MX BNG (Diameter)

Modified: 2018-10-15

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

MX BNG (Diameter)

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 https://support.juniper.net/support/eula/. 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 https://www.juniper.net/documentation/.

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 https://www.juniper.net/books.

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;`
		`  }`

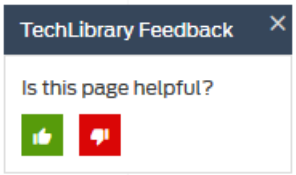
Table 3: Text Conventions (continued)

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# . . .** • https://www.juniper.net/techpubs/software/management/sdx/api-index.html
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 so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:



  - Click the thumbs-up icon if the information on the page was helpful to you.

- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.

- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software 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 Partner Support Service 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 https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://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: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: https://www.juniper.net/cm/

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

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 https://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 https://www.juniper.net/support/requesting-support.html.

PART 1

Overview

CHAPTER 1

Software Features Overview

SRC Component Overview

The SRC software is a dynamic system. It contains many components that you use to build a subscriber management environment. You can use these tools to customize and extend the SRC software for your use and to integrate the SRC software with other systems. The SRC software also provides the operating system and management tools for C Series Controllers.

Table 4 on page 3 gives a brief description of the components that make up the SRC software.

Table 4: Descriptions of SRC Components

Component	Description
Server Components	
Service activation engine (SAE)	• Authorizes, activates, and deactivates subscriber and service sessions by interacting with systems such as Juniper Networks routers, cable modem termination system (CMTS) devices, RADIUS servers, and directories. • Collects accounting information about subscribers and services from routers, and stores the information in RADIUS accounting servers, flat files, and other accounting databases. • Provides plug-ins and application programming interfaces (APIs) for starting and stopping subscriber and service sessions and for integrating with systems that authorize subscriber actions and track resource usage.
Subscriber Information Collector (SIC)	The SIC listens for RADIUS accounting events from IP edge devices (accounting clients) and forwards them to a remote AAA server, allowing the SRC software to gain increased subscriber awareness. Additionally, the SIC can optionally edit accounting events before routing them.
Network information collector (NIC)	Collects information about the state of the network and can provide a mapping from a given type of network data to another type of network data.
Redirect Server	Redirects HTTP requests received from IP Filter to a captive portal page.

Table 4: Descriptions of SRC Components (continued)

Component	Description
3GPP Gateway	The SRC Third-Generation Partnership Project (3GPP) gateway is a Diameter-based component in the SRC software, which provides integration with 3GPP Policy and Charging Control environments, to provide fixed-mobile convergence (FMC). The SRC 3GPP gateway provides Gx-based integration with the Policy and Charging Rules Function (PCRF). The SRC 3GPP gateway uses the northbound Gx interface to mediate between the PCRF and Juniper Networks routers like the E Series Broadband Services routers and MX Series routers. The northbound Gx interface on the SRC 3GPP gateway communicates with the PCRF using the Diameter protocol.
3GPP Gy	The SRC 3GPP Gy is a Diameter-based component in the SRC software, which provides Gy-based integration with the Online Charging System (OCS), to provide FMC. The SRC 3GPP Gy uses the northbound Gy interface to handle charging-related information between the OCS and Juniper Networks routers like the E Series Broadband Services routers and MX Series routers. The northbound Gy interface communicates with the OCS using the Diameter protocol.
Web Application Service	The SRC software includes a Web application server that hosts the Web Services Gateway and the Volume Tracking Application (SRC VTA). In production environments, this application server is designed to host only these applications. However, you can load your own applications into this server for testing or demonstration purposes.
Web Services Gateway	Allows a gateway client—an application that is not part of the SRC network—to interact with SRC components through a Simple Object Access Protocol (SOAP) interface. The Web Services Gateway provides the Dynamic Service Activator which allows a gateway client to dynamically activate and deactivate SRC services for subscribers and to run scripts that manage the SAE.
Repository	
Directory	The SRC software includes the Juniper Networks database, which is a built-in Lightweight Directory Access Protocol (LDAP) directory for storing all SRC data including services, policies, and small subscriber databases. For large subscriber databases, you must supply your own directory.
SRC Configuration and Management Tools	
SRC command line interface (CLI)	Provides a way to configure the SRC software on a C Series Controller from a Junos OS–like CLI. The SRC CLI includes the policies, services, and subscribers CLI, which has separate access privileges.
C-Web interface	Provides a way to configure, monitor, and manage the SRC software on a C Series Controller through a Web browser. The C-Web interface includes a policies, services, and subscribers component, which has separate access privileges.
Simple Network Management Protocol (SNMP) agent	Monitors system performance and availability. It runs on all the SRC hosts and makes management information available through SNMP tables and sends notifications by means of SNMP traps.
Service Management Applications (Run on external system)	
IMS Services Gateway	Integrates into an IP multimedia system (IMS) environment. The SRC software provides a Diameter protocol-based interface that allows the SRC software to integrate with services found on the application layer of IMS.

Table 4: Descriptions of SRC Components (continued)

Component	Description
SRC Programming Interfaces	
NETCONF API	Allows you to configure or request information from the NETCONF server on a C Series Controller that runs the SRC software. Applications developed with the NETCONF API run on a system other than a C Series Controller.
CORBA plug-in service provider interface (SPI)	Tracks sessions and enables linking the rest of the service provider's operations support system (OSS) with the SRC software so that the OSS can be notified of events in the life cycle of SAE sessions. Hosted plug-ins only.
CORBA remote API	Provides remote access to the SAE core API. Applications that use these extensions to the SRC software run on a system other than a C Series Controller.
NIC access API	Performs NIC resolutions. Applications that use these extensions to the SRC software run on a system other than a C Series Controller.
SAE core API	Controls the behavior of the SRC software. Applications that use these extensions to the SRC software run on a system other than a C Series Controller.
Script services	Provides an interface to call scripts that supply custom services such as provisioning policies on a number of systems across a network.
VTA API	The Volume Tracking Application (VTA) API is a Simple Object Access Protocol (SOAP) interface that allows developers to create gateway clients and that administrators use to manage VTA subscribers and sessions. The SRC Web Services Gateway allows a gateway client—an application that is not part of the SRC network—to interact with SRC components, such as the VTA, through a SOAP interface.
Authorization and Accounting Applications	
AAA RADIUS servers	Authenticates subscribers and authorizes their access to the requested system or service. Accepts accounting data—time active and volume of data sent—about subscriber and service sessions. RADIUS servers run on a system other than a C Series Controller.
SRC Admission Control Plug-In (SRC ACP)	Authorizes and tracks subscribers' use of network resources associated with services that the SRC application manages.
Flat file accounting	Stores tracking data to accounting flat files that can be made available to external systems that send the data to a rating and billing system.
Volume Tracking Application	The SRC Volume Tracking Application (SRC VTA) is an SRC component that allows service providers to track and control the network usage of subscribers and services. You can control volume and time usage on a per-subscriber or per-service basis. This level of control means that service providers can offer tiered services that use volume as a metric, while also controlling abusive subscribers and applications. When a subscriber or service exceeds bandwidth limits (or quotas), the SRC VTA can take actions including imposing rate limits on traffic, sending an e-mail notification, or charging extra for additional bandwidth consumed.
Demonstration Applications (available on the Juniper Networks Website)	

Table 4: Descriptions of SRC Components (continued)

Component	Description
Enterprise Audit Plug-In	Defines a callback interface, which receives events when IT managers complete specified operations.
Enterprise Manager Portal	Allows service providers to provision services for enterprise subscribers on routers running JunosE or Junos OS and allows IT managers to manage services. Enterprise Manager Portal can be used with NAT Address Management Portal to allow service providers to manage public IP addresses for use with NAT services on routers running Junos OS and to all IT managers to make requests about public IP addresses through the Enterprise Manager Portal.
Monitoring Agent application	Integrates IP address managers, such as a DHCP server or a RADIUS server, into an SRC-managed network so that the SAE is notified about subscriber events. The Monitoring Agent application runs on a Solaris platform.
Residential service selection portals	Provides a framework for building Web applications that allow residential and enterprise subscribers to manage their own network services. It comes with several full-featured sample Web applications that are easy to customize and suitable for deployment. The Residential service selection portals run on a Solaris platform.
Sample enterprise service portal	Lets service providers supply an interface to their business customers for managing and provisioning services.

