Subscriber Management in a Wireless Roaming Environment
# Table of Contents

About the Documentation ............................................. ix
   Documentation and Release Notes ................................ ix
   Supported Platforms ................................................. ix
   Documentation Conventions ....................................... ix
   Documentation Conventions ..................................... x
   Documentation Feedback .......................................... xii
   Requesting Technical Support .................................. xii
      Self-Help Online Tools and Resources ....................... xiii
   Opening a Case with JTAC ....................................... xiii

Part 1  Overview

Chapter 1  Software Features Overview .......................... 3
   SRC Component Overview ........................................ 3

Chapter 2  Wireless Roaming ........................................ 9
   Wireless Roaming Environment Overview ....................... 9
   Subscriber Access in a Wireless Roaming Environment .......... 9

Part 2  Configuration

Chapter 3  Configuration Task for Subscriber Access for Wireless Location .......... 13
   Configuring Subscriber Access for a Wireless Location .......... 13
      Configuring RADIUS Authentication .......................... 13
      Creating Subscriber Access to an ISP ......................... 16
      Creating Web Access ........................................... 16
      Setting Idle Timeout Options for the SAE .................... 17

Part 3  Index

   Index .......................................................................... 21
List of Figures

Part 1 Overview
Chapter 2 Wireless Roaming ............................................................... 9

Figure 1: Subscriber Access to a Wireless Roaming Group ...................... 10
# List of Tables

About the Documentation ................................................. ix
Table 1: Notice Icons ......................................................... x
Table 2: Notice Icons ......................................................... xi
Table 3: Text Conventions .................................................... xi

## Part 1 Overview

### Chapter 1 Software Features Overview

Table 4: Descriptions of SRC Components ............................ 3

## Part 2 Configuration

### Chapter 3 Configuration Task for Subscriber Access for Wireless Location

Table 5: Packet Types for RADIUS Attributes ........................... 15
About the Documentation

- Documentation and Release Notes on page ix
- Supported Platforms on page ix
- Documentation Conventions on page ix
- Documentation Feedback on page xii
- Requesting Technical Support on page xii

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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon" alt="i" /></td>
<td>Informational note</td>
<td>Indicates important features or instructions.</td>
</tr>
<tr>
<td><img src="icon" alt="⚠️" /></td>
<td>Caution</td>
<td>Indicates a situation that might result in loss of data or hardware damage.</td>
</tr>
<tr>
<td><img src="icon" alt="⚠️⚡️" /></td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td><img src="icon" alt="⚠️🌟" /></td>
<td>Laser warning</td>
<td>Alerts you to the risk of personal injury from a laser.</td>
</tr>
<tr>
<td><img src="icon" alt="💡" /></td>
<td>Tip</td>
<td>Indicates helpful information.</td>
</tr>
<tr>
<td><img src="icon" alt="💡🌟" /></td>
<td>Best practice</td>
<td>Alerts you to a recommended use or implementation.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Info Icon]</td>
<td>Informational note</td>
<td>Indicates important features or instructions.</td>
</tr>
<tr>
<td>![Caution Icon]</td>
<td>Caution</td>
<td>Indicates a situation that might result in loss of data or hardware damage.</td>
</tr>
<tr>
<td>![Warning Icon]</td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td>![Laser Warning Icon]</td>
<td>Laser warning</td>
<td>Alerts you to the risk of personal injury from a laser.</td>
</tr>
<tr>
<td>![Tip Icon]</td>
<td>Tip</td>
<td>Indicates helpful information.</td>
</tr>
<tr>
<td>![Best Practice Icon]</td>
<td>Best practice</td>
<td>Alerts you to a recommended use or implementation.</td>
</tr>
</tbody>
</table>

