JUNIPER NETWORKS

3GPP Gateway

Modified: 2015-06-23

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

3GPP Gateway

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

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

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

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

Supported Platforms

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

- C Series

Documentation Conventions

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

Table 2: Notice Icons

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

Table 3: Text Conventions

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

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

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

Table 3: Text Conventions *(continued)*

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

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at https://www.juniper.net/cgi-bin/docbugreport/.
- 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 http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

CHAPTER 1

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)	Used in conjunction with the MX Series router running the packet-triggered subscribers and policy control (PTSP) solution, the SIC listens for RADIUS accounting events from IP edge devices (accounting clients) and stores them in the Session State Registrar (SSR), or 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.
Juniper Policy Server (JPS)	Acts as a policy decision point (PDP) and policy enforcement point (PEP) that manages the relationships between application managers and CMTS devices in a PCMM environment.
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.

Table 4: Descriptions of SRC Components *(continued)*

Component	Description
Redirect Server	Redirects HTTP requests received from IP Filter to a captive portal page.
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.
Session State Registrar (SSR)	The SSR is a stateless, highly reliable and highly available database cluster. When used in conjunction with an MX Series router running the packet-triggered subscribers and policy control (PTSP) solution, the SSR stores the IP edge attachment subscriber sessions data learned from IP edge devices in the centralized SSR database.
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.

Table 4: Descriptions of SRC Components *(continued)*

Component	Description
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.
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.

Table 4: Descriptions of SRC Components *(continued)*

Component	Description
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)	
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

SRC 3GPP Gateway

SRC 3GPP Gateway Overview

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 Gx interface to mediate between the PCRF and Juniper Networks routers like the E Series Broadband Services routers and MX Series routers. Figure 1 on page 8 shows an example network configuration where the SRC 3GPP gateway acts as a mediator between the PCRF and an MX Series router. The Gx interface on the SRC 3GPP gateway communicates with the PCRF using the Diameter protocol.

Figure 1: SRC 3GPP Gateway as a Mediator Between the PCRF and an MX Series Router

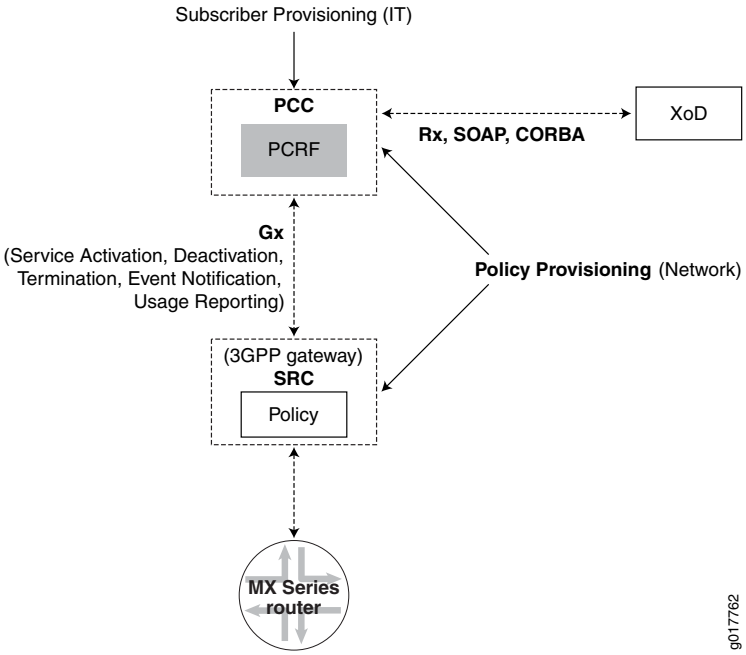
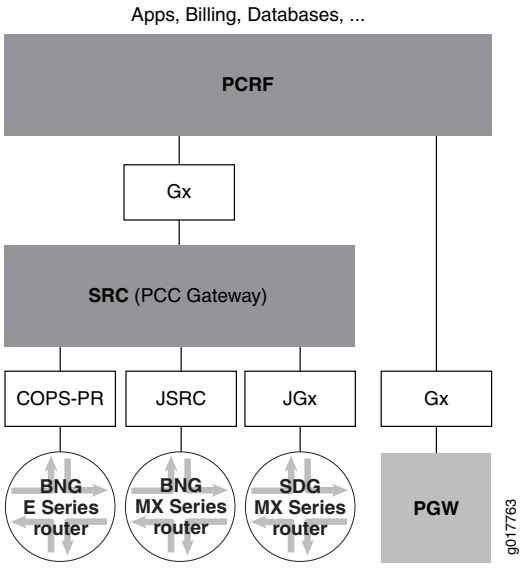


Figure 2 on page 8 represents the different policy references interfaces you can use, when using the SRC 3GPP gateway with other Juniper Networks products.

Figure 2: Various Interfaces on Juniper Networks Products Communicating with a PCRF Through the SRC 3GPP Gateway



The SRC 3GPP gateway supports the following scenarios:

- Subscriber Login Sequence on page 9
- Subscriber Logout Sequence on page 10

The following sections describe the sequences for each of these scenarios based on using an MX Series router.

Subscriber Login Sequence

The subscriber login uses the following sequence:

1. A subscriber session logs in and notifies the JSRC within the MX Series router.
2. The MX Series router sends a Diameter AA-Request (AAR) for the new subscriber session.
3. The service activation engine (SAE) performs necessary tasks such as creating the user session, provisioning any policy objects, and others.
4. When the login is complete, the SAE sends back a Diameter AA-Answer (AAA) to the router.
5. The SAE notifies the SRC 3GPP gateway that a subscriber was logged in successfully. This notification includes information such as the IP Address of the subscriber.
6. The SRC 3GPP gateway sends a Diameter Credit-Control-Request (CCR) with the following information to the PCRF:
   - CC-Request-Type AVP: INITIAL_REQUEST
   - Framed-IP-Address AVP: user equipment IPv4 address or Framed-IPv6-Prefix AVP: user equipment IPv6 address
   - Subscription-Id AVP: the login-name SAE plug-in attribute (Subscription-Id-Type set to END_USER_E164(0)) and, if available, the interface description SAE plug-in attribute (Subscription-Id-Type set to END_USER_PRIVATE(4))
   - CalledStationId AVP: Set to virtual router name.

   The SRC 3GPP gateway selects the PCRF according to the referenced Diameter peers under the **[edit slot 0 gw-3gpp gx diameter-peer]** hierarchy.
7. The SRC 3GPP gateway receives the Credit-Control-Answer (CCA) message from the PCRF.
   - If the PCRF rejected the CCR-I (initial) by providing an error code in the CCA message, the SRC 3GPP gateway logs the subscriber out using the SAE Common Object Request Broker Architecture (CORBA) interface.
   - If the PCRF accepted the CCR-I, the SRC 3GPP gateway iterates over the provided policy and charging control (PCC) rules (if any) from the CCA message and issues service activate calls for those services.

8. The SRC 3GPP gateway iterates over PPC Rules from the CCA message and issues service activate calls for those services, if applicable.
9. For each service to be activated, the SAE issues a Diameter Push-Profile-Request (PPR) to the MX Series router.
10. The MX Series router sends an acknowledgment to the SAE in a Push-Profile-Answer (PPA) message.
11. The SAE sends an acknowledgement to the SRC 3GPP gateway.

    The SRC 3GPP gateway collects all the failed service activations and sends a CCR-U (update) to the PCRF to indicate the failure. The SRC 3GPP gateway sets the experimental result code in the CCR-U to DIAMETER_PCC_RULE_EVENT(5142) and includes a charging-rule-report for each failed activation including the rule-name and the rule-failure-code.

Subscriber Logout Sequence

The subscriber logout uses the following sequence:

1. A subscriber session logs out and notifies the JSRC within the MX Series router.
2. The router sends a Diameter Session-Termination-Request (STR) to the SAE to indicate that the subscriber has logged out.
3. The SAE notifies the SRC 3GPP gateway that the service session has stopped.

   For each service stop event, the SRC 3GPP gateway issues a CC-Request to the PCRF that includes:

   - CC-Request-Type AVP: UPDATE_REQUEST
   - Usage-Monitoring-Information AVP includes:
     - Final accounting data
4. The SAE notifies the SRC 3GPP gateway that the subscriber was logged out successfully. The notification includes one of the following addresses:
   - Framed-IP-Address AVP: user equipment IPv4 address
   - Framed-IPv6-Prefix AVP: user equipment IPv6 address
5. The SRC 3GPP gateway sends a Diameter CCR message with the following information to the PCRF:
   - CC-Request-Type AVP: TERMINATION_REQUEST
   - Subscriber-Id AVP includes one of the following addresses:
     - Framed-IP-Address AVP: user equipment IPv4 address
     - Framed-IPv6-Prefix AVP: user equipment IPv6 address
6. The SRC 3GPP gateway receives the CCA message from the PCRF.
7. The SAE acknowledges the STR sent by the router by sending a Session-Termination-Answer (STA) to the router.

