condition1
   ```

2. (Optional) Specify the direction of the packet flow on which you want to match packets.

   ```
   [edit policies group group1 list list1 rule rule1 traffic-condition condition1]
   ```

```
user@host# set match-direction match-direction
```

Set to one of the following values:

- input
- output
- both
- Parameter of type matchDirection

3. (Optional) Provide a description of the classify-traffic condition.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1]
user@host# set description description
```

4. (Optional) Verify your PTSP classify-traffic condition configuration.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1]
user@host# show
match-direction output;
description "Destination classifier";
```

Configuring Destination Networks for PTSP Classify-Traffic Conditions (SRC CLI)

Use the following configuration statements to add destination networks to a PTSP classify-traffic condition:

```
policies group name list name rule name traffic-condition name destination-network
  network {
  ip-address ip-address;
  ip-mask ip-mask;
}
```

To add a destination network to a PTSP classify-traffic condition:

1. From configuration mode, enter the destination network within a classify-traffic condition. For example:

```
user@host# edit policies group group1 list list1 rule rule1 traffic-condition condition1
  destination-network network
```

2. (Optional) Specify the IP address of the destination network or host.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1
  destination-network network]
user@host# set ip-address ip-address
```

Where ***ip-address*** is one of the following values:

- IP address
- Predefined global parameter:
  - gateway_ipAddress—IP address of the gateway as specified by the service object.
  - interface_ipAddress—IP address of the router interface.

- service_ipAddress—IP address of the service as specified by the service object.
- user_ipAddress—IP address of the subscriber.
- virtual_ipAddress—Virtual portal address of the SAE that is used in redundant redirect server installations.

- Parameter of type address

3. (Optional) Configure the IP mask of the destination network or host.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1
  destination-network network]
user@host# set ip-mask ip-mask
```

Where ***ip-mask*** is one of the following values:

- IP address mask
- Predefined global parameter:
  - interface_ ipMask—IP mask of the router interface.
  - service_ ipMask—IP mask of the service as specified by the service object.
  - user_ ipMask—IP mask of the subscriber.
- Parameter of type address.

4. (Optional) Verify your destination network configuration.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1
 destination-network network]
user@host# show
ip-address interface_ipAddress;
ip-mask interface_ipMask;
```

Configuring Destination Grouped Networks for PTSP Classify-Traffic Conditions (SRC CLI)

Use the following configuration statements to add destination networks in a grouped format to a classify-traffic condition:

```
policies group name list name rule name traffic-condition name destination-network
  group-network {
  network-specifier network-specifier;
}
```

To add a grouped destination network to a classify-traffic condition:

1. From configuration mode, enter the destination network within a classify-traffic condition. For example:

```
user@host# edit policies group group1 list list1 rule rule1 traffic-condition condition1
  destination-network group-network
```

2. (Optional) Configure the IP address of the destination network or host.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1
  destination-network group-network]
```

```
user@host# set network-specifier network-specifier
```

3. (Optional) Verify your destination network configuration.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1
 destination-network group-network]
user@host# show
network-specifier any;
```

Configuring Protocol Conditions for PTSP Classify-Traffic Conditions (SRC CLI)

The procedure in this topic shows how to configure protocol conditions that do not include port conditions.

- If your condition includes port numbers, use the procedure in "Configuring Protocol Conditions with Ports for PTSP Classify-Traffic Conditions (SRC CLI)" on page 44.
- If your condition consists of a protocol that is assigned with a parameter value, use the procedure in "Configuring Protocol Conditions with Parameters for PTSP Classify-Traffic Conditions (SRC CLI)" on page 46.