Related Documentation

- *SRC Product Description*

CHAPTER 2

Services with Diameter on MX Series Routers

SRC Peer Support on MX Series Routers Overview

When the Juniper Networks routing platform supports the use of the Diameter protocol to provide extended authentication, authorization, and accounting (AAA) functionality, the SRC software can dynamically manage services on these devices. The SRC software uses the Diameter protocol for communications between the local SRC peer on a Juniper Networks routing platform, such as the Juniper Networks MX Series Ethernet Services Router, and the service activation engine (SAE). The local SRC peer is known as Junos OS (JSRC) and is part of the AAA application.

JSRC has the following responsibilities:

- Request address authorization from the SAE.
- Request service activations from the SAE.
- Activate and deactivate services as specified by the SAE.
- Log out subscribers as specified by the SAE.
- Update the SAE with status of new service activations and deactivations.
- Synchronize subscriber state and service information with the SAE.
- Notify the SAE when subscribers log out.

The SRC software enables the SAE to activate and deactivate subscriber services and log out subscribers. The SAE can control only those resources that have been provisioned through the SAE. Therefore, the SAE receives information about only those subscribers for whom JSRC has requested provisioning from the SAE. Similarly, the SAE can control only the subscriber services that it has activated.

Related Documentation

- Managing Services on MX Series Routers Using the Diameter Application on page 15
- Configuring JSRC on the MX Series Router on page 13
- Configuring the SAE to Manage Network Devices (SRC CLI) on page 27

- Configuring Diameter Peers (SRC CLI) on page 22

CHAPTER 3

Subscriber Sessions on MX Series Routers

Subscriber Sessions on MX Series Routers Overview

The SRC software can manage subscriber sessions on MX Series routers. Common types of subscriber sessions on MX Series routers include:

- One interface subscriber session for each statically configured virtual local area network (VLAN).
- One address subscriber session for each Dynamic Host Configuration Protocol (DHCP) address.

You can manage subscriber sessions with the External Subscriber Monitor application and the change-of-authorization (COA) script service. You can use External Subscriber Monitor to authorize access requests from the MX Series router and to log in or log out authorized subscribers. You can use the pseudo-RADIUS authorization server in External Subscriber Monitor to limit the number of DHCP leases for a subscriber by specifying the interface-name attribute in the subscriber profile and then setting a parameter substitution for the dhcpLeaseLimit parameter for that interface. You can configure the COA script service to dynamically activate or deactivate services on the MX Series router. This method uses RADIUS attributes and RADIUS vendor-specific attributes (VSAs) to identify a subscriber session whose services are to be activated or deactivated.

Related Documentation

- Configuring External Subscriber Monitor (SRC CLI) on page 39
- Setting Up MX Series Routers in the SRC Network (SRC CLI) on page 25

PART 2

Configuration

CHAPTER 4

Configuration Tasks to Set Up JSRC on the MX Series Router

Configuring JSRC on the MX Series Router

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

1. Configure the Diameter instance.

   See "Configuring the Diameter Application (SRC CLI)" on page 16.

2. Set up the MX Series router so that it can be managed by the SAE.

   See "Adding Network Devices (SRC CLI)" on page 26

3. Configure the Diameter peer.

   See "Configuring Diameter Peers (SRC CLI)" on page 22.

4. Configure the SAE to manage the MX Series router.

   See "Configuring the SAE to Manage Network Devices (SRC CLI)" on page 27.

5. Configure JSRC policies.

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

For more information about JSRC and subscriber access, see the *Junos OS Broadband Subscriber Management and Services Library*.

CHAPTER 5

Configuration Tasks for the Diameter Application

Managing Services on MX Series Routers Using the Diameter Application

You can use the SRC software to manage services on Juniper Networks routing platforms using the Diameter protocol. The SRC software communicates with the local SRC peer on the device using Diameter messages to dynamically manage services for a subscriber session.

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

- AA-Request (AAR)—Attach subscriber to access network
- Accounting-Request (ACR)—Provide accounting information
- Abort-Session-Request (ASR)—Disconnect subscriber
- Push-Profile-Request (PPR)—Start, modify, or stop service session
- Session-Resource-Query (SRQ)—Initiate synchronization
- Session-Termination-Request (STR)—Detach subscriber from access network

You configure the Diameter peers and a device for each device managed by the SAE. The Diameter server searches all devices of type junos-ise for virtual routers that include the local host in their SAE connections. For these devices, the Diameter server establishes a connection with the peers referenced in the device configuration.

Tasks to set up the management of services on devices using Diameter protocol:

- Configuring JSRC on the MX Series Router on page 13
- Configuring the Diameter Application (SRC CLI) on page 16

- Adding Network Devices (SRC CLI) on page 26
- Configuring Diameter Peers (SRC CLI) on page 22
- Configuring the SAE to Manage Network Devices (SRC CLI) on page 27
- Configuring JSRC Policies (SRC CLI) on page 33

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 on page 16
- Configuring the Diameter Client Properties on page 20
- Configuring the Diameter Server Properties on page 20
- Configuring Logging Destinations on page 21

Configuring the Diameter Application Properties

The SRC software supports Diameter application properties such as Juniper Networks Session Resource Control (JSRC) and southbound Gx interface. JSRC and southbound Gx interface communicate with the Service Activation Engine (SAE) (remote SRC peer).

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.

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.
- If the peer connection is configured to be in active mode, you must configure the remote peer address for all Diameter peers by using the **address** option under the **[edit shared network diameter peer *name*]** hierarchy.

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
   ```

See Also

- Configuring the Diameter Server Properties on page 20
- Configuring Logging Destinations on page 21

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
```

See Also

- Configuring the Diameter Client Properties on page 20
- Configuring Logging Destinations on page 21

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 on page 57
- To manage services for JSRC peers on MX Series routers, see Managing Services on MX Series Routers Using the Diameter Application on page 15.

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;
}
```

NOTE: When you commit the Diameter peer configuration, keep in mind the following conditions:

- The origin host, remote peer address, or both should be specified for the Diameter peer.
- If the enforce source address is configured for the Diameter peer, the remote peer address should be specified for the Diameter peer.
- If the peer connection is configured to be in active mode for a particular Diameter peer or globally for all Diameter peers by using the **active-peers** option under the **[edit system diameter]** hierarchy, the remote peer address should be specified for the Diameter peers.

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. (Optional) 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 16
- Viewing SRC Diameter Server State (SRC CLI) on page 63

CHAPTER 6

Configuration Tasks for the SAE

Setting Up MX Series Routers in the SRC Network (SRC CLI)

To set up the MX Series router so that the router can be managed by the SAE:

1. From configuration mode, access the configuration statement that configures network devices. This sample procedure uses mx_device as the name of the router.

   ```
   user@host# edit slot 0 shared network device mx_device
   ```

2. Set the type of device to third-party.

   ```
   [edit shared network device mx_device]
   user@host# set device-type third-party
   ```

3. From configuration mode, access the configuration statements for virtual routers. For MX Series routers, use the name default for the virtual router.

   ```
   [edit shared network device mx_device]
   user@host# edit virtual-router default
   ```

4. Specify the addresses of SAEs that can manage this router.

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

Related Documentation

- Configuring External Subscriber Monitor (SRC CLI) on page 39
- Configuring Pseudo–RADIUS Authorization Server Properties (SRC CLI) on page 40

- Configuring the COA Script Service for MX Series Routers (SRC CLI) on page 53
- Configuring Subscriptions to the Script Service on page 56

Adding Network Devices (SRC CLI)

To set up the MX Series router so that it can be managed by the SAE:

1. From configuration mode, access the statements that configure network devices. This sample procedure uses mx1 as the name of the router.

   ```
   user@host# edit shared network device mx1
   ```

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

   ```
   [edit shared network device mx1]
   user@host# set device-type junos-ise
   ```

3. (Optional) Specify the origin hostname. This example procedure uses mx1-origin-host as the origin hostname. If the origin hostname is not configured, SAE uses the device name (mx1 in the example) as the origin hostname. If configured, the mentioned origin hostname must match the origin hostname of the Diameter peer (for example, MX Series router).

   ```
   [edit shared network device mx1]
   user@host# set origin-host mx1-origin-host
   ```

   NOTE: If the origin hostname is configured under the **[edit shared network device *name*]** hierarchy, the device name does not need to be same as the origin hostname of the Diameter peer. Otherwise, the device name must match the origin hostname of the Diameter peer.

4. Specify the configured peers associated with the device. See "Configuring Diameter Peers (SRC CLI)" on page 22.

   ```
   [edit shared network device mx1]
   user@host# set peers [peers...]
   ```

   NOTE: MX Series routers support only a single peer connection.

5. From configuration mode, access the statements for virtual routers. The name must match the JSRC 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 mx1]
   user@host# edit virtual-router *
   ```