Subscriber Session Termination Sequence (Initiated by PCRF)

When the PCRF initiates the subscriber session termination, the following sequence occurs:

1. The application function requests the termination of the session from the PCRF.
2. The PCRF issues a Re-Auth-Request (RAR) message, which includes the Session-Release-Cause AVP.
3. The SRC 3GPP gateway issues a subscriber disconnect CORBA Call to the SAE. This method is not supported for JunosE Point-to-Point Protocol (PPP) sessions; in that case, the SRC 3GPP gateway only logs the subscriber out.
4. The SAE performs the necessary steps to disconnect the subscriber. For JunosE PPP sessions, the subscriber is logged out using the subscriber logout procedure.
5. The user equipment is disconnected.
6. The router sends an acknowledgement to the SAE.
7. The SAE acknowledges the CORBA Call by sending an acknowledgement to the SRC 3GPP gateway.
8. The SRC 3GPP gateway acknowledges the RAR message sent by the PCRF by sending a Re-Auth-Answer (RAA) message to the PCRF.
9. The SAE sends a Subscriber Stop Event message to the SRC 3GPP gateway.
10. The SRC 3GPP gateway sends a CCR with the following information to the PCRF:
    - CC-Request-Type AVP: TERMINATION_REQUEST
    - Subscriber-Id AVP includes one of the following addresses:
        - Framed-IP-Address AVP: user equipment IPv4 address
        - Framed-IPv6-Prefix AVP: user equipment IPv6 address
11. The SRC 3GPP gateway receives the CCA message.

Service Activation Sequence (Initiated by Application Function)

When the application function (AF) initiates a service activation, the following sequence occurs:

1. The AF receives any kind of trigger to set up a new AF session and issues an AAR message to the PCRF.
2. The PCRF stores all received service information, retrieves profiles, and sends an AA-Answer (AAA) message back to the AF.
3. The PCRF issues an RAR message, with the Charging-Rule-Install AVP set.
4. The SRC 3GPP gateway issues a subscriber activate service session CORBA Call to the SAE, by using the Bearer-Identity AVP (subscriber's IP address) and service name (Charging-Rule-Name AVP).

5. The SAE performs the necessary steps to activate the specified service for the given subscriber, including sending a Push-Profile-Request (PPR) message to the router.
6. The router sends an acknowledgement (PPA) to the SAE.
7. The SAE acknowledges the CORBA Call by sending an acknowledgement to the SRC 3GPP gateway.
8. The SRC 3GPP gateway sends an Re-Auth-Answer (RAA) message to the PCRF.
9. The SAE sends Service Start Event to the SRC 3GPP gateway.

Service Modification Sequence (Initiated by Application Function)

When the application function (AF) initiates a service modification, the following sequence occurs:

1. The AF receives any kind of trigger to update an existing AF session and issues an AAR message to the PCRF.
2. The PCRF stores all received service information, retrieves profiles, and sends an AA-Answer (AAA) message back to the AF.
3. The PCRF issues an RAR message, with the Charging-Rule-Install AVP set.
4. The SRC 3GPP gateway issues a subscriber-modify service CORBA Call to the SAE, which includes the subscriber IP address and the service name (Charging-Rule-Name AVP).
5. The SAE performs the necessary steps to modify the specified service for the given subscriber, including sending a Push-Profile-Request (PPR) message to the router.
6. The router sends an acknowledgement (PPA) to the SAE.
7. The SAE acknowledges the CORBA Call by sending an acknowledgement to the SRC 3GPP gateway.
8. The SRC 3GPP gateway sends a Re-Auth-Answer (RAA) message to the PCRF.

Service Deactivation Sequence (Initiated by Application Function)

When the application function (AF) initiates a service deactivation, the following sequence occurs:

1. The AF receives any kind of trigger to terminate or deactivate an existing session and issues an AAR message to the PCRF.
2. The PCRF stores all received service information, retrieves profiles, and sends an AA-Answer (AAA) message back to the AF.
3. The PCRF issues an RAR message with the Charging-Rule-Remove AVP set.
4. The SRC 3GPP gateway issues a subscriber-deactivate service CORBA Call to the SAE.
5. The SAE performs the necessary steps to deactivate the specified service for the given subscriber, including sending a Push-Profile-Request (PPR) message to the router.

6. The router sends an acknowledgement Push-Profile-Answer (PPA) to the SAE.
7. The SAE acknowledges the CORBA Call by sending an acknowledgement to the SRC 3GPP gateway.
8. The SRC 3GPP gateway sends a Re-Auth-Answer (RAA) message to the PCRF.
9. The SAE sends a Service Stop Event to the SRC 3GPP gateway. The SRC 3GPP gateway issues a CCR to the PCRF including:
   - CC-Request-Type AVP: UPDATE_REQUEST
   - Usage-Monitoring-Information AVP includes:
     - Final accounting data

Related Documentation

- Mapping Between SRC Software, Junos OS, and PCC Concepts on page 13
- SRC 3GPP Gateway Peer Communication and Redundancy on page 19
- Configuring the SRC 3GPP Gateway (SRC CLI) on page 23

Mapping Between SRC Software, Junos OS, and PCC Concepts

This section describes the mapping between the SRC software and Junos OS concepts and the policy and charging control (PCC) concepts. During these discussions, refer to Table 5 on page 13, which describes the mapping between SRC software and Junos OS terminology and the policy and charging control (PCC) function terminology.

Table 5: SRC Software and Junos OS Terminology Versus PCC Terminology

SRC Software and Junos OS Terminology	PCC Terminology
Subscriber session	IP CAN Session
Service with associated policies	PCC Rule
Service activation	Rule-Install
Service deactivation	Rule-Uninstall
Service accounting	Usage-Monitoring
Service templates, defined by SRC	Predefined Rule
Policies, defined by the PCRF	Dynamic Rule

Charging Rule Installation (Service Activation)

A PCRF can activate any number of non-parameterized and parameterized services (predefined PCC rules) in the same CCA or RAR message by providing a Charging-Rule-Install AVP. The Charging-Rule-Install AVP can contain multiple Charging-Rule-Name AVPs, one for each non-parameterized service to be activated.

The Charging-Rule-Install AVP can also contain multiple Charging-Rule-Definition AVPs, one for each parameterized service session that is to be activated.

NOTE: The names appearing in the Charging-Rule-Name AVPs must be unique; the same name must not appear multiple times in the same Gx message.

The SRC 3GPP gateway expects to receive the following AVPs from the PCRF in CCA and RAR messages:

```
Charging-Rule-Install ::= < AVP Header: 1001 >
       *[ Charging-Rule-Definition ]
       *[ Charging-Rule-Name ]
       *[ Charging-Rule-Base-Name ]
       *[ AVP ]
```

Where:

```
Charging-Rule-Definition ::= < AVP Header: 1003 >
   {Charging-Rule-Name}
   [Juniper-Substitution]

   *[Juniper-Substitution]

Juniper-Substitution::= < AVP Header: 2024>
     {Juniper-Substitution-Name}
     {Juniper-Substitution-Value"}
```

Table 6 on page 14 describes these AVPs.

Table 6: AVP Definitions

AVP	Code	Type	VendorID	Description
Charging-Rule-Name	1005	UTF8String	VID_3GPP	To activate a parameterized default service session, specify the serviceName in the format: ruleName@00010001 and specify the ruleName in numeric format.
Juniper-Substitution-Name	2025	UTF8String	VID_JNPR	Name of parameter as defined in the SRC policy definition.
Juniper-Substitution-Value	2026	UTF8String	VID_JNPR	Value to assign to the parameter.

Installing Non-Parameterized Predefined Charging Rules

Non-parameterized predefined charging rules are equivalent to activating an SAE service with no parameters.

The Charging-Rule-Install AVP provides the list of Charging-Rule-Names. The Charging-Rule-Name AVP sent by the PCRF must correspond to the SRC service name.

NOTE: The Charging-Rule-Base-Name AVP is not supported and is ignored by the SRC 3GPP gateway.

Installing Parameterized Predefined Charging Rules

Parameterized predefined charging rules are equivalent to activating an SAE service with parameters.

The Charging-Rule-Definition AVP must be provided with the list of parameters in a list of Juniper-Substitution-Name AVPs.

- For activating a default service session, the Charging-Rule-Name AVP must be set to the SRC service name.
- Specify the serviceName in the format ruleName@dynamicfixedPart. For example, “ruleName@00010001” where ruleName is in numeric format and the dynamicFixedPart is a fixed length (size is 8) identifier generated by the PCRF.

NOTE: Only default sessions are supported.

Example of Charging-Rule Installation

The following example Charging-Rule-Install AVP, sent by the PCRF, activates the services “foo1” and “foo2” with no parameters. It also activates the service “123” with two parameters and the service “456” with one parameter.

```
AVP: Charging-Rule-Install(1001)
        AVP: Charging-Rule-Name(1005) val=foo1  <- Activate service foo1
        AVP: Charging-Rule-Name(1005) val=foo2  <- Activate service foo2
    AVP: Charging-Rule-Definition(1003) vnd=VID_3GPP  <- 3GPP AVP for activating
 parameterized service “123” with 2 parameters
            AVP: Charging-Rule-Name (1005) vnd=3GPP val=123@00010000
      AVP: Juniper-Substitution (2024) vnd=JNPR
                AVP: Juniper-Substitution-Name(2025) vnd=JNPR val=rate
          AVP: Juniper-Substitution-Value(2026) vnd=JNPR val=5
             AVP: Juniper-Substitution (2024) vnd=JNPR
          AVP: Juniper-Substitution-Name(2025) vnd=JNPR val=color
                AVP: Juniper-Substitution-Value(2026) vnd=JNPR val=red
AVP: Charging-Rule-Definition(1003) vnd=VID_3GPP  <- 3GPP AVP for activating
parameterized service “456” with 1 parameter
            AVP: Charging-Rule-Name (1005) vnd=3GPP val=456@00010001
      AVP: Juniper-Substitution (2024) vnd=JNPR
          AVP: Juniper-Substitution-Name(2025) vnd=JNPR val=rate
          AVP: Juniper-Substitution-Value(2026) vnd=JNPR val=10
```

In this example, foo1, foo2, 123 (rate, color), and “456” (rate) are configured services in the SRC software.