Use the following configuration statements to add general protocol conditions to a PTSP classify-traffic condition:

```
policies group name list name rule name traffic-condition name protocol-condition {
  protocol protocol;
}
```

To add general protocol conditions to a classify-traffic condition:

1. From configuration mode, enter the general protocol condition configuration. For example:

```
user@host# edit policies group group1 list list1 rule rule1 traffic-condition condition1
  protocol-condition
```

2. Configure the protocol matched by this classify-traffic condition.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1
  protocol-condition]
user@host# set protocol protocol
```

   Enter the protocol matched by this classifier list, one of the following values:

   - Predefined global parameter—Use a ? at the command line to see a list of valid protocols.
   - Protocol number in the range 0–255.
   - String expression.
   - Parameter of type protocol.

3. (Optional) Verify your protocol condition configuration.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1
 protocol-condition]
```

```
user@host# show
protocol 0;
```

Configuring Protocol Conditions with Ports for PTSP Classify-Traffic Conditions (SRC CLI)

Use the following configuration statements to add general protocol conditions with ports to a PTSP classify-traffic condition:

```
policies group name list name rule name traffic-condition name protocol-port-condition
  {
  protocol  protocol;
}
policies group name list name rule name traffic-condition name protocol-port-condition
  destination-port port {
  from-port from-port;
}
policies group name list name rule name traffic-condition name protocol-port-condition
  source-port port {
  from-port from-port;
}
```

To add general protocol conditions with ports to a PTSP classify-traffic condition:

1. From configuration mode, enter the protocol port condition configuration. For example:

   ```
   user@host# edit policies group group1 list list1 rule rule1 traffic-condition condition1
     protocol-port-condition
   ```

2. Configure the protocol matched by this classify-traffic condition.

   ```
   [edit policies group group1 list list1 rule rule1 traffic-condition condition1
     protocol-port-condition]
   user@host# set protocol  protocol
   ```

   UDP is the only valid value for PTSP.

3. (Optional) Enter the destination port configuration for the protocol port configuration.

   ```
   [edit policies group group1 list list1 rule rule1 traffic-condition condition1
     protocol-port-condition]
   user@host# edit destination-port
   ```

4. (Optional) Configure the destination port.

   ```
   [edit policies group group1 list list1 rule rule1 traffic-condition condition1
     protocol-port-condition destination-port port]
   user@host# set from-port  from-port
   ```

   Where ***from-port*** is one of the following values:

   - service_port—A predefined global parameter that is the port of the service as specified by the service object
   - Integer in the range 0–65535

- Expression—A range of port numbers; for example, 10..20
- Parameter of type port

Use a range of ports to specify port numbers that are greater than or less than a specified port number. For example:

- To set a range of ports that is greater than 10, use 11..65535.
- To set a range of ports that is less than 200, use 0..199.

5. (Optional) Enter the source port configuration for the protocol port configuration.

```
user@host# up

[edit policies group group1 list list1 rule rule1 traffic-condition condition1
  protocol-port-condition]
user@host# edit source-port
```

6. (Optional) Configure the source port.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1
  protocol-port-condition source-port port]
user@host# set from-port from-port

[edit policies group group1 list list1 rule rule1 traffic-condition condition1
  protocol-port-condition source-port port]
user@host# up
```

Where ***from-port*** is one of the following values:

- service_port — A predefined global parameter that is the port of the service as specified by the service object.
- Integer in the range 0–65535
- Expression — A range of port numbers; for example, 10..20.
- Parameter of type port

Use a range of ports to specify port numbers that are greater than or less than a specified port number. For example:

- To set a range of ports that is greater than 10, use 11..65535.
- To set a range of ports that is less than 200, use 0..199.

7. (Optional) Verify your protocol condition configuration.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1
 protocol-port-condition]
user@host# show
protocol udp;
destination-port {
  port {
        from-port service_port;
  }
}
source-port {
```

```
    port {
        from-port service_port;
    }
}
```

Configuring Protocol Conditions with Parameters for PTSP Classify-Traffic Conditions (SRC CLI)

Use the following configuration statements to configure classify-traffic conditions that contain a parameter value for the protocol:

```
policies group name list name rule name traffic-condition name
  parameter-protocol-condition {
  protocol  protocol;
}
policies group name list name rule name traffic-condition name
  parameter-protocol-condition proto-attr destination-port port {
  from-port from-port;
}
policies group name list name rule name traffic-condition name
  parameter-protocol-condition proto-attr source-port port {
  from-port from-port;
}
```

To configure a protocol condition that contains a parameter value for the protocol:

1. From configuration mode, enter the parameter protocol condition configuration. For example:

   ```
   user@host# edit policies group group1 list list1 rule rule1  traffic-condition condition1
     parameter-protocol-condition
   ```

2. Assign a parameter as the protocol matched by this classify-traffic condition.

   Before you assign a parameter, you must create a parameter of type protocol and commit the parameter configuration.