where * matches any JSRC partition. You can also specify that the JSRC 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 mx1 virtual-router default]
user@host# set sae-connection [sae-connection...]
```

7. (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 mx1 virtual-router default]
user@host# set vpn-id (vpn-id | VRF)
```

8. (Optional) Verify your configuration.

```
[edit shared network device mx1]
user@host# show
device-type junos-ise;
origin-host mx1-origin-host;
peers bng-srcmx480b;
virtual-router * {
  sae-connection 10.212.10.2;
  vpn-id 123;
}
```

Related Documentation

- Configuring the SAE to Manage Network Devices (SRC CLI) on page 27
- Configuring JSRC on the MX Series Router on page 13

Configuring the SAE to Manage Network Devices (SRC CLI)

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

```
shared sae configuration driver junos-ise {
  sae-community-manager sae-community-manager;
  pool-retrieval;
  sync-from-sessionstore;
  ignore-framed-ip-netmask;
  cached-driver-expiration cached-driver-expiration;
  concurrent-post-sync-jobs concurrent-post-sync-jobs;
  concurrent-request-timeout concurrent-request-timeout;
  concurrent-requests concurrent-requests ;
  enable-disconnect-ontimeout;
  delay-service-policy-provisioning delay-service-policy-provisioning
  keep-alive-timeout keep-alive-timeout;
  pending-acrs-strs-wait-time pending-acrs-strs-wait-time;
  registry-retry-interval registry-retry-interval;
```

```
    reply-timeout reply-timeout;
    sequential-message-timeout sequential-message-timeout;
    sync-count-wait-timeout sync-count-wait-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-ise
   ```

2. Specify the name of the community manager.

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

3. (Optional) Specify the pool retrieval option.

   ```
   [edit shared sae configuration driver junos-ise]
   user@host# set pool-retrieval
   ```

4. (Optional) Specify whether the SAE should be synchronized from the session store.

   ```
   [edit shared sae group POP-ID configuration driver junos-ise]
   user@host# set sync-from-sessionstore
   ```

5. (Optional) Specify whether to ignore the Framed-IP-Mask AVP and allow IP-based filtering without considering the framed IP netmask.

   ```
   [edit shared sae group POP-ID configuration driver junos-ise]
   user@host# set ignore-framed-ip-netmask
   ```

6. (Optional) Specify the number of jobs that can be processed concurrently to log in to subscriber sessions that are incomplete after synchronizing state with the router. You can configure a value ranging from 10 through 50. Default value is 20.

   ```
   [edit shared sae configuration driver junos-ise]
   user@host# set concurrent-post-sync-jobs concurrent-post-sync-jobs
   ```

7. (Optional) Specify the timeout for sending concurrent requests. You can configure a value ranging from 0 through 900 seconds. Default value is 30 seconds.

   ```
   [edit shared sae configuration driver junos-ise]
   user@host# set concurrent-request-timeout concurrent-request-timeout
   ```

8. (Optional) Specify the number of unsolicited requests that can be sent concurrently. You can configure a value ranging from 1 through 500. Default value is 100.

```
[edit shared sae configuration driver junos-ise]
user@host# set concurrent-requests concurrent-requests
```

9. (Optional) Specify whether the user session needs to be removed from the router.

```
[edit shared sae configuration driver junos-ise]
user@host# set enable-disconnect-ontimeout
```

10. (Optional) Specify the amount of time by which scheduler tasks are delayed after the user login is completed. You can configure a value ranging from 0 through 1000 milliseconds. Default value is 0.

```
[edit shared sae configuration driver junos-ise]
user@host# set delay-service-policy-provisioning delay-service-policy-provisioning
```

11. (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-ise]
user@host# set cached-driver-expiration cached-driver-expiration
```

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

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

13. (Optional) Specify the maximum time that the device driver waits for completing sessions restoration to start processing pending Accounting-Request (ACR) and Session-Termination-Request (STR) messages. You can configure a value ranging from 600 through 18000 seconds. Default value is 3600 seconds.

```
[edit shared sae configuration driver junos-ise]
user@host# set pending-acrs-strs-wait-time pending-acrs-strs-wait-time
```

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

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

15. (Optional) Specify the timeout before a request sent to a Diameter server expires.

```
[edit shared sae configuration driver junos-ise]
```

```
user@host# set reply-timeout reply-timeout
```

16. (Optional) Specify the timeout before an expected message expires.

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

17. (Optional) Specify the interval after which SAE stops waiting for the sync-AAR messages and triggers unsolicited synchronization. You can configure a value ranging from 0 through 20132147483647 seconds. Default value is 2 seconds.

```
[edit shared sae configuration driver junos-ise]
user@host# set sync-count-wait-timeout sync-count-wait-timeout
```

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

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

19. (Optional) Specify the timeout for stopping working threads after they become idle.

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

20. (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-ise session-store
```

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

Related Documentation

- Adding Network Devices (SRC CLI) on page 26
- Configuring the Diameter Application (SRC CLI) on page 16
- *Configuring Local Properties for the SAE (SRC CLI)*
- SRC Peer Support on MX Series Routers Overview on page 7

Specifying Initialization Scripts for the Intelligent-Service-Edge Device Driver (SRC CLI)

Use the following configuration statements to specify initialization scripts for the intelligent-service-edge device driver:

```
shared sae configuration driver scripts {
   extension-path extension-path;
   general general;
   junos-ise junos-ise;
}
```

To configure initialization scripts for the intelligent-service-edge device driver:

1. From configuration mode, access the configuration statements that configure initialization scripts. In this sample procedure, the scripts are configured in the west-region group.

   ```
   user@host# edit shared sae group west-region configuration driver scripts
   ```

2. Specify the initialization script for the intelligent-service-edge device driver.

   ```
   [edit shared sae group west-region configuration driver scripts]
   user@host# set junos-ise junos-ise
   ```

   SAE runs the specified script when the intelligent-service-edge device driver is activated and again when the driver is deactivated.

3. Configure the initialization script that can be used for all other types of routers supported by the SRC module.

   ```
   [edit shared sae group west-region configuration driver scripts]
   user@host# set general general
   ```

4. Configure a path to initialization scripts that are not in the default location, */opt/UMC/sae/lib*.

   ```
   [edit shared sae group west-region configuration driver scripts]
   user@host# set extension-path extension-path
   ```

5. (Optional) From operational mode, verify your initialization script configuration.