Charging Rule Removal (Service Deactivation)

A PCRF can deactivate any number of non-parameterized and parameterized services (predefined PCC rules) in the same CCA or RAR message by providing a Charging-Rule-Remove AVP. The Charging-Rule-Remove AVP can contain multiple Charging-Rule-Name AVPs, one for each non-parameterized or parameterized service to be deactivated.

The following AVPs are expected by the SRC (PCEF) from the PCRF in CCA and RAR messages:

```
Charging-Rule-Remove ::= < AVP Header: 1002 >
       *[ Charging-Rule-Definition ]
       *[ Charging-Rule-Name ]
       *[ Charging-Rule-Base-Name ]
       *[ AVP ]
```

- For non-parameterized charging rules, the Charging-Rule-Name AVP must correspond to the one provided in the Charging-Rule-Install AVP.
- For parameterized charging rules, the Charging-Rule-Name AVP must correspond to the one provided in the Charging-Rule-Definition AVP. If this format is not specified, the value in the Charging-Rule-Name AVP is treated as the serviceName.

NOTE: Charging-Rule-Base-Name AVP is not supported and is ignored by the SRC 3GPP gateway.

Example of Charging-Rule Removal

The following example Charging-Rule-Removal AVP, sent by the PCRF, deactivates the SRC services called “foo1”, “foo2”, and “123”.

```
AVP: Charging-Rule-Remove(1002)
             AVP: Charging-Rule-Name(1005) val=foo1 <- Deactivate service foo1
             AVP: Charging-Rule-Name(1005) val=foo2 <- Deactivate service foo2
           AVP: Charging-Rule-Name(1005) val=123@00010001  <- Deactivate service
 123
```

Charging Rule Report

The SRC 3GPP gateway can send charging rule reports for any number of non-parameterized and parameterized services in the same Credit Control Update (CCR-U) request or RAA message. This is achieved by providing a Charging-Rule-Report AVP for each failed service. The Charging-Rule-Report AVP contains a single Charging-Rule-Name AVP (for a non-parameterized or a parameterized service).

```
Charging-Rule-Report ::= < AVP Header: 1018 >
       *[ Charging-Rule-Name ]
       *[ Charging-Rule-Base-Name ]
     [ PCC-Rule-Status ]
       [ Rule-Failure-Code ]
    *[ AVP ]
```

- For non-parameterized charging rules, the Charging-Rule-Name AVP corresponds to the one provided in the Charging-Rule-Install AVP.
- For parameterized charging rules, the Charging-Rule-Name AVP must correspond to the one provided in the Charging-Rule-Definition AVP. If this format is not specified, the value in the Charging-Rule-Name AVP is treated as the serviceName.

NOTE: The Charging-Rule-Base-Name AVP is not supported and is never sent by the SRC 3GPP gateway.

Service Accounting

You can perform service accounting for one or more PCC rules.

When a PCRF requests service accounting, it needs to include an Event-Trigger AVP, set to “USAGE_REPORT”. This setting must be set in either the RAR message (if the PRCF initiates the PCC rule changes), or the CCA message (if the user equipment initiates the rule changes).

The PCRF may also provide usage threshold levels to the SRC 3GPP gateway at session establishment or modification time (CCA or RAR message). This is done, by setting those thresholds in the grouped Grant-Service-Unit AVP per Monitoring-Key in the Usage-Monitoring-Information AVP. The threshold level may be defined for:

- Total volume only (CC-Total-Octets AVP within Granted-Service-Unit hold threshold for total volume)
- Uplink volume only (CC-Input-Octets AVP within Granted-Service-Unit hold threshold for uplink volume)
- Downlink volume only (CC-Output-Octets AVP within Granted-Service-Unit hold threshold for downlink volume)

The Monitoring-Key AVP format is similar to the format of the Charging-Rule-Removal and Charging-Rule-Report AVPs:

- For non-parameterized charging rules, the Monitoring-Key AVP must be set to the Charging-Rule-Name AVP provided in the Charging-Rule-Install AVP.
- For parameterized charging rules, the Monitoring-Key AVP must be set to the Charging-Rule-Name AVP provided in the Charging-Rule-Install AVP (from the Charging-Rule-Definition AVP).

The SRC 3GPP gateway does not support SESSION_LEVEL monitoring. This means that the only supported value for the Usage-Monitoring-Level AVP is PCC_RULE_LEVEL.

The SRC 3GPP gateway sends accounting updates when it receives interim updates from the SAE for the service session. This is done by setting the usage counters in the Used-Service-Unit AVP within the Usage-Monitoring-Information AVP. Like the Granted-Service-Unit AVP (for setting the threshold), the Used-Service-Unit AVP is a grouped AVP and the SRC 3GPP gateway uses the CC-Total-Octet, CC-Input-Octets,

and CC-Output-Octets AVP within the Used-Service-Unit AVP to report the usage to the PCRF. The SRC 3GPP gateway sends this only in CCR messages (not in RAA messages). The reporting is done when any of the following conditions are met:

- When a usage threshold is reached.
  - The SRC 3GPP gateway stores the threshold information (provided by the PCRF) in the SAE session during service activation or modification.
  - After the SRC 3GPP gateway receives an interim update for a service session, it checks whether any of the thresholds were reached.
  - If a threshold is reached, the SRC 3GPP gateway generates a CCR-U to the PCRF and includes the accumulated usage volume in the Usage-Monitoring-Information AVP.
  - The Event-Trigger AVP is set to USAGE_REPORT.
- When the service is deactivated (the PCC rule, for which service accounting is enabled, is removed).
  - This is done after the SRC 3GPP gateway deactivates a given service (in response to an RAR or CCA message).
  - The SRC 3GPP gateway generates a CCR-U to the PCRF and includes the accumulated usage volume in the Usage-Monitoring-Information AVP.
  - The Event-Trigger AVP is set to USAGE_REPORT.
- When service accounting is explicitly disabled by the PCRF for a specific PCC rule.
  - This is done if the SRC 3GPP gateway receives a CCA or RAR message with the Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED for a specific Monitoring-Key within the Usage-Monitoring-Information AVP.
  - The SRC 3GPP gateway generates a CCR-U to the PCRF and includes the accumulated usage volume in the Usage-Monitoring-Information AVP.
  - The Event-Trigger AVP is set to USAGE_REPORT.
- When an IP-CAN session is terminated (either by the PCRF through an RAR message, or initiated by the user equipment).
  - For each service (the PCC rule, for which service accounting is enabled):
    - The SRC 3GPP gateway generates a CCR-U to the PCRF and includes the accumulated usage volume in the Usage-Monitoring-Information AVP for the specific service.
    - The Event-Trigger AVP is set to USAGE_REPORT.
  - The SRC 3GPP gateway also generates a termination request (CCR-T) message to the PCRF but does not include any usage report in it.
- When requested by the PCRF.

- This is done if the SRC 3GPP gateway receives an RAR message with the Usage-Monitoring-Report AVP set to USAGE_MONITORING_REPORT-REQUIRED within the Usage-Monitoring-Information AVP.
- The SRC 3GPP gateway generates a CCR-U to the PCRF for each requested Monitoring-Key AVP and includes the accumulated usage volume in the Usage-Monitoring-Information AVP.
- The Event-Trigger AVP is set to USAGE_REPORT

Related Documentation

- SRC 3GPP Gateway Overview on page 7
- SRC 3GPP Gateway Peer Communication and Redundancy on page 19
- Configuring the SRC 3GPP Gateway (SRC CLI) on page 23

SRC 3GPP Gateway Peer Communication and Redundancy

The SRC 3GPP gateway configuration allows the definition of multiple Diameter peers to act as PCRFs. The SRC 3GPP gateway picks one peer to become the “active” peer, and forwards all CCR messages to it. If the SRC software detects a failure of the active peer, the SRC 3GPP gateway selects another peer to become the active peer. The SRC 3GPP gateway does not switch back to the original active peer when it comes back online.

For redundancy purposes, you can configure multiple SRC 3GPP gateways to handle the communication between the same group of SAEs and PCRFs. To achieve this redundancy, you configure multiple SRC 3GPP gateway instances to point to the same namespace in the shared configuration.

All SRC 3GPP gateway instances pointing to the same namespace use a Community Manager to elect the active member. The active member registers itself with the naming server and is the only member receiving subscriber-tracking events from the SAE and forwarding them to the PCRF.

NOTE: **All the other SRC 3GPP gateway community members can still receive and process RAR messages from PCRF peers.**

If the active SRC 3GPP gateway member fails, the Community Manager detects the failure and elects another member to become the active member. The new active member registers itself with the naming server thus overwriting the old member’s endpoints. During the failure period, the SAE keeps a fail queue for the SRC 3GPP plug-in and replays the queue to the new active member.

Related Documentation

- SRC 3GPP Gateway Overview on page 7
- Mapping Between SRC Software, Junos OS, and PCC Concepts on page 13
- Configuring the SRC 3GPP Gateway (SRC CLI) on page 23

PART 2

Configuration

CHAPTER 3

Configuration Tasks for the SRC 3GPP Gateway

Configuring the SRC 3GPP Gateway (SRC CLI)

To configure the SRC 3GPP gateway:

1. Configure initial properties, including the connection to the directory and directory-monitoring properties.

   See "Configuring Initial Properties for the SRC 3GPP Gateway (SRC CLI)" on page 25.

   See "Changing the Location of Data in the Directory" on page 25.

   See "Configuring Directory-Connection Properties for the SRC 3GPP Gateway (SRC CLI)" on page 26.

   See "Configuring Initial Directory-Eventing Properties for the SRC 3GPP Gateway (SRC CLI)" on page 27.

2. Configure the connection to the PCRF (remote Diameter peer).

   See "Configuring Diameter Peers (SRC CLI)" on page 28.

3. Configure the SRC 3GPP gateway Gx interface.

   See "Configuring the SRC 3GPP Gateway Gx Interface (SRC CLI)" on page 31.