   ```
   [edit policies group group1 list list1 rule rule1 traffic-condition condition1
     parameter-protocol-condition]
   user@host# set protocol  protocol
   ```

3. (Optional) Enter the protocol attribute configuration.

   ```
   [edit policies group group1 list list1 rule rule1 traffic-condition condition1
     parameter-protocol-condition]
   user@host# edit proto-attr
   ```

4. (Optional) Enter the destination port configuration.

   ```
   [edit policies group group1 list list1 rule rule1 traffic-condition condition1
     parameter-protocol-condition proto-attr]
   user@host# edit destination-port port
   ```

5. (Optional) Configure the TCP or UDP destination port.

   ```
   [edit policies group group1 list list1 rule rule1 traffic-condition condition1
     parameter-protocol-condition proto-attr destination-port port]
   ```

```
user@host# set from-port from-port
```

Where ***from-port*** is one of the following values:

- service_port—A predefined global parameter that is the port of the service as specified by the service object.
- Integer in the range 0–65535.
- Expression—A range of port numbers; for example, 10..20.
- Parameter of type port.

Use a range of ports to specify port numbers that are greater than or less than a specified port number. For example:

- To set a range of ports that is greater than 10, use 11..65535.
- To set a range of ports that is less than 200, use 0..199.

6. (Optional) Enter the source port configuration.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1
  parameter-protocol-condition proto-attr destination-port port]
user@host# up
[edit policies group group1 list list1 rule rule1 traffic-condition condition1
  parameter-protocol-condition proto-attr]
user@host# edit source-port port
```

7. (Optional) Configure the TCP or UDP source port.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1
  parameter-protocol-condition proto-attr source-port port]
user@host# set from-port from-port

[edit policies group group1 list list1 rule rule1 traffic-condition condition1
  parameter-protocol-condition proto-attr source-port port]
user@host# up

[edit policies group group1 list list1 rule rule1 traffic-condition condition1
  parameter-protocol-condition proto-attr source-port]
user@host# up

[edit policies group group1 list list1 rule rule1 traffic-condition condition1
  parameter-protocol-condition proto-attr ]
user@host# up
```

Where ***from-port*** is one of the following values:

- service_port — A predefined global parameter that is the port of the service as specified by the service object.
- Integer in the range 0–65535.
- Expression — A range of port numbers; for example, 10..20.
- Parameter of type port.

Use a range of ports to specify port numbers that are greater than or less than a specified port number. For example:

- To set a range of ports that is greater than 10, use 11..65535.
- To set a range of ports that is less than 200, use 0..199.

8. (Optional) Verify the parameter protocol configuration.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1
 parameter-protocol-condition]
user@host# show
protocol protocol;
  destination-port {
    port {
      from-port service_port;
    }
  }
}
```

Configuring TCP Conditions for PTSP Classify-Traffic Conditions (SRC CLI)

Use the following configuration statements to add TCP conditions to a PTSP classify-traffic condition:

```
policies group name list name rule name traffic-condition name tcp-condition {
  protocol tcp;
}
```

Because the protocol is already set to TCP, do not change the protocol or protocol-operation options.

```
policies group name list name rule name traffic-condition name tcp-condition
  destination-port port {
  from-port from-port;
}
```

```
policies group name list name rule name traffic-condition name tcp-condition
  source-port port {
  from-port from-port;
}
```

To add TCP conditions to a PTSP classify-traffic condition:

1. From configuration mode, enter the TCP configuration. For example:

```
user@host# edit policies group group1 list list1 rule rule1 traffic-condition  condition1
  tcp-condition
```

2. (Optional) Enter the protocol for the TCP configuration.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1 tcp-condition]
user@host# set protocol protocol
```

For PTSP this is set to TCP.

3. (Optional) Enter the destination port configuration for the TCP configuration.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1 tcp-condition]
```

```
user@host# edit destination-port port
```

4. (Optional) Configure the destination port.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1 tcp-condition
  destination-port port]
user@host# set from-port  from-port
```

Where ***from-port*** is one of the following values:

- service_port—A predefined global parameter that is the port of the service as specified by the service object.
- Integer in the range 0–65535.
- Expression—A range of port numbers; for example, 10..20.
- Parameter of type port.