   ```
   [edit shared sae group west-region configuration driver scripts]
   user@host# show
   junos-ise isePoolPublisher;
   ```

Related Documentation

- *Copying Initialization Scripts to the C Series Controller*
- *Developing Router Initialization Scripts for Network Devices and Juniper Networks Routers*

CHAPTER 7

Configuration Tasks for JSRC Policies

Configuring JSRC Policies (SRC CLI)

Tasks to configure JSRC policies are:

Configuring JSRC Policy Lists

To configure policy lists:

1. From configuration mode, create a policy list. For example, to create a policy list called l1 within a policy group called ise:

   ```
   user@host# edit policies group ise list l1
   ```

2. Specify the type of policy list.

   ```
   [edit policies group ise list l1]
   user@host# set role junos-ise
   ```

3. Specify where the policy is applied on the device.

   ```
   [edit policies group ise list l1]
   user@host# set applicability both
   ```

Configuring JSRC Policy Rules

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 r1 within policy list l1:

```
user@host# edit policies group ise list l1 rule r1
```

2. Specify the type of policy rule.

```
[edit policies group ise list l1 rule r1]
user@host# set type junos-ise
```

Configuring Dynamic Profile Actions

Use this action to install existing dynamic profiles. You can configure dynamic profile actions for devices such as the MX Series routers.

The profile name must match a dynamic profile configured on the device and the variable name must match a variable configured for the dynamic profile.

Use the following configuration statements to configure a dynamic profile action:

```
policies group name list name rule name dynamic-profile name {
   profile-name profile-name;
   description description;
}
```

```
policies group name list name rule name dynamic-profile name variables name {
   value value;
   type type;
}
```

To configure a dynamic profile action:

1. From configuration mode, enter the dynamic profile action configuration. In this sample procedure, dp is the name of the dynamic profile action.

```
user@host# edit policies group ise list l1 rule r1 dynamic-profile dp
```

2. Enter the profile name to activate.

```
[edit policies group ise list l1 rule r1 dynamic-profile dp]
user@host# set profile-name profile-name
```

3. (Optional) Enter a description for the dynamic profile action.

```
[edit policies group ise list l1 rule r1 dynamic-profile dp]
user@host# set description description
```

4. From configuration mode, enter the parameters used by the profile.

```
user@host# edit policies group ise list l1 rule r1 dynamic-profile dp variables name
```

For example:

```
user@host# edit policies group ise list l1 rule r1 dynamic-profile dp variables
  upstreamBandwidth
```

5. (Optional) Configure the value for the variable.

```
[edit policies group ise list l1 rule r1 dynamic-profile dp variables name]
user@host# set value value
```

For example:

```
[edit policies group ise list l1 rule r1 dynamic-profile dp variables upstreamBandwidth]
user@host# set value rateParameter
```

6. (Optional) Configure the variable type. Variable types are mapped to parameter types.

```
[edit policies group ise list l1 rule r1 dynamic-profile dp variables name]
user@host# set type type
```

For example:

```
[edit policies group ise list l1 rule r1 dynamic-profile dp variables upstreamBandwidth]
user@host# set type rate
```

For more information about dynamic profiles and subscriber access, see the *Junos OS Broadband Subscriber Management and Services Library*.

See Also

- Configuring JSRC on the MX Series Router on page 13

Configuring Operation Script for Policy Provisioning (SRC CLI)

You can use operation scripts to support the policy provisioning for JSRC policy rules. The SRC software passes the operation script values configured by using the **operation-script** option under the **[edit policies group *name* list *name* rule *name*]** hierarchy level to the Extensible Subscriber Services Manager Daemon on the MX Series router. You can assign the operation script only to the rules for which the role of the policy list is set as **junos-ise** and the **applicability** is set as **both**.

NOTE:

- AA-Answer message can have both dynamic profile and operation script in the policy rule, whereas the Push-Profile-Request can have either dynamic profile or operation script in the policy rule.
- In the policy rule configuration, the **dynamic-profile** and **operation-script** options are mutually exclusive.

Use the following configuration statements to configure an operation script for JSRC policy rules:

```
policies group name list name rule name operation-script{
   description description;
   script-name script-name;
   script-args-format script-args-format ;
}
policies group name list name rule name operation-script variables name {
   value value;
   type type;
}
```

To configure an operation script for JSRC policy rules:

1. From configuration mode, enter the operation script configuration.

   ```
   [edit policies group name list name rule name]
   user@host# set operation-script
   ```

2. (Optional) Enter a description for the operation script.

   ```
   [edit policies group name list name rule name operation-script]
   user@host# set description description
   ```

3. Enter a name for the operation script.

   ```
   [edit policies group name list name rule name operation-script]
   user@host# set script-name script-name
   ```

4. Enter the operation script arguments.

```
[edit policies group name list name rule name operation-script]
user@host# set script-args-format script-args-format
```

   Use the format *'$[arg1];$[arg2];$[arg3]'*.

   For example: **'$[user_ipAddress];[vlan]';**

   NOTE:
   - You must enclose the arguments in quotation marks.
   - The operation script argument name must match a variable name configured for policy provisioning.

5. From configuration mode, enter the parameters used by the operation script for policy provisioning.

```
[edit]
user@host# set policies group name list name rule name operation-script variables
  name]
```

6. (Optional) Configure a value for the variable.

```
[edit policies group name list name rule name operation-script variables name]
user@host# set value value
```

7. (Optional) Configure the variable type. Variable types are mapped to parameter types.

```
[edit policies group name list name rule name operation-script variables name]
user@host# set type type
```

8. (Optional) Verify the operation script configuration.

```
[edit policies group name list name rule name
   user@host# show
    operation-script {
      script-args-format '$[user_ipAddress];$[vlan]';
    script-name ngcoco;
     variables {
         var1 {
           type any;
           value user_ipAddress;
       }
     var2 {
           type any;
           value vlan;
       }
       }
  }
 type junos-ise;
```

See Also

- *Configuring Dynamic Profile Actions (SRC CLI)*
- *Policy Rules Overview*

Related Documentation

- Configuring JSRC on the MX Series Router on page 13
- *Policy Rules Overview*

CHAPTER 8

Configuration Tasks for Managing Subscriber Sessions Using External Subscriber Monitor Application

Configuring External Subscriber Monitor (SRC CLI)

Use External Subscriber Monitor to log in and log out authorized subscribers and to provide interim updates for authorized subscribers.

To configure External Subscriber Monitor as a pseudo–RADIUS accounting server:

1. From configuration mode, access the configuration statement that configures the local properties.

   ```
   user@host# edit slot 0 external-subscriber-monitor
   ```

2. Configure the local properties for External Subscriber Monitor.

   If you are configuring the pseudo–RADIUS authorization server, specify the **include-mac-address** and **include-interface-name** options when configuring External Subscriber Monitor so that the MAC address and interface name attributes are included in the event notifications sent to the SAE.

   ```
   [edit slot 0 external-subscriber-monitor]
   user@host# set ?
   ```

For more information about configuring External Subscriber Monitor, see *Configuring External Subscriber Monitor (SRC CLI)*.

Related Documentation

- Configuring Pseudo–RADIUS Authorization Server Properties (SRC CLI) on page 40
- Configuring the NIC Proxy for the Pseudo-RADIUS Authorization Server (SRC CLI) on page 46
- Extracting RADIUS Attributes with the Pseudo–RADIUS Authorization Server (SRC CLI) on page 49
- Setting Up MX Series Routers in the SRC Network (SRC CLI) on page 25

Configuring Pseudo–RADIUS Authorization Server Properties (SRC CLI)

Tasks to configure the pseudo–RADIUS authorization server are:

- Configuring the Pseudo–RADIUS Authorization Server (SRC CLI) on page 40
- Configuring the Directory Connection Properties for the Subscriber Data on page 43
- Configuring Directory Connection Properties for the Cached DHCP Profiles on page 44

Configuring the Pseudo–RADIUS Authorization Server (SRC CLI)

Use the following configuration statements to configure the pseudo–RADIUS authorization server:

```
slot number external-subscriber-monitor radius-authorization {
   port port;
   local-address local-address;
   check-lease-limit-with-sae;
   query-cached-dhcp-profile;
   default-lease-limit default-lease-limit;
   invalid-pool-name invalid-pool-name;
   lease-time-limit lease-time-limit;
   cleanup-interval cleanup-interval;
   maximum-age maximum-age;
   minimum-pool-size minimum-pool-size;
   maximum-queue-length maximum-queue-length;
   service-type (all | login | framed | callback-login | callback-framed | outbound |
      administrative | nas-prompt | authenticate-only | callback-nas-prompt | callback-check
      | callback-administrative);
}
slot number external-subscriber-monitor radius-authorization client client-address {
   secret secret;
}
```