4. Configure the basic local properties for the SRC 3GPP gateway.

   See "Configuring Basic Local Properties for the SRC 3GPP Gateway (SRC CLI)" on page 32.

5. Configure the object adapter Internet address.

   "Configuring the Object Adapter Internet Address for the SRC 3GPP Gateway (SRC CLI)" on page 33.

6. Configure logging destinations.

   See "Configuring Logging Destinations to Store Messages in a File (SRC CLI)" on page 43.

   See "Configuring Logging Destinations to Send Messages to the System Logging Facility (SRC CLI)" on page 44.

7. Create an SRC 3GPP gateway grouped configuration.

   See "Creating Grouped Configurations for the SRC 3GPP Gateway (SRC CLI)" on page 34.

8. Configure subscriber types.

   See "Configuring the Subscriber Type (SRC CLI)" on page 35.

9. Configure the NIC proxies.

   See "Configuring a NIC Proxy for the SRC 3GPP Gateway (SRC CLI)" on page 35.

10. Start the SRC 3GPP gateway.

    See "Starting the SRC 3GPP Gateway (SRC CLI)" on page 61.

11. Configure the SAE for the SRC 3GPP gateway.

    See "Configuring the SAE for the SRC 3GPP Gateway" on page 41.

Related Documentation

- SRC 3GPP Gateway Overview on page 7

- Configuration Statements for the SRC 3GPP Gateway on page 55
- Mapping Between SRC Software, Junos OS, and PCC Concepts on page 13

Configuring Initial Properties for the SRC 3GPP Gateway (SRC CLI)

Use the following configuration statements to configure initial properties for the SRC 3GPP gateway:

```
slot number gw-3gpp initial {
   static-dn static-dn;
   dynamic-dn dynamic-dn;
}
```

To configure initial local properties:

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

   ```
   user@host# edit slot 0 gw-3gpp initial
   ```

2. Specify the properties for the SRC 3GPP gateway.

   ```
   [edit slot 0 gw-3gpp initial]
   user@host# set ?
   ```

   For more information about configuring local properties for SRC components, see "Changing the Location of Data in the Directory" on page 25.

3. (Optional) Verify your configuration.

   ```
   [edit slot 0 gw-3gpp initial]
   user@host# show
   ```

Related Documentation

- SRC 3GPP Gateway Overview on page 7
- Configuration Statements for the SRC 3GPP Gateway on page 55
- Configuring the SRC 3GPP Gateway (SRC CLI) on page 23
- Configuring Directory-Connection Properties for the SRC 3GPP Gateway (SRC CLI) on page 26

Changing the Location of Data in the Directory

In most cases, you use the default configuration for the location of SRC data in the directory:

- Administrator-defined configuration data—*ou=staticConfiguration,ou=Configuration,o=Management,o=umc*
- Programmatically defined configuration data—*ou=dynamicConfiguration,ou=Configuration,o=Management, o=umc*

You can specify the full distinguished name (DN), or a DN relative to a base DN, identified as *<base>*.

You can change the location of data in the directory at the Expert CLI editing level.

Use the following configuration statements to change the location of data for a component in the directory:

```
slot number component-name initial {
  static-dn static-dn ;
  dynamic-dn dynamic-dn ;
}
```

To change the location of data in the directory:

1. From configuration mode, access the configuration statement that specifies the configuration for a component on a slot.

   ```
   [edit]
   user@host# edit slot number nic initial
   ```

   For example:

   ```
   [edit]
   user@host# edit slot 0 nic initial
   ```

2. (Optional) Change the location of administrator-defined configuration data in the directory.

   ```
   [edit slot 0 nic initial]
   user@host# set static-dn static-dn
   ```

3. (Optional) Change the location of programmatically defined configuration data in the directory.

   ```
   [edit slot 0 nic initial]
   user@host# set dynamic-dn dynamic-dn
   ```

Related Documentation

- *Configuring Initial Directory Eventing Properties for SRC Components*
- *Configuring Basic Local Properties*
- *Configuration Statements for Local Configuration*
- *Managing Directory Communication*

Configuring Directory-Connection Properties for the SRC 3GPP Gateway (SRC CLI)

Use the following configuration statements to configure directory-connection properties for the SRC 3GPP gateway:

```
slot number gw-3gpp initial directory-connection {
  url url;
  backup-urls [backup-urls...];
```

```
    principal principal;
    credentials credentials;
    protocol (ldaps);
    timeout timeout;
    check-interval check-interval;
    blacklist;
    snmp-agent;
}
```

To configure directory-connection properties:

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

   ```
   user@host# edit slot 0 gw-3gpp initial directory-connection
   ```

2. Specify the properties for the SRC 3GPP gateway.

   ```
   [edit slot 0 gw-3gpp initial directory-connection]
   user@host# set ?
   ```

   For more information about configuring local properties for the SRC components, see *Configuring Basic Local Properties*.

3. (Optional) Verify your configuration.

   ```
   [edit slot 0 gw-3gpp initial directory-connection]
   user@host# show
   url ldap://127.0.0.1:389/;
   principal cn=conf,o=Operators,<base>;
   credentials ********;
   ```

Related Documentation

- SRC 3GPP Gateway Overview on page 7
- Configuring the SRC 3GPP Gateway (SRC CLI) on page 23
- Configuring Initial Properties for the SRC 3GPP Gateway (SRC CLI) on page 25
- Configuring Initial Directory-Eventing Properties for the SRC 3GPP Gateway (SRC CLI) on page 27
- Configuration Statements for the SRC 3GPP Gateway on page 55

Configuring Initial Directory-Eventing Properties for the SRC 3GPP Gateway (SRC CLI)

Use the following configuration statements to configure initial directory-eventing properties for the SRC 3GPP gateway:

```
slot number gw-3gpp initial directory-eventing {
    eventing;
    signature-dn signature-dn;
    polling-interval polling-interval;
    event-base-dn event-base-dn;
    dispatcher-pool-size dispatcher-pool-size;
}
```

To configure initial directory-eventing properties:

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

   user@host# edit slot 0 gw-3gpp initial eventing

2. Specify the initial directory-eventing properties for SRC 3GPP gateway.

   [edit slot 0 gw-3gpp initial directory-eventing]
   user@host# set ?

   For more information about configuring local properties for the SRC components, see *Configuring Basic Local Properties*.

3. (Optional) Verify your configuration.

   ```
   [edit slot 0 gw-3gpp initial directory-eventing]
   user@host# show
   eventing;
   polling-interval 30;
   ```

Related Documentation

- SRC 3GPP Gateway Overview on page 7
- Configuring the SRC 3GPP Gateway (SRC CLI) on page 23
- Configuring Initial Properties for the SRC 3GPP Gateway (SRC CLI) on page 25
- Configuring Directory-Connection Properties for the SRC 3GPP Gateway (SRC CLI) on page 26
- Configuration Statements for the SRC 3GPP Gateway on page 55

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)*
- *Viewing SRC Diameter Server State (SRC CLI)*

Configuring the SRC 3GPP Gateway Gx Interface (SRC CLI)

Use the following configuration statements to configure the SRC 3GPP gateway Gx interface:

```
slot number gw-3gpp gx {
    destination-host destination-host;
    destination-realm destination-realm;
    diameter-peer [diameter-peer.....];
    protocol (tcp | sctp);
    port port;
    address address;
    origin-host origin-host;
    origin-realm origin-realm;
}
```

NOTE: The SRC 3GPP gateway uses its own Diameter stack, which is configured under the **[edit slot 0 gw-3gpp gx]** hierarchy. It does not use the Diameter stack configured under the **[edit system diameter]** hierarchy; this Diameter stack is used for SAE and router communication.

To configure the SRC 3GPP gateway Gx interface:

1. From configuration mode, access the statement that configures the SRC 3GPP gateway Gx interface.

   user@host# **edit slot 0 gw-3gpp gx**

2. (Optional) Specify the Diameter identifier for the remote endpoint, which is the destination of the Diameter message. The Destination-Host AVP (AVP Code 293) is of the DiameterIdentity type and is present in all Diameter messages.

   [edit slot 0 gw-3gpp gx]
   user@host# **set destination-host *destination-host***

3. Specify the Diameter identifier for the realm of the remote endpoint, which is the destination of the Diameter message. The Destination-Realm AVP (AVP Code 283) is of the DiameterIdentity type and is present in all Diameter messages.

   [edit slot 0 gw-3gpp gx]
   user@host# **set destination-realm *destination-realm***

4. Specify the list of remote Diameter peers (PCRFs) that connect to the SRC 3GPP gateway over the Gx interface.

   [edit slot 0 gw-3gpp gx]
   user@host# **set diameter-peer [*diameter-peer*....]**

   Each Diameter peer you specify must be previously configured under the **[edit shared network diameter peer]** hierarchy.

5. (Optional) Specify the protocol for the transport connection.

   ```
   [edit slot 0 gw-3gpp gx]
   user@host# set protocol [(tcp | sctp)...]
   ```

6. (Optional) Specify the port to use for incoming connections.

   ```
   [edit slot 0 gw-3gpp gx]
   user@host# set port port
   ```

7. Specify the local address of the peer.

   ```
   [edit slot 0 gw-3gpp gx]
   user@host# set address address
   ```

8. Specify the Diameter identifier for the local endpoint that is the originator of the Diameter message.

   ```
   [edit slot 0 gw-3gpp gx]
   user@host# set origin-host origin-host
   ```

9. Specify the Diameter identifier for the realm of the local endpoint that is the originator of the Diameter message.

   ```
   [edit slot 0 gw-3gpp gx]
   user@host# set origin-realm origin-realm
   ```

10. (Optional) Verify your configuration.