Use a range of ports to specify port numbers that are greater than or less than a specified port number. For example:

- To set a range of ports that is greater than 10, use 11..65535.
- To set a range of ports that is less than 200, use 0..199.

5. (Optional) Enter the source port configuration for the TCP configuration.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1 tcp-condition
  source-port port]
user@host# up

[edit policies group group1 list list1 rule rule1 traffic-condition condition1]
user@host# edit source-port port
```

6. (Optional) Configure the source port.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1 tcp-condition
  source-port port]
user@host# set from-port  from-port

[edit policies group group1 list list1 rule rule1 traffic-condition condition1 tcp-condition
  source-port port]
user@host# up
```

Where ***from-port*** is one of the following values:

- service_port — A predefined global parameter that is the port of the service as specified by the service object.
- Integer in the range 0–65535
- Expression — A range of port numbers; for example, 10..20.
- Parameter of type port

Use a range of ports to specify port numbers that are greater than or less than a specified port number. For example:

- To set a range of ports that is greater than 10, use 11..65535.
- To set a range of ports that is less than 200, use 0..199.

7. (Optional) Verify the TCP condition configuration.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1
 tcp-condition]
user@host# show
protocol tcp;
protocol-operation is;
destination-port {
  port {
        from-port service_port;
  }
}
source-port {
  port {
       from-port service_port;
  }
}
```

Configuring Traffic Match Conditions for PTSP Classify-Traffic Conditions (SRC CLI)

Use the following configuration statements to configure traffic match conditions for PTSP classify traffic conditions.

```
policies group name list name rule name traffic-condition name traffic-match-condition
  {
  application  [application...];
  application-group [application-group...];
  nested-application [nested-application...];
  term-precedence term-precedence;
}
```

To add traffic match conditions to PTSP classify-traffic conditions:

1. From configuration mode, enter the traffic condition configuration. For example:

   ```
   user@host# edit policies group group1 list list1 rule rule1 traffic-condition condition1
     traffic-match-condition
   ```

2. (Optional) Configure the application protocol to match.

   ```
   [edit policies group group1 list list1 rule rule1 traffic-condition condition1
     traffic-match-condition]
   user@host# set application [application...]
   ```

3. (Optional) Configure a list of application groups to match for this policy.

   ```
   [edit policies group group1 list list1 rule rule1 traffic-condition condition1
     traffic-match-condition]
   user@host# set application-group [application-group...]
   ```

4. (Optional) Configure a list of nested applications to match this policy.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1
  traffic-match-condition]
user@host# set nested-application  [nested-application...]
```

Separate items in the list with commas.

5. (Optional) Configure the **term-precedence** for this term in a given policy in relation to other terms. Lower precedence terms are searched first. Precedence matters only within the same class of policies, either dynamic or static. Terms with the same precedence may be evaluated in any order.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1
  traffic-match-condition]
user@host# set term-precedence term-precedence
```

Enter an integer in the range 1–254.

6. (Optional) Verify the filter condition configuration.

```
[edit policies group group1 list list1 rule rule1 traffic-condition condition1
 traffic-match-condition]
user@host# show
term-precedence 100;
application-group group1;
}
```

Configuring PTSP Actions

Actions define the action taken on packets that match conditions in a policy rule. You create actions within policy rules.

Topics that discuss how to configure PTSP actions include:

- Configuring Policer-Ref Actions (SRC CLI) on page 51
- Configuring Forwarding Instance Actions (SRC CLI) on page 52
- Configuring Forwarding Class Actions (SRC CLI) on page 53
- Configuring Filter Actions (SRC CLI) on page 54

Configuring Policer-Ref Actions (SRC CLI)

Use this action to specify an action that references a PTSP policer instance. You can configure policer ref actions for PTSP policy rules. The policer instance can be shared by different service rules inside the same policy list. Multiple policy rules can reference the same policer instance, so that the traffic matched by those rules is policed by the same policer instance. If the policer instance is shared, all packets matching any of the service rules are policed together.

NOTE: For PTSP you must:

- Set the role of the policy list to junos-ptsp
- Set the policy list rule type to ptsp-service-rule
- Set the policy list applicability option to both
- Create a policer instance.

Use the following configuration statements to configure a policer-ref action:

```
policies group name list name rule name policer-ref {
  policer-ref policer-name ;
  description description ;
}
```

To configure the policer-ref action:

1. From configuration mode, access the statements for the policer-ref action.

   user@host# edit policies group *name* list *name* rule *name* policer-ref

2. Specify the name of the policer instance you want to reference.

   [edit policies group name list name rule name policer-ref]
   user@host# set *policer–name*

3. Enter a description for the action.

   [edit policies group name list name rule name policer-ref]
   user@host# set description *description*

Configuring Forwarding Instance Actions (SRC CLI)

You can configure forwarding instance actions for routers running the PTSP feature. This action specifies a forwarding instance to assign to flows that match this policy.

NOTE: For PTSP you must:

- Set the role of the policy list to junos-ptsp
- Set the policy list rule type to ptsp-service-rule
- Set the policy list applicability option to both
- Create a policer instance.

Use the following configuration statements to configure a forwarding instance action:

```
policies group name list name rule name forwarding-instance {
  forwarding-instance;
  forwarding-unit forwarding-unit ;
  description description ;
```

```
}
```

To configure a forwarding instance action:

1. From configuration mode, enter the forwarding instance configuration. For example:

   user@host# edit policies group group1 list list1 rule rule1 forwarding-instance

2. (Optional) Specify a forwarding instance to assign to flows matching the policy.

   user@host# edit policies group group1 list list1 rule rule1 forwarding-instance "_same_"

   Allowed values are __same__, or one of the forwarding instances configured on the router. The value __same__ forwards the flow in whatever forwarding instance it came in or is set from static configuration.

3. (Optional) Specify a forwarding unit to assign to flows matching this policy. Forwarding unit specifies the multiservice interface unit number for forward flows to in order to reach the forwarding instance specified by the attribute forwarding-instance. Note that there is only a very loose coupling between this unit number and the forwarding instance. The binding between them only happens with the aid of additional router configuration.

   [edit policies group group1 list list1 rule rule1 forwarding-instance]
   user@host# set forwarding-unit *forwarding-unit*

   Enter a value in the range 0–16384.

4. (Optional) Enter a description for the forwarding instance action.

   [edit policies group group1 list list1 rule rule1 forwarding-instance]
   user@host# set description *description*

5. (Optional) Verify the forwarding instance action configuration.

```
[edit policies group bod list input rule pr forwarding-instance]
user@host# show
"'fi1'" forwarding-instance 1 description fi-sample
```

Configuring Forwarding Class Actions (SRC CLI)

You can configure forwarding class actions for Junos OS filter policy rules. The forwarding class action causes the router to assign a forwarding class to packets that match the associated classify-traffic condition.

The type of action that you can create depends on the type of policy rule. See *Policy Information Model*.

Use the following configuration statements to configure a forwarding class action:

```
policies group name list name rule name forwarding-class {
  forwarding-class;
  description description;
}
```

To configure a forwarding class action:

1. From configuration mode, enter the forwarding class action configuration.

   user@host# edit policies group bod list input rule pr forwarding-class

2. (Optional) Configure the name of the forwarding class assigned to packets.

   [edit policies group bod list input rule pr forwarding-class]
   user@host# set *forwarding-class*

3. (Optional) Enter a description for the forwarding class action.

   [edit policies group bod list input rule pr forwarding-class]
   user@host# set description *description*

4. (Optional) Verify the forwarding class action configuration.

```
[edit policies group bod list input rule pr forwarding-class]
user@host# show
forwarding-class fc_expedited;
description "Expedited forwarding class";
```

Configuring Filter Actions (SRC CLI)

Use this action to discard packets. You can configure filter actions for Junos OS filters and JunosE policy rules. The type of action that you can create depends on the type of policy rule. See *Policy Information Model*.

Use the following configuration statement to configure a filter action:

```
policies group name list name rule name filter {
  description description ;
}
```

To configure a filter action:

1. From configuration mode, enter the filter action configuration.

   user@host# edit policies group junos_filter list in rule pr filter

2. (Optional) Enter a description for the filter action.

   [edit policies group junos_filter list in rule pr filter]
   user@host# set description *description*

3. (Optional) Verify the filter action configuration.