Table 3: Text Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold text like this</strong></td>
<td>Represents keywords, scripts, and tools in text. Represents a GUI element that the user selects, clicks, checks, or clears.</td>
<td>• Specify the keyword <code>exp-msg</code>. • Run the <code>install.sh</code> script. • Use the <code>pkgadd</code> tool. • To cancel the configuration, click <code>Cancel</code>.</td>
</tr>
<tr>
<td><strong>Bold text like this</strong></td>
<td>Represents text that the user must type.</td>
<td><code>user@host# set cache-entry-age cache-entry-age</code></td>
</tr>
<tr>
<td><strong>Fixed-width text like this</strong></td>
<td>Represents information as displayed on your terminal's screen, such as CLI commands in output displays.</td>
<td><code>nic-locators { login { resolution { resolver-name /realms/login/A1; key-type LoginName; value-type SaeId; } }</code></td>
</tr>
<tr>
<td><strong>Regular sans serif typeface</strong></td>
<td>Represents configuration statements. Indicates SRC CLI commands and options in text. Represents examples in procedures. Represents URLs.</td>
<td>• <code>system ldap server{ stand-alone;</code> • Use the <code>request sae modify device failover command</code> with the <code>force</code> option • <code>user@host# ...</code> • <code>http://www.juniper.net/techpubs/software/management/sdx/api-index.html</code></td>
</tr>
</tbody>
</table>
Table 3: Text Conventions (continued)

<table>
<thead>
<tr>
<th><strong>Italic sans serif typeface</strong></th>
<th>Represents variables in SRC CLI commands.</th>
<th>user@host# set local-address local-address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Angle brackets</td>
<td>In text descriptions, indicate optional keywords or variables.</td>
<td>Another runtime variable is &lt;gfwif&gt;.</td>
</tr>
<tr>
<td>Key name</td>
<td>Indicates the name of a key on the keyboard.</td>
<td>Press Enter.</td>
</tr>
<tr>
<td>Key names linked with a plus sign (+)</td>
<td>Indicates that you must press two or more keys simultaneously.</td>
<td>Press Ctrl + b.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Backslash</th>
<th>At the end of a line, indicates that the text wraps to the next line.</th>
<th>Plugin.radiusAcct-1.class=\net.juniper.smgt.sae.plugin\RadiusTrackingPluginEvent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Words separated by the</td>
<td>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.)</td>
<td>diagnostic</td>
</tr>
</tbody>
</table>

**Documentation Feedback**

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

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

**Requesting Technical Support**

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

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

- Software Features Overview on page 3
- Wireless Roaming on page 9
CHAPTER 1

Software Features Overview

• SRC Component Overview on page 3

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Components</td>
<td></td>
</tr>
<tr>
<td>Service activation engine (SAE)</td>
<td>• Authorizes, activates, and deactivates subscriber and service sessions by interacting with systems such as Juniper Networks routers, cable modern termination system (CMTS) devices, RADIUS servers, and directories.</td>
</tr>
<tr>
<td></td>
<td>• Collects accounting information about subscribers and services from routers, and stores the information in RADIUS accounting servers, flat files, and other accounting databases.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Subscriber Information Collector (SIC)</td>
<td>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.</td>
</tr>
<tr>
<td>Juniper Policy Server (JPS)</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 4: Descriptions of SRC Components  (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network information collector (NIC)</td>
<td>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.</td>
</tr>
<tr>
<td>Redirect Server</td>
<td>Redirects HTTP requests received from IP Filter to a captive portal page.</td>
</tr>
<tr>
<td>3GPP Gateway</td>
<td>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. The Gx interface on the SRC 3GPP gateway communicates with the PCRF using the Diameter protocol.</td>
</tr>
<tr>
<td>Web Application Service</td>
<td>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.</td>
</tr>
<tr>
<td>Web Services Gateway</td>
<td>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.</td>
</tr>
<tr>
<td>Repository</td>
<td>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.</td>
</tr>
<tr>
<td>Session State Registrar (SSR)</td>
<td>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.</td>
</tr>
<tr>
<td>SRC Configuration and Management Tools</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 4: Descriptions of SRC Components (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C-Web interface</td>
<td>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.</td>
</tr>
<tr>
<td>Simple Network Management Protocol (SNMP) agent</td>
<td>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.</td>
</tr>
<tr>
<td>Service Management Applications (Run on external system)</td>
<td></td>
</tr>
<tr>
<td>IMS Services Gateway</td>
<td>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.</td>
</tr>
<tr>
<td>SRC Programming Interfaces</td>
<td></td>
</tr>
<tr>
<td>NETCONF API</td>
<td>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.</td>
</tr>
<tr>
<td>CORBA plug-in service provider interface (SPI)</td>
<td>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.</td>
</tr>
<tr>
<td>CORBA remote API</td>
<td>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.</td>
</tr>
<tr>
<td>NIC access API</td>
<td>Performs NIC resolutions. Applications that use these extensions to the SRC software run on a system other than a C Series Controller.</td>
</tr>
<tr>
<td>SAE core API</td>
<td>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.</td>
</tr>
<tr>
<td>Script services</td>
<td>Provides an interface to call scripts that supply custom services such as provisioning policies on a number of systems across a network.</td>
</tr>
<tr>
<td>VTA API</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 4: Descriptions of SRC Components (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authorization and Accounting Applications</strong></td>
<td></td>
</tr>
<tr>
<td>AAA RADIUS servers</td>
<td>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.</td>
</tr>
<tr>
<td>SRC Admission Control Plug-In (SRC ACP)</td>
<td>Authorizes and tracks subscribers’ use of network resources associated with services that the SRC application manages.</td>
</tr>
<tr>
<td>Flat file accounting</td>
<td>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.</td>
</tr>
<tr>
<td>Volume Tracking Application</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Demonstration Applications (available on the Juniper Networks Web site)</strong></td>
<td></td>
</tr>
<tr>
<td>Enterprise Audit Plug-In</td>
<td>Defines a callback interface, which receives events when IT managers complete specified operations.</td>
</tr>
<tr>
<td>Enterprise Manager Portal</td>
<td>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.</td>
</tr>
<tr>
<td>Monitoring Agent application</td>
<td>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.</td>
</tr>
<tr>
<td>Residential service selection portals</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 4: Descriptions of SRC Components (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample enterprise service portal</td>
<td>Lets service providers supply an interface to their business customers for managing and provisioning services.</td>
</tr>
</tbody>
</table>