To configure the pseudo–RADIUS authorization server:

1. From configuration mode, access the configuration statement that configures the pseudo–RADIUS authorization server.

   ```
   user@host# edit slot 0 external-subscriber-monitor radius-authorization
   ```

2. Specify the listening port for RADIUS requests.

```
[edit slot 0 external-subscriber-monitor radius-authorization]
user@host# set port port
```

3. (Optional) Specify the host address to bind to the pseudo–RADIUS authorization server. Absence (or deletion) of this attribute means binding it to a wildcard (*) address.

```
[edit slot 0 external-subscriber-monitor radius-authorization]
user@host# set local-address local-address
```

4. (Optional) Specify whether to query the SAE for the number of active subscribers for a given interface. If set to true, the response to the RADIUS access request depends on the comparison between the number of active subscriber sessions and the lease limit for the interface. If the number of active subscriber sessions is less than the lease limit, the response is the RADIUS access accept message without the lease limit RADIUS attribute; otherwise, the response is the RADIUS access accept message where the subscriber is not assigned an address. If set to false, the response is the RADIUS access accept message with the lease limit RADIUS attribute. If the lease limit RADIUS vendor-specific attribute is returned, the MX Series router verifies the lease limit.

```
[edit slot 0 external-subscriber-monitor radius-authorization]
user@host# set check-lease-limit-with-sae
```

5. (Optional) Specify whether to search for a cached DHCP profile in the o=AuthCache directory based on the MAC address. If set to true, you must configure a directory connection to the cached DHCP profiles.

   If set to true, the following conditions apply:

   - If a cached DHCP profile is found, the RADIUS response message includes the RADIUS attribute values for framed IP address, pool name, service bundle, and RADIUS class attributes that are present in the cached DHCP profile.
   - If the **check-lease-limit-with-sae** option is set to true and the number of active subscriber sessions is less than the lease limit, the RADIUS access accept message includes the cached DHCP profile.
   - If the **check-lease-limit-with-sae** option is set to false, the RADIUS response includes the lease limit.

   If set to false, the RADIUS response message does not include the cached DHCP profile information.

```
[edit slot 0 external-subscriber-monitor radius-authorization]
user@host# set query-cached-dhcp-profile
```

6. (Optional) Specify the default lease limit for all interfaces.

```
[edit slot 0 external-subscriber-monitor radius-authorization]
user@host# set default-lease-limit default-lease-limit
```

7. Specify the invalid pool name returned when the number of active subscriber sessions exceeds the lease limit.

```
[edit slot 0 external-subscriber-monitor radius-authorization]
user@host# set invalid-pool-name invalid-pool-name
```

8. (Optional) Specify the timeout of a cached authenticated request.

```
[edit slot 0 external-subscriber-monitor radius-authorization]
user@host# set lease-time-limit lease-time-limit
```

9. Specify the amount of time to wait before cleaning up cached RADIUS access requests that have been accepted.

```
[edit slot 0 external-subscriber-monitor radius-authorization]
user@host# set cleanup-interval cleanup-interval
```

10. Specify the maximum age of an unacknowledged RADIUS access request cached in memory. We recommend a value slightly greater than the RADIUS packets retry interval.

```
[edit slot 0 external-subscriber-monitor radius-authorization]
user@host# set maximum-age maximum-age
```

11. Specify the minimum number of concurrent threads processing RADIUS access messages subtasks.

```
[edit slot 0 external-subscriber-monitor radius-authorization]
user@host# set minimum-pool-size minimum-pool-size
```

12. Specify the maximum number of unacknowledged RADIUS messages to be received from the RADIUS server before it discards new messages.

```
[edit slot 0 external-subscriber-monitor radius-authorization]
user@host# set maximum-queue-length maximum-queue-length
```

13. Specify the service type of the RADIUS packets that will be forwarded.

```
[edit slot 0 external-subscriber-monitor radius-authorization]
user@host# set service-type service-type
```

14. (Optional) Verify your configuration.

```
[edit slot 0 external-subscriber-monitor radius-authorization]
user@host# show
```

15. Access the configuration statement that specifies the trusted RADIUS clients.

```
[edit slot 0 external-subscriber-monitor radius-authorization]
user@host# edit client client-address
[edit slot 0 external-subscriber-monitor radius-authorization client client-address]
```

16. Specify the RADIUS shared secret for the client.

```
[edit slot 0 external-subscriber-monitor radius-authorization client client-address]
user@host# set secret secret
```

Configuring the Directory Connection Properties for the Subscriber Data

The subscriber data can be queried for information such as the interface's lease limit.

Use the following statements to configure the directory connection to the directory in which the subscriber data is stored:

```
slot number external-subscriber-monitor radius-authorization ldap subscriber-data {
   base base;
   base-dn base-dn;
}
slot number external-subscriber-monitor radius-authorization ldap subscriber-data
   directory-connection {
   url url;
   principal principal;
   credentials credentials;
   protocol (ldaps);
   backup-urls [backup-urls...];
   timeout timeout;
   check-interval check-interval;
   blacklist;
   snmp-agent;
   signature-dn signature-dn;
}
```

To configure directory connection properties:

1. From configuration mode, access the configuration statement that configures the directory connection.

```
user@host# edit slot 0 external-subscriber-monitor radius-authorization ldap
   subscriber-data
```

2. Specify the top-level directory DN.

```
[edit slot 0 external-subscriber-monitor radius-authorization ldap subscriber-data]
user@host# set base base
```

3. Specify the subtree in the directory in which the subscriber data is stored.

```
[edit slot 0 external-subscriber-monitor radius-authorization ldap subscriber-data]
user@host# set base-dn base-dn
```

4. Access the configuration statement that configures the directory connection properties.

```
[edit slot 0 external-subscriber-monitor radius-authorization ldap subscriber-data]
user@host# edit directory-connection
```

5. Specify the directory connection properties for the subscriber data.

```
[edit slot 0 external-subscriber-monitor radius-authorization ldap subscriber-data
   directory-connection]
user@host# set ?
```

6. (Optional) Verify your configuration.

```
[edit slot 0 external-subscriber-monitor radius-authorization ldap subscriber-data]
user@host# show
```

Configuring Directory Connection Properties for the Cached DHCP Profiles

The DHCP profiles can be queried by MAC address for the RADIUS framed IP address for authorized subscribers or invalid pool name for unauthorized subscribers.

Use the following statements to configure the directory connection to the directory in which the cached DHCP profiles are stored:

```
slot number external-subscriber-monitor radius-authorization ldap cached-dhcp-profile
   {
   base base;
   base-dn base-dn;
}
slot number external-subscriber-monitor radius-authorization ldap cached-dhcp-profile
   directory-connection {
   url url;
   principal principal;
   credentials credentials;
   protocol (ldaps);
   backup-urls [backup-urls...];
   timeout timeout;
   check-interval check-interval;
   blacklist;
   snmp-agent;
   signature-dn signature-dn;
```

```
}
```

To configure directory connection properties:

1. From configuration mode, access the configuration statement that configures the directory connection.

   ```
   user@host# edit slot 0 external-subscriber-monitor radius-authorization ldap
     cached-dhcp-profile
   ```

2. Specify the top-level directory DN.

   ```
   [edit slot 0 external-subscriber-monitor radius-authorization ldap cached-dhcp-profile]
   user@host# set base base
   ```

3. Specify the subtree in the directory in which the cached DHCP profiles are stored.

   ```
   [edit slot 0 external-subscriber-monitor radius-authorization ldap cached-dhcp-profile]
   user@host# set base-dn base-dn
   ```

4. Access the configuration statement that configures the directory connection properties.

   ```
   [edit slot 0 external-subscriber-monitor radius-authorization ldap cached-dhcp-profile]
   user@host# edit directory-connection
   ```

5. Specify the directory connection properties for the cached DHCP profiles.

   ```
   [edit slot 0 external-subscriber-monitor radius-authorization ldap cached-dhcp-profile
     directory-connection]
   user@host# set ?
   ```

6. (Optional) Verify your configuration.