    ```
    [edit slot 0 gw-3gpp gx]
    user@host# show
    address 10.10.10.10;
    destination-host testpcrf;
    destination-realm englab.juniper.net;
    diameter-peer [ primary-pcrf secondary-pcrf ];
    origin-host duke;
    origin-realm example;
    port 3868;
    protocol tcp;
    }
    ```

Related Documentation

- SRC 3GPP Gateway Overview on page 7
- Configuration Statements for the SRC 3GPP Gateway on page 55
- Configuring the SRC 3GPP Gateway (SRC CLI) on page 23

Configuring Basic Local Properties for the SRC 3GPP Gateway (SRC CLI)

The local configuration for the SRC 3GPP gateway component defines the directory where the shared configuration is and points to the component namespace.

Use the following configuration statements to configure basic local properties for the SRC 3GPP gateway:

```
slot number gw-3gpp {
  shared shared;
}
```

To configure basic local properties:

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

   ```
   [edit]
   user@host# edit slot 0 gw-3gpp
   ```

2. Specify the configuration namespace for the SRC 3GPP gateway as the path, relative to the root of the static configuration properties, that defines the object for the namespace.

   ```
   [edit slot 0 gw-3gpp]
   user@host# set shared shared
   ```

   For example:

   ```
   [edit slot 0 gw-3gpp]
   user@host# set shared /sample
   ```

   NOTE: All SRC 3GPP gateway instances pointing to the same shared namespace run in the same redundant community.

3. (Optional) Verify your configuration.

   ```
   [edit slot 0 gw-3gpp]
   user@host# show
   ```

Related Documentation

- SRC 3GPP Gateway Overview on page 7
- Configuration Statements for the SRC 3GPP Gateway on page 55
- Configuring Initial Properties for the SRC 3GPP Gateway (SRC CLI) on page 25

Configuring the Object Adapter Internet Address for the SRC 3GPP Gateway (SRC CLI)

Use the following configuration statements to configure the object adapter Internet address:

```
slot number gw-3gpp java-orb object-adapter {
  address address;
}
```

To configure the object adapter Internet address:

1. From configuration mode, access the statement that configures the object adapter Internet address.

   ```
   user@host# edit slot number gw-3gpp java-orb object-adapter
   ```

2. Configure the address of the object adapter.

   ```
   [edit slot number gw-3gpp java-orb object-adapter]
   user@host# set address address
   ```

Related Documentation

- SRC 3GPP Gateway Overview on page 7
- Configuration Statements for the SRC 3GPP Gateway on page 55
- Configuring the SRC 3GPP Gateway (SRC CLI) on page 23

Creating Grouped Configurations for the SRC 3GPP Gateway (SRC CLI)

Configuration groups allow you to share the SRC 3GPP gateway configuration with different SRC 3GPP gateway instances in the SRC network. You can also set up different configurations for different instances.

You can then create a grouped SRC 3GPP gateway configuration that is shared among multiple SRC 3GPP gateway instances. For example, if you create two different SRC 3GPP gateway groups called config1 and config2 within the shared SRC 3GPP gateway configuration, you could select the SRC 3GPP gateway configuration that should be associated with a particular SRC 3GPP gateway instance.

Use the **shared** option of the **slot *number* gw-3gpp** statement to select the group for an SRC 3GPP gateway instance as part of the local configuration. Use the **shared gw-3gpp group *name* configuration** statements to configure the group.

To select and configure a group:

1. From configuration mode, select a group for an SRC 3GPP gateway instance. For example, to select a group called config1 in the root group:

   ```
   [edit]
   user@host# set slot 0 gw-3gpp shared /config1
   ```

2. Commit the configuration.

   ```
   [edit]
   user@host# commit
   commit complete.
   ```

3. From configuration mode, configure a group. For example, to configure a group called config1, specify the group as part of the SRC 3GPP gateway configuration.

   ```
   [edit]
   user@host# edit shared gw-3gpp group config1
   ```

Related Documentation

- Configuring the SRC 3GPP Gateway (SRC CLI) on page 23
- Configuring Basic Local Properties for the SRC 3GPP Gateway (SRC CLI) on page 32
- Configuring Initial Properties for the SRC 3GPP Gateway (SRC CLI) on page 25

Configuring the Subscriber Type (SRC CLI)

Use the following configuration statements to configure the subscriber type:

```
shared gw-3gpp configuration subscriber-types (session-handle) {
  subscriber-id-type (session-handle);
  nic-proxy nic-proxy;
}
```

To configure the subscriber type:

1. From configuration mode, access the statement that configures the subscriber type.

   user@host# **edit shared gw-3gpp configuration subscriber-types session-handle)**

2. Specify the subscriber ID type.

   NOTE: **The only subscriber ID type supported is session-handle.**

   edit shared gw-3gpp configuration subscriber-types session-handle
   user@host# set subscriber-id-type session-handle)

3. Specify the namespace that defines the properties for the NIC proxy operations for the specified subscriber ID type. Each subscriber type must use a different NIC proxy. In this sample procedure, the namespace for the NIC proxy called nic2 is configured.

   edit shared gw-3gpp configuration subscriber-types session-handle
   user@host# set nic-proxy nic2

4. (Optional) Verify your configuration.

   ```
   [edit shared configuration subscriber-types session-handle]
   user@host# show
   nic-proxy nic2;
   subscriber-id-type session-handle;
   ```

Related Documentation

- Configuring the SRC 3GPP Gateway (SRC CLI) on page 23
- Configuring Basic Local Properties for the SRC 3GPP Gateway (SRC CLI) on page 32
- Configuring Initial Properties for the SRC 3GPP Gateway (SRC CLI) on page 25
- Configuring a NIC Proxy for the SRC 3GPP Gateway (SRC CLI) on page 35

Configuring a NIC Proxy for the SRC 3GPP Gateway (SRC CLI)

Tasks to configure the NIC proxy are:

- Configuring Resolution Information for a NIC Proxy on page 36
- Changing the Configuration for the NIC Proxy Cache on page 37

Configuring Resolution Information for a NIC Proxy

You create a NIC proxy for each subscriber type to be configured. Subscriber types that have different subscriber ID types can use the same NIC proxy.

Use the following configuration statements to configure the NIC proxy:

```
shared gw-3gpp configuration nic-proxy-configuration name {
}
shared gw-3gpp configuration nic-proxy-configuration name resolution {
   resolver-name resolver-name;
   key-type key-type;
   value-type value-type;
   expect-multiple-values;
   constraints constraints;
}
```

To configure resolution information for a NIC proxy:

1. From configuration mode, access the statement that configures the NIC proxy configuration. In this sample procedure, the NIC proxy called nic2 is configured.

   user@host# edit shared gw-3gpp configuration nic-proxy-configuration nic2 resolution

2. Specify the path to the NIC resolver that this NIC proxy uses. This resolver must be the same as the one that is configured on the NIC host.

   [edit shared gw-3gpp configuration nic-proxy-configuration nic2 resolution]
   user@host# set resolver-name *resolver-name*

3. Specify the NIC data type that the key provides for the NIC resolution. You can provide a qualifier to a data type to distinguish between different instances of a data type in a resolution scenario, or to provide information about a data type to clarify the use of that data type in a resolution.

   [edit shared gw-3gpp configuration nic-proxy-configuration nic2 resolution]
   user@host# set key-type *key-type*

   NOTE: **The only valid key-type for the SRC 3GPP gateway is SessionHandle.**

4. Specify the type of value to be returned in the resolution for the application that uses the NIC proxy.

   [edit shared gw-3gpp configuration nic-proxy-configuration nic2 resolution]
   user@host# set value-type *value-type*

   For the SRC 3GPP gateway, you must set **value-type** to **SaeId**.

5. (Optional) If the key can have more than one value, specify that the key can have multiple corresponding values.

```
[edit shared gw-3gpp configuration nic-proxy-configuration nic2 resolution]
user@host# set expect-multiple-values
```

6. (Optional. Available at the Advanced editing level.) If the application provides a constraint in the resolution request, specify the data type for the constraint. The constraint represents a condition that must or may be satisfied before the next stage of the resolution process can proceed.

   ```
   [edit shared gw-3gpp configuration nic-proxy-configuration nic2 resolution]
   user@host# set constraints constraints
   ```

   Configure a constraint only if the constraint will be provided by the application in the resolution request. Typically, you do not need to configure constraints.

7. (Optional) Verify your configuration.

   ```
   [edit shared gw-3gpp configuration nic-proxy-configuration nic2 resolution]
   user@host# show
   resolver-name /realms/nic2/A1;
   key-type SessionHandle;
   value-type SaeId;
   ```

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:

```
shared gw-3gpp configuration nic-proxy-configuration name 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 statement that specifies the NIC proxy configuration. In this sample procedure, the NIC proxy called nic2 is configured.

   ```
   user@host# edit shared gw-3gpp configuration nic-proxy-configuration nic2 cache
   ```

2. (Optional) Specify the maximum number of keys for which the NIC proxy retains data.

   ```
   [edit shared gw-3gpp configuration nic-proxy-configuration nic2 cache]
   user@host# set cache-size cache-size
   ```

   If you decrease the cache size or disable the cache while the NIC proxy is running, the NIC proxy removes entries in order of descending age until the cache size meets the new limit.

3. Specify the time interval at which the NIC proxy removes expired entries from its cache.

   ```
   [edit shared gw-3gpp configuration nic-proxy-configuration nic2 cache]
   ```

user@host# **set cache-cleanup-interval** *cache-cleanup-interval*

4. (Optional) Specify how long an entry remains in the cache.

   [edit shared gw-3gpp configuration nic-proxy-configuration nic2 cache]
   user@host# **set cache-entry-age** *cache-entry-age*

5. (Optional) Verify your configuration.