**Related Documentation**
- *SRC Product Description*
Wireless Roaming Environment Overview

In a roaming wireless environment, subscribers can log in to a wireless access point at a variety of wireless locations owned by service providers that participate in a roaming network agreement. The wireless locations participating in the agreement can be owned by one or more service providers.

Typically, RADIUS manages information about subscribers between the wireless locations. A RADIUS server for an Internet service provider (ISP) manages authentication for its subscribers, and shares information with the other ISPs with which the service provider has a roaming agreement. Subscribers can log in to an service activation engine (SAE) from any supported site.

The SAE provides support for RADIUS vendor-specific attributes for wireless Internet service provider roaming (WISPr).

Related Documentation

- Subscriber Access in a Wireless Roaming Environment on page 9
- Configuring Subscriber Access for a Wireless Location on page 13
- For more information about RADIUS vendor-specific attributes for wireless Internet service provider roaming (WISPr): http://www.wi-fialliance.org/opensection/wispr.asp

Subscriber Access in a Wireless Roaming Environment

When subscribers log in to a wireless location that has a roaming agreement with other locations, the following sequence of events occurs:

1. Subscribers connect to the local wireless location and provide login information on a portal page that provides a universal access method. This login information is forwarded to the SAE.
2. Based on the login information, an access service starts.
3. The subscriber is authenticated by RADIUS; the authorization includes RADIUS vendor-specific attributes for WISPr.
4. Policies are activated for the subscriber on the router.

5. After successful start of the access service, the portal page redirects the subscriber to a specified start page.

Figure 1 on page 10 shows how subscribers interact with an SAE-managed wireless location that has a roaming agreement with wireless locations.

Figure 1: Subscriber Access to a Wireless Roaming Group

Related Documentation

- Wireless Roaming Environment Overview on page 9
- Configuring Subscriber Access for a Wireless Location on page 13
PART 2

Configuration

- Configuration Task for Subscriber Access for Wireless Location on page 13
CHAPTER 3

Configuration Task for Subscriber Access for Wireless Location

- Configuring Subscriber Access for a Wireless Location on page 13

Configuring Subscriber Access for a Wireless Location

Tasks to use the SAE to manage a wireless access point that participates in a roaming agreement are:

1. Configuring RADIUS Authentication on page 13
2. Creating Subscriber Access to an ISP on page 16
3. Creating Web Access on page 16
4. Setting Idle Timeout Options for the SAE on page 17

Configuring RADIUS Authentication

You configure RADIUS authentication for users who connect from a wireless location, and set up RADIUS authentication to support a roaming environment between wireless Internet service providers. You can use the Flexible RADIUS Authentication plug-in that is provided with the SRC software, or you can create a custom RADIUS authentication plug-in.