   ```
   [edit slot 0 external-subscriber-monitor radius-authorization ldap cached-dhcp-profile]
   user@host# show
   ```

Related Documentation

- Configuring External Subscriber Monitor (SRC CLI) on page 39
- Configuring the NIC Proxy for the Pseudo-RADIUS Authorization Server (SRC CLI) on page 46
- Extracting RADIUS Attributes with the Pseudo–RADIUS Authorization Server (SRC CLI) on page 49
- Enabling the Pseudo-RADIUS Authorization Server (SRC CLI) on page 52
- Viewing Statistics for the Pseudo–RADIUS Authorization Server (SRC CLI) on page 61
- Monitoring Statistics for the Pseudo–RADIUS Authorization Server (SRC CLI) on page 64

Configuring the NIC Proxy for the Pseudo-RADIUS Authorization Server (SRC CLI)

When the **check-lease-limit-with-sae** option is set to true, you must configure the NIC proxy so that the pseudo-RADIUS authorization server can find the SAE managing the interface and determine the number of subscriber sessions already established on the interface (that is, the number of leases on the interface). The NIC proxy must be configured for a NIC scenario that maps VRs to SAEs.

Tasks to configure the NIC proxy are:

- Configuring Resolution Information for a NIC Proxy on page 46
- Changing the Configuration for the NIC Proxy Cache on page 47
- Configuring a NIC Proxy for NIC Replication on page 47

Configuring Resolution Information for a NIC Proxy

Use the following configuration statements to configure the NIC proxy:

```
slot number external-subscriber-monitor nic-proxy-configuration radius-authorization-nic
  resolution {
  resolver-name resolver-name;
  constraints constraints;
}
```

To configure resolution information for a NIC proxy:

1. From configuration mode, access the configuration statement that configures the NIC proxy configuration. In this sample procedure, the NIC proxy called radius-authorization-nic is configured.

   ```
   user@host# edit slot 0 external-subscriber-monitor nic-proxy-configuration
     radius-authorization-nic resolution
   ```

2. Specify the resolution information for this NIC proxy.

   ```
   [edit slot 0 external-subscriber-monitor nic-proxy-configuration radius-authorization-nic
     resolution]
   user@host# set ?
   ```

   For more information about configuring resolution information for a NIC proxy, see *Configuring Resolution Information for a NIC Proxy (SRC CLI)*.

3. (Optional) Verify your configuration.

   ```
   [edit slot 0 external-subscriber-monitor nic-proxy-configuration radius-authorization-nic
     resolution]
   user@host# show
   ```

Changing the Configuration for the NIC Proxy Cache

You can modify cache properties for the NIC proxy to optimize the resolution performance for your network configuration and system resources. Typically, you can use the default settings for the cache properties. The configuration statements are available at the Advanced editing level.

Use the following configuration statements to change values for the NIC proxy cache:

```
slot number external-subscriber-monitor nic-proxy-configuration radius-authorization-nic
  cache {
  cache-size cache-size;
  cache-cleanup-interval cache-cleanup-interval;
  cache-entry-age cache-entry-age;
}
```

To configure the cache for a NIC proxy:

1. From configuration mode, access the configuration statement that specifies the NIC proxy configuration. In this sample procedure, the NIC proxy called radius-authorization-nic is configured.

   ```
   user@host# edit slot 0 external-subscriber-monitor nic-proxy-configuration
     radius-authorization-nic cache
   ```

2. Specify the cache properties for the NIC proxy.

   ```
   [edit slot 0 external-subscriber-monitor nic-proxy-configuration radius-authorization-nic
     cache]
   user@host# set ?
   ```

   For more information about configuring the cache for a NIC proxy, see *Changing the Configuration for the NIC Proxy Cache (SRC CLI)*.

3. (Optional) Verify your configuration.

   ```
   [edit slot 0 external-subscriber-monitor nic-proxy-configuration
   radius-authorization-nic cache]
   user@host# show
   cache-size 10000;
   cache-cleanup-interval 15;
   ```

Configuring a NIC Proxy for NIC Replication

Typically, you configure NIC replication to keep the NIC highly available. You configure NIC host selection to specify the groups of NIC hosts to be contacted to resolve a request, and to define how the NIC proxy handles NIC hosts that the proxy is unable to contact. The configuration statements are available at the Normal editing level.

Use the following configuration statements to configure NIC host selection for a NIC proxy:

```
slot number external-subscriber-monitor nic-proxy-configuration radius-authorization-nic
  nic-host-selection {
  groups groups;
  selection-criteria (roundRobin | randomPick | priorityList);
}
slot number external-subscriber-monitor nic-proxy-configuration radius-authorization-nic
  nic-host-selection blacklisting {
  try-next-system-on-error;
  number-of-retries-before-blacklisting number-of-retries-before-blacklisting;
  blacklist-retry-interval blacklist-retry-interval;
}
```

To configure a NIC proxy to use NIC replication:

1. From configuration mode, access the configuration statement that specifies the NIC proxy configuration. In this sample procedure, the NIC proxy called radius-authorization-nic is configured.

   ```
   user@host# edit slot 0 external-subscriber-monitor nic-proxy-configuration
     radius-authorization-nic nic-host-selection
   ```

2. (Optional) Configure NIC host selection for a NIC proxy.

   ```
   [edit slot 0 external-subscriber-monitor nic-proxy-configuration radius-authorization-nic
     nic-host-selection]
   user@host# set ?
   ```

   For more information about configuring NIC host selection for a NIC proxy, see *Configuring a NIC Proxy for NIC Replication (SRC CLI)*.

3. (Optional) Verify your configuration.

   ```
   [edit slot 0 external-subscriber-monitor nic-proxy-configuration
   radius-authorization-nic nic-host-selection]
   user@host# show
   groups ;
   selection-criteria roundRobin;
   ```

4. Access the configuration statement that specifies the NIC proxy configuration for blacklisting—the process of handling nonresponsive NIC hosts.

   ```
   [edit slot 0 external-subscriber-monitor nic-proxy-configuration radius-authorization-nic
     nic-host-selection]
   user@host# edit blacklisting
   [edit slot 0 external-subscriber-monitor nic-proxy-configuration radius-authorization-nic
     nic-host-selection blacklisting]
   ```

5. (Optional) Configure blacklisting for a NIC proxy.

```
[edit slot 0 external-subscriber-monitor nic-proxy-configuration radius-authorization-nic
  nic-host-selection blacklisting]
user@host# set ?
```

For more information about configuring NIC host selection for a NIC proxy, see *Configuring a NIC Proxy for NIC Replication (SRC CLI)*.

6. (Optional) Verify your configuration.

```
[edit slot 0 external-subscriber-monitor nic-proxy-configuration
radius-authorization-nic nic-host-selection blacklisting]
user@host# show
```

```
[edit slot 0 external-subscriber-monitor nic-proxy-configuration
radius-authorization-nic nic-host-selection blacklisting]
user@host# show
try-next-system-on-error;
number-of-retries-before-blacklisting 3;
blacklist-retry-interval 15;
```

Related Documentation

- Configuring External Subscriber Monitor (SRC CLI) on page 39
- Configuring Pseudo–RADIUS Authorization Server Properties (SRC CLI) on page 40
- Extracting RADIUS Attributes with the Pseudo–RADIUS Authorization Server (SRC CLI) on page 49
- Enabling the Pseudo-RADIUS Authorization Server (SRC CLI) on page 52

Extracting RADIUS Attributes with the Pseudo–RADIUS Authorization Server (SRC CLI)

The pseudo–RADIUS authorization server extracts RADIUS attribute values from the MX Series router for which it receives access requests.