```
[edit shared configuration nic-proxy-configuration nic2 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:

```
shared gw-3gpp configuration nic-proxy-configuration name nic-host-selection {
  groups [groups...];
  selection-criteria (roundRobin | randomPick | priorityList);
}
shared gw-3gpp configuration nic-proxy-configuration name 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 statement that specifies the NIC proxy configuration. In this sample procedure, the NIC proxy called nic2 is configured.

   user@host# **edit shared gw-3gpp configuration nic-proxy-configuration nic2 nic-host-selection**

2. (Optional) Specify the list of groups of NIC hosts that the NIC proxy can contact for resolution requests.

   [edit shared gw-3gpp configuration nic-proxy-configuration nic2 nic-host-selection]
   user@host# **set groups** *groups*

3. (Optional) If you configure more than one group, specify the selection criteria that the NIC proxy uses to determine which NIC host to contact.

   [edit shared gw-3gpp configuration nic-proxy-configuration nic2 nic-host-selection]
   user@host# **set selection-criteria** (roundRobin | randomPick | priorityList)

where:

- roundRobin—NIC proxy selects NIC hosts in a fixed, cyclic order. The NIC proxy always selects the next host in the list.
- randomPick—NIC proxy selects NIC hosts randomly from the list.
- priorityList—NIC proxy selects NIC hosts according to their assigned priorities in the list. If the host with the highest priority in the list is not available, the NIC proxy tries the host with the next-highest priority, and so on.

  Priorities are defined by the order in which you specify the groups. You can change the order of NIC hosts in the list by using the **insert** command.

4. (Optional) Verify your configuration.

```
[edit shared gw-3gpp configuration nic-proxy-configuration nic2
nic-host-selection]
user@host# show
groups ;
selection-criteria round-;
```

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

```
[edit shared gw-3gpp configuration nic-proxy-configuration nic2 nic-host-selection]
user@host# edit blacklisting
[edit shared gw-3gpp configuration nic-proxy-configuration nic2 nic-host-selection
  blacklisting]
```

6. (Optional) Specify whether or not the NIC proxy should contact the next specified NIC host if a NIC host is determined to be unavailable.

```
[edit shared gw-3gpp configuration nic-proxy-configuration nic2 nic-host-selection
  blacklisting]
user@host# set try-next-system-on-error
```

7. (Optional) Change the number of times the NIC proxy tries to communicate with a NIC host before the NIC proxy stops communicating with the NIC host for a period of time. The default is 3.

```
[edit shared gw-3gpp configuration nic-proxy-configuration nic2 nic-host-selection
  blacklisting]
user@host# set number-of-retries-before-blacklisting
  number-of-retries-before-blacklisting
```

8. (Optional) Change the interval at which the NIC proxy attempts to connect to an unavailable NIC host. The default is 15 seconds.

```
[edit shared gw-3gpp configuration nic-proxy-configuration nic2 nic-host-selection
  blacklisting]
user@host# set blacklist-retry-interval blacklist-retry-interval
```

9. (Optional) Verify your configuration.

```
[edit shared gw-3gpp configuration nic-proxy-configuration nic2
nic-host-selection blacklisting]
```

```
user@host# show
try-next-system-on-error;
number-of-retries-before-blacklisting 3;
blacklist-retry-interval 15;
```

Configuring NIC Test Data

To test a resolution without the NIC, you can configure a NIC proxy stub to take the place of the NIC. The NIC proxy stub comprises a set of explicit mappings of data keys and values in the NIC proxy configuration. When the SRC component configured to use a NIC proxy stub passes a specified key to the NIC proxy stub, the NIC proxy stub returns the corresponding value. When you use a NIC proxy stub, no NIC infrastructure is required.

Use the following configuration statements to configure a NIC proxy stub from the **[edit]** hierarchy level.

```
shared gw-3gpp configuration nic-proxy-configuration name test-nic-bindings {
  use-test-bindings;
}
shared gw-3gpp configuration nic-proxy-configuration name test-nic-bindings key-values
  name {
  value;
}
```

To use the NIC proxy stub for the SRC 3GPP gateway:

1. In configuration mode, navigate to the NIC proxy configuration and specify the data type of the key you want to map to a value. In this sample procedure, the key nic2 is specified for the NIC proxy called nic2.

   ```
   [edit shared gw-3gpp configuration nic-proxy-configuration nic2]
   user@host# set resolution key-type nic2
   ```

2. Enable a NIC proxy stub for a resolution.

   ```
   [edit shared gw-3gpp configuration nic-proxy-configuration nic2]
   user@host# set test-nic-bindings use-test-bindings
   ```

3. Specify the values of the keys for testing. These statements are available at the Advanced CLI editing level.

   ```
   [edit shared gw-3gpp configuration nic-proxy-configuration nic2]
   user@host# set test-nic-bindings key-values name value
   ```

   where:

   - *name*—Indicates the NIC data value for the proxy.
   - *value*—Specifies a value for the NIC data type.

   For example, to set up a login name to IP mapping for login name jane@virneo.com to the IP address 192.0.2.30:

   ```
   [edit shared gw-3gpp configuration nic-proxy-configuration nic2]
   user@host# set test-nic-bindings key-values jane@virneo.com 192.0.2.30
   ```

Related Documentation

- *Configuring NIC Test Data (SRC CLI)*

- *Configuring a NIC Proxy for NIC Replication (SRC CLI)*
- Configuration Statements for the SRC 3GPP Gateway on page 55

Configuring the SAE for the SRC 3GPP Gateway

You must configure the SAE to recognize the SRC 3GPP gateway by adding information about it to the SAE properties. Tasks for configuring the SAE for the SRC 3GPP gateway are:

- Configuring the SRC 3GPP Gateway as an External Plug-In on page 41
- Configuring Event Publishers on page 42

Configuring the SRC 3GPP Gateway as an External Plug-In

To configure an external plug-in for the SAE:

1. From configuration mode, access the statement that configures the external plug-ins.

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

2. Configure the object reference of the external plug-in that is exported to the SAE.

   [edit shared sae configuration plug-ins name *name* external]
   user@host# set corba-object-reference *corba-object-reference*

   where ***corba-object-reference*** is one of the following references:

   - Path to the interoperable object reference (IOR) file in the format file:///opt/UMC/3gpp/var/run/3gpp-gw.ior
   - The corbaloc URL in the format corbaloc::*host*:9801/ASGGx/statesync/<namespace> where *host* is the IP address of the C Series Controller or 127.0.0.1
   - Common Object Services (COS) in the format corbaname::*host*:2809/NameService#ASGGx/statesync/<namespace>

3. Specify the plug-in attributes.

   [edit shared sae configuration plug-ins name *name* external]
   user@host# set attributes attribute

   Plug-in attributes for the SRC 3GPP gateway include:

   USER-SESSION-HANDLE

   LOGIN-NAME

   INTERFACE-DESCR

   USER-INET-ADDRESS

   PROPERTY

   SERVICE-SESSION-NAME

   SERVICE-NAME

IN-OCTETS

OUT-OCTETS

TERMINATE-CAUSE

ROUTER-NAME

For more information about configuring plug-in attributes, see *Configuring the SAE for External Plug-Ins (SRC CLI)*.

Configuring Event Publishers

You must configure the SAE to publish the global service-tracking events to the SRC 3GPP gateway. Any other events are ignored.

For information about configuring event publishers, see *Special Types of Event Publishers*.

Related Documentation

- *Configuring the SAE for External Plug-Ins (SRC CLI)*
- *Special Types of Event Publishers*

CHAPTER 4

Configuration Tasks for Logging

Configuring Logging Destinations to Store Messages in a File (SRC CLI)

Use the following configuration statements to configure file logging for the SRC 3GPP gateway:

```
slot number gw-3gpp logger name ...
slot number gw-3gpp 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. In this sample procedure, the logging destination called log1 is configured.

   ```
   user@host# edit slot 0 gw-3gpp logger log1 file
   ```

2. Specify the properties for the logging destination.

   ```
   [edit slot 0 gw-3gpp logger log1 file]
   user@host# set ?
   ```

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

3. (Optional) Verify your configuration.

   ```
   [edit slot 0 gw-3gpp logger log1 file]
   user@host# show
   filter /info-;
   filename var/log/gw-3gpp-info.log;
   rollover-filename var/log/gw-3gpp-info.alt;
   maximum-file-size 2000000;
   ```

Related Documentation

- Configuring Basic Local Properties for the SRC 3GPP Gateway (SRC CLI) on page 32
- Configuring Initial Properties for the SRC 3GPP Gateway (SRC CLI) on page 25
- Configuring Logging Destinations to Send Messages to the System Logging Facility (SRC CLI) on page 44

Configuring Logging Destinations to Send Messages to the System Logging Facility (SRC CLI)

Use the following configuration statements to configure system logging for the SRC 3GPP gateway:

```
slot number gw-3gpp logger name ...
slot number gw-3gpp logger name syslog {
    facility facility
    filter filter;
    format format;
    host host;
    port port;
}
```

To configure logging destinations to send log messages to the system logging facility:

1. From configuration mode, access the statement that configures the name and type of logging destination. In this sample procedure, the logging destination called log2 is configured.

   ```
   user@host# edit slot 0 gw-3gpp logger log2 syslog
   ```

2. Specify the properties for the logging destination.

   ```
   [edit slot 0 gw-3gpp logger log2 syslog]
   user@host# set ?
   ```

   For more information about configuring properties for the logging destination, see *Configuring System Logging (SRC CLI)*.

3. (Optional) Verify your configuration.