Configuring a Custom RADIUS Authentication Plug-In

If you create a custom plug-in, be sure that it supports the same RADIUS attributes as those configured for the flexible RADIUS authentication plug-in. See “Configuring the Flexible RADIUS Authentication Plug-In” on page 13.

For information about creating a custom plug-in, see SAE CORBA Plug-In Service Provider Interface (SPI) on the Juniper Networks Web site at:
http://www.juniper.net/techpubs/software/management/src/api-index.html

Configuring the Flexible RADIUS Authentication Plug-In

The default flexible RADIUS authentication plug-in, flexRadiusAuth, provides support for RADIUS vendor-specific attributes for WISPr, which are listed in the following procedure. These attributes use the IANA private enterprise number 14122 assigned to the Wi-Fi Alliance. For more information about these attributes, see
http://www.wi-fialliance.org/opensection/wispr.asp

Copyright © 2014, Juniper Networks, Inc.
You should be familiar with the general procedure for configuring the flexible RADIUS authentication plug-in before configuring it to include the WISPr attributes. For information about configuring the flexible RADIUS authentication plug-in, see Configuring Tracking Plug-Ins (SRC CLI).

When you configure the plug-in, you can use the following standard attribute values to set values in authentication response packets:

- `setAcctInterimTime`
- `setSubstitution`
- `setTerminateTime`

Examples in the following procedure show how you can use these attribute values.

To configure the plug-in to support a roaming environment:

1. Configure attributes.
   - Required attributes:
     
     - An identifier for the wireless location:
       ```
       vendor-specific.WISPr.Location-ID=Identifier
       ```
       This attribute can be an interface description (ifAlias) or other value that identifies the JunosE interface to which the wireless access point connects.
     
     - The URL of the start page returned by the RADIUS server of the ISP:
       ```
       vendor-specific.WISPr.Redirection-URL=Command to make the URL available to the SRC software
       ```
       For example:
       ```
       vendor-specific.WISPr.Redirection-URL=setProperty(" startURL=%s" % ATTR)
       ```
       The default configuration sets a session property named startURL.
     
     - The URL of a page that a subscriber can use to log out of the network:
       ```
       vendor-specific.WISPr.Logoff-URL=URL of a log out page
       ```
   
   - Bandwidth attributes (recommended):
     
     - The maximum transmission rate in bits per second:
       ```
       vendor-specific.WISPr.Bandwidth-Max-Up=Command to make the rate available to the SRC software
       ```
       For example:
       ```
       vendor-specific.WISPr.Bandwidth-Max-Up=setSubstitution(" max_up_rate=%s" % ATTR)
       ```
     
     - The maximum receive rate in bits per second:
       ```
       vendor-specific.WISPr.Bandwidth-Max-Down=Command to make the rate available to the SRC software
       ```
       For example:
vendor-specific.WISPr.Bandwidth-Max-Down=setSubstitution("max_down_rate=%s" % \ ATTR)

- Optional attributes:
  - The name of the wireless location:
    vendor-specific.WISPr.Location-Name=Name of the wireless location
  - The date and time that the subscriber session is to end:
    vendor-specific.WISPr.Session-Terminate-Time=Command to set the session terminate time
    For example:
    vendor-specific.WISPr.Session-Terminate-Time=setTerminateTime(ATTR)
  - The end of the subscriber session at the end of the billing day:
    vendor-specific.WISPr.Session-Terminate-End-Of-Day=ATTR or setTerminateTime("00:00:00")
    If the operator of the wireless location does not support daily billing, do not configure this attribute, and remove it if present.
  - A service type for billing:
    vendor-specific.WISPr.Billing-Class-Of-Service=Service type

2. For each attribute that you configure, configure the packet type to which the attribute applies. Table 5 on page 15 shows the packet types associated with each attribute.