Tasks to configure the RADIUS attribute value extraction are:

- Extracting Interface Name Attribute Values on page 49
- Extracting Virtual Router Name Attribute Values on page 50

Extracting Interface Name Attribute Values

The interface name value is the subscriber line interface. This value is extracted from the NAS-Port-ID attribute. The default settings for this configuration are sufficient for most applications.

Use the following configuration statements to extract the interface name value from the RADIUS access request:

```
slot number external-subscriber-monitor radius-attribute-extraction default interface-name
  {
```

```
    regular-expression [regular-expression...];
}
```

To extract the interface name value:

1. From configuration mode, access the configuration statement that configures RADIUS attribute extraction for the interface name value.

   ```
   user@host# edit slot 0 external-subscriber-monitor radius-attribute-extraction default
     interface-name
   ```

2. (Optional) Specify the RADIUS attribute value format with a regular expression. You can group regular expressions by enclosing them in parentheses. The value for the interface is the part of the NAS-Port-ID matched by the first group in your regular expression. For more information about using regular expressions, see http://docs.oracle.com/javase/1.5.0/docs/api/java/util/regex/Pattern.html.

   ```
   [edit slot 0 external-subscriber-monitor radius-attribute-extraction default
     interface-name]
   user@host# set regular-expression [regular-expression...]
   ```

   For example, to specify that the extracted interface name value is ge-0/0/3.0 from the NAS-Port attribute value of ge-0/0/3.0[:0-0]:

   ```
   [edit slot 0 external-subscriber-monitor radius-attribute-extraction default
     interface-name]
   user@host# set regular-expression ([a-zA-Z0-9-/.]+)\\[:.*
   ```

Extracting Virtual Router Name Attribute Values

In most cases, the virtual router name value is in the format default@<NAS-ID attribute>. The default settings extract a virtual router name in this format. If your environment is different, you can configure a different format for the extracted value.

Use the following configuration statements to extract the virtual router name value from the RADIUS access request:

```
slot number external-subscriber-monitor radius-attribute-extraction default
  virtual-router-name {
  id id;
  vsa;
  vsa-id vsa-id;
  regular-expression [regular-expression...];
  type (raw-byte | chars);
  prefix prefix;
}
```

To extract the virtual router name value:

1. From configuration mode, access the configuration statement that configures RADIUS attribute extraction for the virtual router name value.

```
user@host# edit slot 0 external-subscriber-monitor radius-attribute-extraction default
  virtual-router-name
```

2. Specify the RADIUS attribute identifier.

```
[edit slot 0 external-subscriber-monitor radius-attribute-extraction default
  virtual-router-name]
user@host# set id id
```

3. (Optional) Specify whether the RADIUS attribute is a vendor-specific attribute.

```
[edit slot 0 external-subscriber-monitor radius-attribute-extraction default
  virtual-router-name]
user@host# set vsa
```

4. (Optional) Specify the RADIUS vendor-specific attribute identifier.

```
[edit slot 0 external-subscriber-monitor radius-attribute-extraction default
  virtual-router-name]
user@host# set vsa-id vsa-id
```

5. (Optional) Specify the RADIUS attribute value format with a regular expression. You can group regular expressions by enclosing them in parentheses. The value for the interface is the part of the NAS-Port-ID matched by the first group in your regular expression. For more information about using regular expressions, see http://docs.oracle.com/javase/1.5.0/docs/api/java/util/regex/Pattern.html.

```
[edit slot 0 external-subscriber-monitor radius-attribute-extraction default
  virtual-router-name]
user@host# set regular-expression [regular-expression...]
```

For example:

```
[edit slot 0 external-subscriber-monitor radius-attribute-extraction default
  virtual-router-name]
user@host# set regular-expression ([a-zA-Z0-9-/.]+)\\[:.*
```

6. (Optional) Specify the value type of this RADIUS attribute.

```
[edit slot 0 external-subscriber-monitor radius-attribute-extraction default
  virtual-router-name]
user@host# set type (raw-byte | chars)
```

where:

- **raw-byte**—Raw bytes
- **chars**—Sequence of characters

7. (Optional) Specify the prefix that is prepended to the extracted RADIUS attribute value.

```
[edit slot 0 external-subscriber-monitor radius-attribute-extraction default
  virtual-router-name]
user@host# set prefix prefix
```

Related Documentation

- Configuring External Subscriber Monitor (SRC CLI) on page 39
- Configuring Pseudo–RADIUS Authorization Server Properties (SRC CLI) on page 40
- Configuring the NIC Proxy for the Pseudo-RADIUS Authorization Server (SRC CLI) on page 46
- Enabling the Pseudo-RADIUS Authorization Server (SRC CLI) on page 52

Enabling the Pseudo-RADIUS Authorization Server (SRC CLI)

To enable the pseudo–RADIUS authorization server, configure the pseudo-RADIUS authorization server and make sure the External Subscriber Monitor is running.

To start External Subscriber Monitor:

```
user@host> enable component extsubmon
```

Related Documentation

- Configuring External Subscriber Monitor (SRC CLI) on page 39
- Configuring Pseudo–RADIUS Authorization Server Properties (SRC CLI) on page 40
- Disabling the Pseudo-RADIUS Authorization Server (SRC CLI) on page 52
- Viewing Statistics for the Pseudo–RADIUS Authorization Server (SRC CLI) on page 61
- Monitoring Statistics for the Pseudo–RADIUS Authorization Server (SRC CLI) on page 64

Disabling the Pseudo-RADIUS Authorization Server (SRC CLI)

To disable the pseudo–RADIUS authorization server, delete the pseudo–RADIUS authorization server configuration for External Subscriber Monitor from configuration mode.

```
[edit slot 0 external-subscriber-monitor]
user@host# delete radius-authorization
```

Related Documentation

- Enabling the Pseudo-RADIUS Authorization Server (SRC CLI) on page 52

CHAPTER 9

Configuration Tasks for Managing Subscriber Sessions Using COA Script Service

Configuring the COA Script Service for MX Series Routers (SRC CLI)

To configure the script service for the MX Series router:

1. Create a script service in the services global service name hierarchy or the services scope name service name hierarchy. For example:

   ```
   [edit]
   user@host# edit services global service cos-service
   ```

2. Set the type to script.

   ```
   [edit services global service cos-service]
   user@host# set type script
   ```

3. (Optional) Configure other properties as needed for your service.

4. Configure the script properties.

   a. Access the script hierarchy for the configured script service.

      ```
      [edit services global service cos-service]
      user@host# edit script
      ```

   b. Specify URL as the script type.

      ```
      [edit services global service cos-service script]
      ```

```
user@host# set script-type url
```

c. Specify the name of the Java class that implements the script service.

```
[edit services global service cos-service script]
user@host# set class-name net.juniper.smgt.scriptServices.coa.CoaService
```

d. Configure the URL of the script service or the path and filename of the service.

```
[edit services global service cos-service script]
user@host# set file file:///opt/UMC/sae/lib/coa.jar
```

If you specify a file URL, you must copy the file to the C Series Controller. If you specify an ftp or http URL, the file can reside on a centralized server. You can find the *coa.jar* file in the application and SDK distribution on the Juniper Networks website at:

https://www.juniper.net/support/downloads/?p=src#sw

in the *SDK+AppSupport+Demos+Samples.tar.gz* archive file with the pathname:

AppSupport+Demos+Samples/SDK/scriptServices/coa/lib/coa.jar

5. Verify the configuration.

```
[edit services global service cos-service script]
user@host# show
type script;
status active;
available;
script {
  script-type url;
  class-name net.juniper.smgt.scriptServices.coa.CoaService;
  file file:///opt/UMC/sae/lib/coa.jar;
}
```

6. Configure the parameters for the script service.

See "Configuring Parameters for the Script Service for MX Series Routers (SRC CLI)" on page 54.

Related Documentation

- Setting Up MX Series Routers in the SRC Network (SRC CLI) on page 25
- Configuring Parameters for the Script Service for MX Series Routers (SRC CLI) on page 54
- Configuring Subscriptions to the Script Service on page 56

Configuring Parameters for the Script Service for MX Series Routers (SRC CLI)

Provide parameter substitutions with the values that are in the service definitions for the script service.