   ```
   [edit slot 0 gw-3gpp logger log2 syslog]
   user@host# show
   ```

Related Documentation

- Configuring Basic Local Properties for the SRC 3GPP Gateway (SRC CLI) on page 32
- Configuring Initial Properties for the SRC 3GPP Gateway (SRC CLI) on page 25
- Configuring Logging Destinations to Store Messages in a File (SRC CLI) on page 43

CHAPTER 5

Example

Example: Configuring the SRC 3GPP Gateway

This example describes how to configure the SRC 3GPP gateway.

Requirements

This example uses the following hardware and software components:

- One or more C Series Controllers running the Juniper Networks Session and Resource Control (SRC) software
- One or more MX Series 3D Universal Edge Routers or E Series Broadband Services Routers
- One PCRF
- Junos OS Release 11.4 or later

No special configuration beyond device initialization is required before you can configure this feature.

Before you configure and apply the configurations in this example, be sure you have an understanding of the following:

- SRC 3GPP gateway
- Diameter
- SAE

Overview

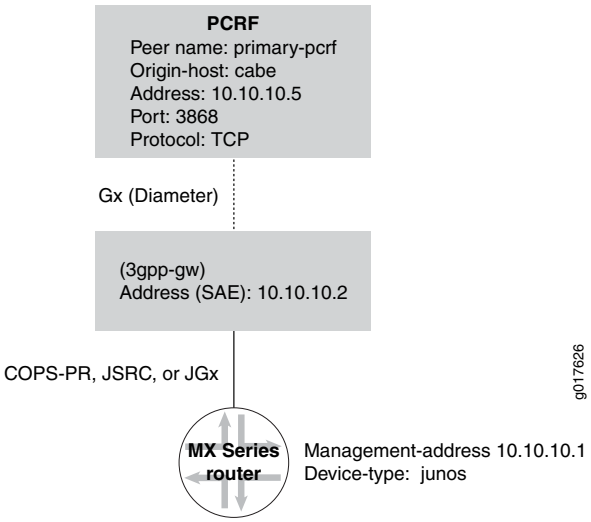
This example does not show all possible configuration choices.

Topology

This example shows how to configure the SRC software for the SRC 3GPP gateway component. The SRC 3GPP gateway is connected to a single PCRF over the Gx interface running the Diameter application. The C Series Controller is also connected to an MX Series router called mx1. In this example, the connection to the mx1 router is using the Junos OS device driver.

This example does not show all possible configuration choices.

Figure 3: SRC 3GPP Gateway Example Topology



Configuration

To configure the SRC 3GPP gateway, perform these tasks:

- Configure the Local Properties for the SRC 3GPP Gateway on page 47
- Configure the Shared Properties for the SRC 3GPP Gateway on page 50
- Adding the PCRF as a Diameter Peer on page 51
- Add the MX Series Router as a Shared Network Device. on page 51
- Configuring the SRC 3GPP Gateway as an External Plug-In for the SAE on page 52

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
set slot 0 gw-3gpp initial directory-connection credentials testing1
set slot 0 gw-3gpp initial directory-connection principal cn=conf,o=operators,o=umc
set slot 0 gw-3gpp initial directory-connection url ldap://127.0.0.1:389
set slot 0 gw-3gpp initial directory-eventing eventing
set slot 0 gw-3gpp gx address 10.10.10.2
set slot 0 gw-3gpp gx diameter-peer primary-pcrf
set slot 0 gw-3gpp gx origin-host duke
set slot 0 gw-3gpp gx origin-realm example.com
```

```
set slot 0 gw-3gpp gx port 3868
set slot 0 gw-3gpp gx protocol tcp
set slot 0 gw-3gpp logger debug file filename var/log/3gpp-gx-debug.log filter /debug
set slot 0 gw-3gpp logger debug file maximum-file-size 1000000
set slot 0 gw-3gpp logger error file filename var/log/3gpp-gx-error.log filter /error
set slot 0 gw-3gpp logger error file maximum-file-size 2000000
set slot 0 gw-3gpp logger error file rollover-filename var/log/3gpp-gx-error.alt
set slot 0 gw-3gpp logger info file filename var/log/3gpp-gx-info.log /info
set slot 0 gw-3gpp logger info file maximum-file-size 2000000
set slot 0 gw-3gpp logger info file rollover-filename var/log/3gpp-gx-info.alt
set slot 0 gw-3gpp shared /3gpp-gw-share
set slot 0 nic hostname DemoHost scenario-name OnePopSessionHandle snmp-agent
  initial directory-connection credentials testing1 principal
  cn=nic,ou=Components,o=Operators url ldap://127.0.0.1:389/
set slot 0 nic hostname DemoHost scenario-name OnePopSessionHandle snmp-agent
  initial directory-eventing eventing
set shared gw-3gpp group 3gpp-gw-share
set shared gw-3gpp group 3gpp-gw-share configuration nic-proxy-configuration
  sessionHdl resolution key-type SessionHandle resolver-name /realms/sessionHandle/A1
  value-type SessionHandle
set shared gw-3gpp group 3gpp-gw-share configuration subscriber-types session-handle
  subscriber-id-type session-handle
set shared network diameter peer primary-pcrf address [ 10.10.10.5 ]
set shared network diameter peer primary-pcrf origin-host cabe
set shared network diameter peer primary-pcrf port 3868
set shared network diameter peer primary-pcrf protocol tcp
set shared network device mx1 device-type junos
set shared network device mx1 management-address 10.10.10.1
set shared network device mx1 virtual-router * sae-connection 10.10.10.2
set shared sae configuration driver junos beep-server-port 3333 tls-beep-server-port
  3434 sdx-group-name sdx sdx-session-group-name sdx-sessions
set shared sae configuration plug-ins name 3gppgw-test external
set corba-object-reference file:///opt/UMC/3gpp/var/run/3gpp-gw.ior
set attributes service-session-name
commit
Exit
enable component gw-3gpp
```

Configure the Local Properties for the SRC 3GPP Gateway

Step-by-Step Procedure

Local properties for the SRC 3GPP gateway include the Gx interface, the connection to the Juniper Networks database directory, the directory-monitoring properties, logging, specifying which group configuration to use for the SRC 3GPP gateway, and configuring the NIC operating properties.

1. Configure the directory-connection properties for the SRC 3GPP gateway.

   ```
   [edit slot 0 gw-3gpp initial directory-connection]
   user@host# set credentials credentials
   user@host# set principal principal
   user@host# set url ldap://127.0.0.1:389
   ```

2. Configure directory-eventing.

   ```
   [edit slot 0 gw-3gpp initial directory-eventing]
   ```

```
user@host# set eventing
```

3. Configure the SRC 3GPP gateway Gx interface:

```
[edit slot 0 gw-3gpp gx]
user@host# set address 10.10.10.2
user@host# set diameter-peer primary-pcrf
user@host# set origin-host duke
user@host# set origin-realm example.com
user@host# set port 3868
user@host# set protocol tcp
```

4. Configure logging.

```
[edit slot 0 gw-3gpp logger debug]
user@host# set file filename var/log/3gpp-gx-debug.log
user@host# set filter /debug-
user@host# set maximum-file-size 1000000
user@host# up
user@host# set logger error file filename var/log/3gpp-gx-error.log
user@host# set filter /error-
user@host# set maximum-file-size 2000000
user@host# set rollover-filename var/log/3gpp-gx-error.alt
user@host# up
user@host# set logger info file filename var/log/3gpp-gx-info.log
user@host# set filter /info-
user@host# set maximum-file-size 2000000
user@host# set rollover-filename var/log/3gpp-gx-info.alt
user@host# up
```

5. Specify the shared group for the local configuration.

```
[edit slot 0 gw-3gpp]
user@host# set shared /3gpp-gw-share
user@host# commit
```

6. Configure the NIC operating properties:

```
[edit slot 0 nic]
user@host# set hostname DemoHost
user@host# set scenario-name OnePopSessionHandle
user@host# set snmp-agent
user@host# edit initial directory-connection
[edit slot 0 nic initial directory-connection]
user@host# set credentials testing1
user@host# set principal cn=nic,ou=Components,o=Operators
user@host# set url ldap://127.0.0.1:389/
user@host# up
user@host# edit initial directory-eventing
[edit slot 0 nic initial directory-eventing]
user@host# set eventing
user@host# up
user@host# up
user@host# commit
```

Results Confirm the local configuration properties. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit slot 0 gw-3gpp]
user@duke# show
gx {
  address 10.10.10.2;
  diameter-peer primary-pcrf;
  origin-host duke;
  origin-realm example.com;
  port 3868;
  protocol tcp;
}
initial {
  directory-connection {
    backup-urls '';
    credentials ********;
    principal cn=conf,o=operators,o=umc;
    url ldap://127.0.0.1:389/;
  }
  directory-eventing {
    eventing;
    polling-interval 30;
  }
}
logger debug {
  file {
    filename var/log/3gpp-gx-debug.log;
    filter /debug-;
    maximum-file-size 1000000;
  }
}
logger error {
  file {
    filename var/log/3gpp-gx-error.log;
    filter /error-;
    maximum-file-size 2000000;
    rollover-filename var/log/3gpp-gx-error.alt;
  }
}
logger info {
  file {
    filename var/log/3gpp-gx-info.log;
    filter /info-;
    maximum-file-size 2000000;
    rollover-filename var/log/3gpp-gx-info.alt;
  }
}
shared /3gpp-gw-share;

[edit slot 0 gw-3gpp]
user@duke#

[edit slot 0 nic]
user@duke# show
base-dn o=umc;
hostname DemoHost;
initial {
  directory-connection {
    backup-urls '';
    credentials ********;
```

```
    principal cn=nic,ou=Components,o=Operators,<base>;
url ldap://10.10.10.10:389/;
  }
  directory-eventing {
    eventing;
    polling-interval 15;
  }
}
scenario-name OnePopSessionHandle;
snmp-agent;

[edit slot 0 nic]
user@duke#
```

Configure the Shared Properties for the SRC 3GPP Gateway

Step-by-Step Procedure

Configure the shared properties for the SRC 3GPP gateway including the shared group configuration, NIC proxy configuration, and subscriber type.