Table 5: Packet Types for RADIUS Attributes

<table>
<thead>
<tr>
<th>RADIUS Attribute</th>
<th>Associated RADIUS Packet Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>vendor-specific.WISPr.Location-ID</td>
<td>RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Location-ID</td>
</tr>
<tr>
<td>vendor-specific.WISPr.Redirection-URL</td>
<td>RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Redirection-URL</td>
</tr>
<tr>
<td>vendor-specific.WISPr.Logoff-URL</td>
<td>RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Logoff-URL</td>
</tr>
<tr>
<td>vendor-specific.WISPr.Location-Name</td>
<td>RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Location-Name</td>
</tr>
<tr>
<td>vendor-specific.WISPr.Session-Terminate-Time</td>
<td>RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Session-Terminate-Time</td>
</tr>
<tr>
<td>vendor-specific.WISPr.Session-Terminate-End-Of-Day</td>
<td>RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Session-Terminate-End-Of-Day</td>
</tr>
</tbody>
</table>
Creating Subscriber Access to an ISP

Configure a service that lets subscribers connect to an ISP through a captive portal, a single Web page to which subscribers connect. The policies associated with the service should specify a Junos OS policing or JunosE rate-limiting policy to set the maximum bandwidth at which:

- A subscriber can send traffic.
- A subscriber can receive traffic.

When you configure the policies, define the bandwidth values as parameters so that the policies can be applied across a number of subscribers.

To configure a service to access the ISP:

1. Create the SRC service to use RADIUS authentication.
   
   See Adding a Normal Service (SRC CLI).

2. Create a policy group the sets the maximum bandwidth at which a subscriber can send traffic, and the maximum bandwidth at which a subscriber can receive traffic. Use parameters to set these values.

   To configure policies, see:

   - Configuring Policy Groups (SRC CLI)
   - Configuring Global Parameters (SRC CLI)
   - Configuring Local Parameters (SRC CLI)

For example, you can create a policy configuration that includes:

- A local parameter named max_up_rate that sets the maximum rate at which the subscriber can send data
- A local parameter named max_down_rate that sets the maximum rate at which the subscriber can receive data
- A policy group Receive(Downstream) that references max_down_rate
- A policy group Send(Upstream) that references max_up_rate

Substitutions for these parameters can then be referenced in the RADIUS attributes:

```plaintext
vendor-specific.WISPr.Bandwidth-Max-Up=setSubstitution("max_up_rate=%s" % ATTR)
vendor-specific.WISPr.Bandwidth-Max-Down=setSubstitution("max_down_rate=%s" % ATTR)
```

Creating Web Access

When subscribers connect to and log in to a wireless access point, they are directed to a single Web page that is referred to as a captive portal page. This page is part of a service selection portal. A captive portal page receives and manages redirected Web requests.
The SRC Application Library provides an unsupported, demonstration application for a residential service selection portal.

When creating a captive portal page for a wireless roaming environment, configure the page to:

- Start an access service that is configured to be authenticated by the RADIUS server of the ISP.
- After the access service starts, redirect the subscriber to the page specified by the Redirect-URL RADIUS attribute. This page is the start page for the subscriber's home ISP.

You can retrieve the URL of the start page from the service session property startURL. Note that startURL is the default name used for the flexible RADIUS authentication plug-in; you can assign a different name to this property.

You can use the Subscriber.readSubscription() method in the Common Object Request Broker Architecture (CORBA) remote application programming interface (API) to retrieve the redirect URL.

Note that when you develop the portal, you can use the following methods in the SAE CORBA remote API to retrieve session data after the access service starts:

- Subscriber.readSubscriber()
- Subscriber.readSubscription()

For more information about these methods, see the SAE CORBA remote API documentation on the Juniper Networks Web site at http://www.juniper.net/techpubs/software/management/src/api-index.html.

Setting Idle Timeout Options for the SAE

You can configure the following options to ensure that the timeout values are consistent with the requirements for your environment:

- Idle timeout—Defines how long a session is idle before the connection is closed.
- Adjust session time—Adjusts the session time reported in an accounting message by subtracting idle time from the time if the session times out.

To configure the timeout settings:

1. Configure the service activation authentication through a RADIUS server to return an idle timeout. This configuration requires that the RADIUS server returns the idle timeout vendor-specific attribute (VSA).
   
   or

Configure the idle timeout in the SRC service definition. For example:

```
[edit services global service service1]
user@host# set idle-timeout 5
```
Although an interval up to 5 minutes is typically recommended, for the SRC software, we recommend a minimum of 15 minutes.

2. Configure the `adjust-session-time` statement for the SAE to ensure that session time is accurately reported for accounting purposes. For example:

```plaintext
[edit shared sae group wireless configuration]
user@host# set idle-timeout adjust-session-time
```

Related Documentation
- Wireless Roaming Environment Overview on page 9
- Subscriber Access in a Wireless Roaming Environment on page 9
PART 3

Index

- Index on page 21