Table 5 on page 55 lists the parameters specified by the sample script service.

Table 5: Parameter Substitutions for MX Series Routers COA Services

Parameter Name	Description
dynClientIp	IP address of the device.
dynClientPort	UDP port number of the device.
dynServerIp	IP address of the C Series Controller.
dynServerPort	UDP port number of the C Series Controller.
dynSecret	Shared secret between RADIUS server and RADIUS client.
dynRetry	Number of retries for sending RADIUS packets when no RADIUS response is received. The retry interval is 3 seconds.

dynConfig	Content of service definition in the format
	
	<action>.<radiusAttributeName>=<pluginEventAttribute>\n
	
	• action—Action that is executed on packet content (attribute):
	  ◦ start
	  ◦ stop
	  ◦ start-stop
	• radiusAttributeName—Valid RADIUS attribute specified as follows:
	  ◦ Standard RADIUS attribute name or number
	  ◦ VSA in the format vendor-specific.<vendor#>.<vsa#>.string
	• pluginEventAttribute—Valid Python expression
	• \n—New-line character included between the lines of a configuration containing multiple lines; the entire configuration must be enclosed in quotation marks.
	
	For example:
	
	start-stop.Acct-Session-Id = ifSessionId
	
	“start-stop.Acct-Session-Id=ifSessionId\nstart.vendor-specific.4874.10.string=’video’\nstop.vendor-specific.4874.10.string=’default’\n"

To configure substitutions for the script parameters:

1. At the hierarchy for the script service, specify substitutions for the parameters. For example:

```
[edit services global service cos-service]
user@host# set parameter substitution [ dynSecret=\”secret\” dynRetry=2
  dynClientIp=10.227.7.111 dynClientPort=9099
  "dynConfig=\"start-stop.1.string=primaryUserName\\nstart-stop.Acct-Session-id=ifSessionId
  \\nstart.vendor-specific.4874.108.string=['T01 3m', 'T04
```

```
consumer-scheduler-map']\\nstop.vendor-specific.4874.108.string=['T011m', 'T04
data-scheduler-map']\\nstart.vendor-specific.4874.10.string='video'
\\nstop.vendor-specific.4874.10.string='default'\\n\"" ]
```

2. Verify the configuration.

```
[edit services global service cos-service]
user@host# show
```

Related Documentation

- Configuring the COA Script Service for MX Series Routers (SRC CLI) on page 53
- Configuring Subscriptions to the Script Service on page 56

Configuring Subscriptions to the Script Service

You need to configure subscriptions to the script service. You can set up the subscriptions to activate immediately on login.

For more information, see *Adding Subscribers (SRC CLI)*.

Related Documentation

- Configuring the COA Script Service for MX Series Routers (SRC CLI) on page 53
- Configuring Parameters for the Script Service for MX Series Routers (SRC CLI) on page 54

CHAPTER 10

Configuration Statements and Commands

SRC CLI Commands to Monitor the SRC Diameter Server

You can view statistics and status for the SRC Diameter server. Table 6 on page 57 lists the commands you use to monitor the SRC Diameter server

Table 6: Commands to Monitor the Diameter Server

Command	Output Displayed
show diameter statistics	Information about the server process and the current state of the Diameter server.
show diameter statistics message-handler	Information about the Diameter server message handler.
show diameter statistics message-handler message-flow	Information about the Diameter server message flows.
show diameter statistics process	Information about the Diameter server process.
show diameter statistics requests	Information about the Diameter server requests.
show diameter status	Status of the Diameter server.
show diameter status clients	Status of the Diameter clients.
show diameter status peers	Status of the Diameter peers.

Related Documentation

- Configuring the Diameter Application (SRC CLI) on page 16
- Viewing Statistics for the SRC Diameter Server (SRC CLI) on page 62
- Viewing Message Handler Information for the SRC Diameter Server (SRC CLI) on page 62
- Viewing Server Process Information for the SRC Diameter Server (SRC CLI) on page 62

- Viewing Information About SRC Diameter Server Requests (SRC CLI) on page 63
- Viewing SRC Diameter Server State (SRC CLI) on page 63

PART 3

Administration

CHAPTER 11

Routine Monitoring

Viewing Statistics for the Pseudo–RADIUS Authorization Server (SRC CLI)

Purpose View RADIUS statistics for the pseudo–RADIUS authorization server.

Action To display client statistics for the pseudo–RADIUS authorization server:

```
user@host> show external-subscriber-monitor statistics radius-authorization
Client Statistics
Client Address                                      10.227.7.45
Number of received radius access-request            602524
Number of dropped radius access-request             0
Number of radius access-accept sent                 602524
Number of radius access-reject sent                 0
Number of dropped radius authentication response    0
Number of access request received per second        58
```

To display specific client statistics for the pseudo–RADIUS authorization server:

```
user@host> show external-subscriber-monitor statistics radius-authorization client-address
client-address
```

Related Documentation

- Configuring Pseudo–RADIUS Authorization Server Properties (SRC CLI) on page 40
- Monitoring Statistics for the Pseudo–RADIUS Authorization Server (SRC CLI) on page 64

Viewing Statistics for the SRC Diameter Server (SRC CLI)

Purpose View information about the server process and the state of the Diameter server.

Action To display information about the server process and the state of the Diameter server:

user@host> **show diameter statistics**

Related Documentation

- Configuring the Diameter Application (SRC CLI) on page 16
- SRC CLI Commands to Monitor the SRC Diameter Server on page 57

Viewing Message Handler Information for the SRC Diameter Server (SRC CLI)

Purpose View information about the message handler and message flows for the Diameter server.

Action To display information about the message handler for the Diameter server:

user@host> **show diameter statistics message-handler**

To display information about message flows for the Diameter server:

user@host> **show diameter statistics message-handler message-flow**

To display information about a specific message flow:

user@host> **show diameter statistics message-handler message-flow id** *id*

Related Documentation

- Configuring the Diameter Application (SRC CLI) on page 16
- SRC CLI Commands to Monitor the SRC Diameter Server on page 57

Viewing Server Process Information for the SRC Diameter Server (SRC CLI)

Purpose View information about the server process.

Action To display about the server process:

user@host> **show diameter statistics process**

Related Documentation
- Configuring the Diameter Application (SRC CLI) on page 16
- SRC CLI Commands to Monitor the SRC Diameter Server on page 57

Viewing Information About SRC Diameter Server Requests (SRC CLI)

Purpose View information about Diameter server requests.

Action To display information about Diameter server requests:

user@host> **show diameter statistics requests**

Related Documentation
- Configuring the Diameter Application (SRC CLI) on page 16
- SRC CLI Commands to Monitor the SRC Diameter Server on page 57

Viewing SRC Diameter Server State (SRC CLI)

Purpose View status information about the Diameter server.

Action To display information about the status of the Diameter server:

user@host> **show diameter status**

To display information about the Diameter clients:

user@host> **show diameter status clients**

To display information about a specific client:

user@host> **show diameter status clients client-name** *client-name*

To display information about the Diameter peers:

user@host> **show diameter status peers**

To display information about a specific peer:

user@host> **show diameter status peers peer-name** *peer-name*

Related Documentation
- Configuring the Diameter Application (SRC CLI) on page 16
- Configuring Diameter Peers (SRC CLI) on page 22

- SRC CLI Commands to Monitor the SRC Diameter Server on page 57

Monitoring Statistics for the Pseudo–RADIUS Authorization Server (SRC CLI)

Purpose Display real-time RADIUS authorization statistics for the pseudo–RADIUS authorization server.

Action To display real-time client statistics for the pseudo–RADIUS authorization server:

```
user@host> monitor external-subscriber-monitor statistics radius-authorization client-address
client-address
```

Related Documentation

- Configuring Pseudo–RADIUS Authorization Server Properties (SRC CLI) on page 40
- Viewing Statistics for the Pseudo–RADIUS Authorization Server (SRC CLI) on page 61