1. Specify the group to configure:

   ```
   [edit shared gw-3gpp]
   user@host# edit group 3gpp-gw-share
   ```

2. Configure the NIC proxy configuration:

   ```
   [edit shared gw-3gpp group 3gpp-gw-share configuration]
   user@host# edit nic-proxy-configuration sessionHdl resolution
   [edit shared gw-3gpp group 3gpp-gw-share configuration nic-proxy-configuration
     sessionHdl resolution]
   user@host# set key-type SessionHandle
   user@host# set resolver-name /realms/sessionHandle/A1
   user@host# set value-type SessionHandle
   ```

3. Configure the subscriber type:

   ```
   [edit shared gw-3gpp]
   user@host# edit configuration subscriber-types session-handle
   [edit shared gw-3gpp group 3gpp-gw-share configuration subscriber-types
     session-handle]
   user@host# set subscriber-id-type session-handle
   ```

Results

Confirm the shared configuration properties. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit shared gw-3gpp group 3gpp-gw-share]
user@duke show
configuration {
  nic-proxy-configuration {
    sessionHdl {
      resolution {
        key-type SessionHandle;
        resolver-name /realms/sessionHandle/A1;
        value-type SaeId;
      }
    }
  }
```

```
  subscriber-types {
    session-handle {
      nic-proxy sessionHdl;
      subscriber-id-type session-handle;
    }
  }
}

[edit shared gw-3gpp group 3gpp-gw-share]
user@duke#
```

Adding the PCRF as a Diameter Peer

Step-by-Step Procedure

You must specify the PCRF as a Diameter peer. This example uses a single PCRF, which connects to the C Series Controller over the SRC 3GPP gateway Gx interface using the Diameter application.

1. To add the PCRF as a Diameter peer:

```
[edit shared network diameter peer]
user@host# edit primary-pcrf
[edit shared network diameter peer primary-pcrf]
user@host# set address [ 10.10.10.5 ]
user@host# set origin-host cabe
user@host# set port 3868
user@host# set protocol tcp
```

Results

From configuration mode, confirm the configuration for the PCRFs. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit shared network diameter peer primary-pcrf]
user@duke# show
address [ 10.10.10.5 ];
connect-timeout 10;
origin-host cabe;
port 3868;
protocol tcp;

[edit shared network diameter peer primary-pcrf]
user@duke#
```

Add the MX Series Router as a Shared Network Device.

Step-by-Step Procedure

Add the MX Series router as a shared network device using the Junos OS device driver.

1. Add the MX Series router as a shared network device.

```
[edit shared network device mx1]
user@host# set management-address 10.10.10.1
user@host# set device-type junos
user@host# set virtual-router * sae-connection 10.10.10.2
user@host# commit
```

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

```
[edit shared network device mx1]
```

```
user@host# top
user@host# edit shared sae configuration driver junos
user@host# set beep-server-port 3333
user@host# set tls-beep-server-port 3434
user@host# set sdx-group-name sdx
user@host# set sdx-session-group-name sdx-sessions
user@host# commit
```

Results

```
[edit shared network device mx1]
user@duke# show
device-type junos;
management-address 10.10.10.1;
virtual-router * {
  sae-connection 10.10.10.2;
}

[edit shared network device mx1]
user@duke#

[edit shared sae configuration driver junos]
user@host# show
beep-server-port 3333;
tls-beep-server-port 3434;
connection-attempts 50;
keepalive-interval 45;
message-timeout 30000;
batch-size 10;
transaction-batch-time 2000;
sdx-group-name sdx;
sdx-session-group-name sdx-sessions;
send-commit-check true;

[edit shared sae configuration driver junos]
user@duke#
```

Configuring the SRC 3GPP Gateway as an External Plug-In for the SAE

Step-by-Step Procedure

1. Configure the SRC 3GPP gateway as an external plug-in for the SAE.

```
user@host# edit shared sae configuration plug-ins name 3gppgw-test external
user@host# set corba-object-reference file:///opt/UMC/3gpp/var/run/3gpp-gw.ior
user@host# set attributes service-session-name
user@host# commit
```

Results

```
[edit shared sae configuration plug-ins name 3gppgw-test external]
user@duke# show
attributes service-session-name;
corba-object-reference file:///opt/UMC/3gpp/var/run/3gpp-gw.ior;

[edit shared sae configuration plug-ins name 3gppgw-test external]
user@duke#
```

Related Documentation

- Configuration Statements for the SRC 3GPP Gateway on page 55
- Configuring the SRC 3GPP Gateway (SRC CLI) on page 23

- SRC 3GPP Gateway Overview on page 7

CHAPTER 6

Configuration Statements and Commands

Configuration Statements for the SRC 3GPP Gateway

Use the following configuration statements to configure the SRC 3GPP gateway at the **[edit]** hierarchy level.

```
slot number gw-3gpp {
   shared shared;
}
slot number gw-3gpp gx {
   destination-host destination-host;
   destination-realm destination-realm;
   diameter-peer [diameter-peer.....];
   protocol (tcp | sctp);
   port port;
   address address;
   origin-host origin-host;
   origin-realm origin-realm;
}
slot number gw-3gpp initial {
   static-dn static-dn;
   dynamic-dn dynamic-dn;
}
slot number gw-3gpp initial directory-connection {
   url url;
   backup-urls [backup-urls...];
   principal principal;
   credentials credentials;
   protocol (ldaps);
   timeout timeout;
   check-interval check-interval;
   blacklist;
   snmp-agent;
}
slot number gw-3gpp initial directory-eventing {
   eventing;
   signature-dn signature-dn;
   polling-interval polling-interval;
```

```
    event-base-dn event-base-dn;
    dispatcher-pool-size dispatcher-pool-size;
}
slot number gw-3gpp java-orb object-adapter {
    address address;
}
slot number gw-3gpp logger name file {
    filter filter;
    filename filename;
    rollover-filename rollover-filename;
    maximum-file-size maximum-file-size;
}
slot number gw-3gpp logger name syslog {
    facility facility
    filter filter;
    format format;
    host host;
    port port;
}
shared gw-3gpp group name
shared gw-3gpp configuration subscriber-types (session-handle) {
    subscriber-id-type (session-handle);
    nic-proxy nic-proxy;
}
shared gw-3gpp configuration nic-proxy-configuration name {
}
shared gw-3gpp configuration nic-proxy-configuration name resolution {
    resolver-name resolver-name;
    key-type key-type;
    value-type value-type;
    expect-multiple-values;
    constraints constraints;
}
shared gw-3gpp configuration nic-proxy-configuration name cache {
    cache-size cache-size;
    cache-cleanup-interval cache-cleanup-interval;
    cache-entry-age cache-entry-age;
}
shared gw-3gpp configuration nic-proxy-configuration name nic-host-selection {
    groups [groups...];
    selection-criteria (roundRobin | randomPick | priorityList);
}
shared gw-3gpp configuration nic-proxy-configuration name 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;
}
shared gw-3gpp configuration nic-proxy-configuration name test-nic-bindings {
    use-test-bindings;
}
shared gw-3gpp configuration nic-proxy-configuration name test-nic-bindings key-values
    name {
    value;
}
```

Related Documentation

- Configuring the SRC 3GPP Gateway (SRC CLI) on page 23
- SRC 3GPP Gateway Overview on page 7
- Mapping Between SRC Software, Junos OS, and PCC Concepts on page 13
- Configuring the SRC 3GPP Gateway Gx Interface (SRC CLI) on page 31

PART 3

Administration

CHAPTER 7

Managing the SRC 3GPP Gateway

Starting the SRC 3GPP Gateway (SRC CLI)

To start the SRC 3GPP gateway:

```
user@host> enable component gw-3gpp
```

The system responds with a start message. If the SRC 3GPP gateway is already running, the system responds with a warning message.

Related Documentation

- SRC 3GPP Gateway Overview on page 7
- Configuring the SRC 3GPP Gateway (SRC CLI) on page 23
- Restarting the SRC 3GPP Gateway (SRC CLI) on page 61
- Stopping the SRC 3GPP Gateway (SRC CLI) on page 62

Restarting the SRC 3GPP Gateway (SRC CLI)

You must restart the SRC 3GPP gateway after you commit a configuration change.

To restart the SRC 3GPP gateway:

```
user@host> restart component gw-3gpp
```

The system responds with a start message. If the SRC 3GPP gateway is already running, the system responds with a shutdown message and then a start message.

Related Documentation

- SRC 3GPP Gateway Overview on page 7
- Configuring the SRC 3GPP Gateway (SRC CLI) on page 23
- Starting the SRC 3GPP Gateway (SRC CLI) on page 61
- Stopping the SRC 3GPP Gateway (SRC CLI) on page 62

Stopping the SRC 3GPP Gateway (SRC CLI)

To stop the SRC 3GPP gateway:

```
user@host> disable component gw-3gpp
```

The system responds with a shutdown message. If SRC 3GPP gateway is not running when you issue the command, the system responds with the command prompt.

Related Documentation

- SRC 3GPP Gateway Overview on page 7
- Configuring the SRC 3GPP Gateway (SRC CLI) on page 23
- Restarting the SRC 3GPP Gateway (SRC CLI) on page 61
- Starting the SRC 3GPP Gateway (SRC CLI) on page 61

PART 4

Index

Index

Symbols

C

D

E

L