```
[edit policies group junos_filter list in rule pr filter]
user@host# show
description "Filter action for Junos OS policies";
```

Related Documentation

- Configuring PTSP Policies (SRC CLI) on page 33
- Configuring PTSP Policy Lists (SRC CLI) on page 36
- Configuring the PTSP Policer Instance (SRC CLI) on page 34
- Configuring PTSP Policy Rules (SRC CLI) on page 37

- Configuring PTSP Classify-Traffic Conditions (SRC CLI) on page 40

CHAPTER 8

Configuration Examples

Example: Configuring the SRC Software to Support PTSP on the MX Series Router

The following example illustrates how to configure two SAEs running on hosts *src1* and *src2* to manage packet-triggered subscriber sessions on all routing instances of an MX Series router:

```
shared {
   network {
      device mx-name {
         origin-host mx-origin-host;
         device-type junos-ptsp;
         peers mx-name-peer;
         virtual-router * {
            sae-connection [src1 src2];
         }
      }
   }
   diameter {
      peer mx-name-peer {
         address 10.0.0.1;
         port 3868;
         protocol tcp;
      }
   }
}
   policies group MXPolicy list ptsp {
      role junos-ptsp;
      applicability both;
      policer MXpolicer {
         bandwidth 100000;
         max-burst-size 10000;
      }
      rule ptsp-r1 {
         type service-rule;
         precedence 100;
```

```
        accounting;
        traffic-condition 1 {
          destination-network {
            group-network network-specifier 1.2.3.0/24;
          }
          match-direction both;
        }
        traffic-condition 2 {
          destination-network {
            group-network network-specifier 2.3.4.0/23;
          }
          match-direction input;
        }
        forwarding-instance 1 forwarding-unit 2;
      }
      rule ptsp-r2 {
        type service-rule;
        precedence 100;
        traffic-condition 1 {
          destination-network {
            group-network network-specifier 3.4.5.0/24;
          }
          match-direction both;
        }
        filter;
      }
    }
    shared {
      sae {
        group <name-of-config-group> {
          configuration {
            driver {
              junos-ptsp {
                cached-driver-expiration 600;
                keep-alive-timeout 60;
                registry-retry-interval 30;
                reply-timeout 20;
                sae-community-manager PTSPCommunityManager;
                sequential-message-timeout 20;
                session-store {
                  communications-timeout 60000;
                  disk-load-buffer-size 1000000;
                  idle-timeout 3600000;
                  load-timeout 420000;
                  maximum-backlog-ratio 1.5;
                  maximum-file-size 25000000;
                  maximum-queue-age 100;
                  maximum-queue-size 51050;
                  maximum-queued-operations 50;
                  maximum-session-size 10000;
                  minimum-backlog 5000000;
                  minimum-disk-space-usage 25;
                  network-buffer-size 51050;
                  retry-interval 300000;
                  rotation-batch-size 50;
                }
```

```
            thread-idle-timeout 60;
            thread-pool-size 200;
          }
        }
      }
    }
  }
```

The active SAE registers events from the MX Series router based on the configured origin host (mx-origin-host in the example). If the origin host is not configured, the SAE uses the device name (mx-name) instead.

Related Documentation

- Configuring PTSP on the MX Series Router on page 11
- Managing Subscriber-Level Policies on MX Series Routers Overview on page 3
- Configuring PTSP to Manage Subscriber-Level Policies on page 9
- *Managing Services on MX Series Routers Using the Diameter Application*

Example: Configuring the SRC Software to Support Both PTSP and JSRC on the MX Series Router

If you are using both the *junos-ise* device driver for the JSRC feature and the PTSP device driver, you need to configure two network device entries, one for each device driver. For example:

```
shared {
  network {
    device mx-name-ptsp {
      origin-host mx-origin-host;
      device-type junos-ptsp;
      peers mx-name-peer;
      virtual-router * {
        sae-connection [src1 src2];
      }
    }
    device mx-name-jsrc {
      origin-host mx-origin-host;
      device-type junos-ise;
      peers mx-name-peer;
      virtual-router * {
        sae-connection [src2 src3];
      }
    }
  }
  diameter {
    peer mx-name-peer {
      address 10.0.0.1;
      port 3868;
      protocol tcp;
    }
  }
}
```

In this example, the JSRC and PTSP device drivers are being used simultaneously. Notice:

- The two device entries have different names (mx-name-ptsp and mx-name-jsrc).
- Both the device entries contain the origin host attribute that matches the diameter host as configured in the MX Series router .

If the origin host is not specified, the name of the device is used instead. In other words, it is also possible to configure two entries, where the name of one entry matches the Diameter host name of the MX Series router (without origin host), and the second entry contains the origin host. For example:

```
shared network {
   device mx-origin-host { ... }
   device mx-origin-host-2 {
      origin-host mx-origin-host;
      ...
   }
}
```

Related Documentation

- Managing Subscriber-Level Policies on MX Series Routers Overview on page 3
- *Adding Network Devices (SRC CLI)*
- *Configuring JSRC on the MX Series Router*
- *Managing Services on MX Series Routers Using the Diameter Application*

CHAPTER 9

Configuration Statements and Commands

Configuration Statements for PTSP Policies (SRC CLI)

Use the following configuration statements to configure PTSP policies:

```
policies group name {
  description description ;
}
policies group name list name {
  role [(junos | junose-ipv4 | junose-ipv6 | junose-l2tp | pcmm | aaa | junos-ise | junos-ptsp)];
  applicability [(input | output | both | secondary-input)];
  description description;
}
policies group name list name rule name {
  precedence precedence;
  accounting;
  application-accounting application-accounting;
  type [(ptsp-service-rule | ptsp-subscriber-profile | ptsp-template)];
  subscriber-profile subscriber-profile;
}
policies group name list name policer name {
  bandwidth bandwidth;
  max-burst-size max-burst-size;
}
policies group name list name rule name traffic-condition name {
  match-direction match-direction;
  description description;
}
policies group name list name rule name traffic-condition name destination-network
  network {
  ip-address ip-address;
  ip-mask ip-mask;
}
policies group name list name rule name traffic-condition name destination-network
  group-network {
  network-specifier network-specifier;
}
policies group name list name rule name traffic-condition name protocol-condition {
```

```
    protocol  protocol;
}
policies group name list name rule name traffic-condition name protocol-port-condition
    {
    protocol  protocol;
}
policies group name list name rule name traffic-condition name protocol-port-condition
    destination-port port {
    from-port from-port;
}
policies group name list name rule name traffic-condition name protocol-port-condition
    source-port port {
    from-port from-port;
}
policies group name list name rule name traffic-condition name
    parameter-protocol-condition {
    protocol  protocol;
}
policies group name list name rule name traffic-condition name
    parameter-protocol-condition proto-attr destination-port port {
    from-port from-port;
}
policies group name list name rule name traffic-condition name
    parameter-protocol-condition proto-attr source-port port {
    from-port from-port;
}
policies group name list name rule name traffic-condition name tcp-condition {
    protocol  protocol;
}
policies group name list name rule name traffic-condition name tcp-condition
    destination-port port {
    from-port from-port;
}
policies group name list name rule name traffic-condition name tcp-condition
    source-port port {
    from-port from-port;
}
policies group name list name rule name traffic-condition name traffic-match-condition
    {
    term-precedence term-precedence
    application [application...];
    application-group [application-group...];
}
policies group name list name rule name policer-ref {
    policer-name;
    description  description;
}
policies group name list name rule name forwarding-instance {
    forwarding-instance;
    forwarding-unit  forwarding-unit ;
    description  description ;
}
policies group name list name rule name forwarding-class name {
    forwarding-class forwarding-class ;
    description description ;
}
```

```
policies group name list name rule name filter name {
  description description ;
}
```

Related Documentation

- Configuring PTSP Policies (SRC CLI) on page 33
- Configuring PTSP to Manage Subscriber-Level Policies on page 9
- Configuring PTSP Policy Lists (SRC CLI) on page 36
- Configuring Policy Groups (SRC CLI) on page 35
- Configuring PTSP Policy Rules (SRC CLI) on page 37
- Configuring the PTSP Policer Instance (SRC CLI) on page 34

PART 3

Index

Index

S

T