Chapter 2

Managing Subscribers for a Wireless Roaming Environment

This chapter describes how you can use the SAE to manage wireless locations that support roaming from one wireless location to another. Topics include:

- Overview of a Wireless Roaming Environment on page 21
- Subscriber Access in a Wireless Roaming Environment on page 22
- Configuring Subscriber Access for a Wireless Location on page 23

Overview of a Wireless Roaming Environment

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 SAE from any supported site.

The SAE provides support for RADIUS vendor-specific attributes for wireless Internet service provider roaming (WISPr). For more information about these attributes, see

http://www.wi-fialliance.org/opensection/wispr.asp

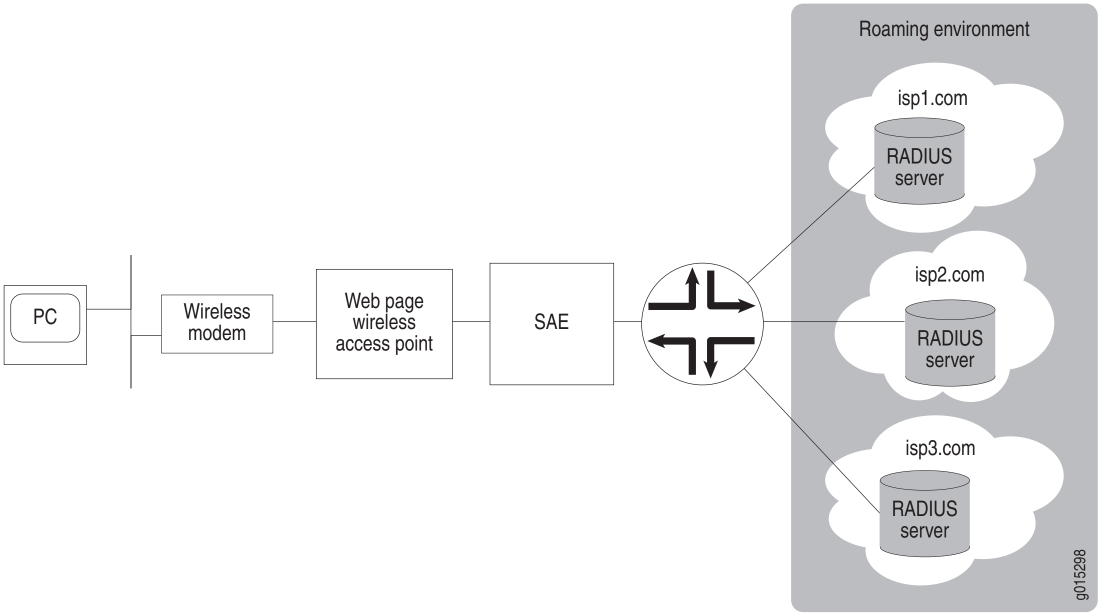
Subscriber Access in a Wireless Roaming Environment

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 4 shows how subscribers interact with an SAE-managed wireless location that has a roaming agreement with wireless locations.

Figure 4: Subscriber Access to a Wireless Roaming Group



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 23
2. Creating Subscriber Access to an ISP on page 26
3. Creating Web Access on page 28
4. Setting Idle Timeout Options for the SAE on page 29

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 23.

For information about creating a custom plug-in, see *SAE CORBA Plug-In Service Provider Interface (SPI)* in the SRC software distribution in the folder *SDK/doc/idl* or on the Juniper Networks Web site at

http://www.juniper.net/techpubs/software/management/sdx/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

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 *SRC-PE Subscribers and Subscriptions Guide, Chapter 11, Configuring Accounting and Authentication Plug-Ins with the 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 bites 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 bites 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 6 shows the packet types associated with each attribute.

Table 6: Packet Types for RADIUS Attributes

RADIUS Attribute	Associated RADIUS Packet Definition
vendor-specific.WISPr.Location-ID	RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Location-ID
vendor-specific.WISPr.Redirection-URL	RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Redirection-URL
vendor-specific.WISPr.Logoff-URL	RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Logoff-URL
vendor-specific.WISPr.Bandwidth-Max-Up	RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Bandwidth-Max-Up
vendor-specific.WISPr.Maximum-Max-Down	RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Maximum-Max-Down
vendor-specific.WISPr.Location-Name	RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Location-Name
vendor-specific.WISPr.Session-Terminate-Time	RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Session-Terminate-Time

Table 6: Packet Types for RADIUS Attributes (continued)

RADIUS Attribute	Associated RADIUS Packet Definition
vendor-specific.WISPr.Session-Terminate-End-Of-Day	RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Session-Terminate-End-Of-Day
vendor-specific.WISPr.Billing-Class-Of-Service	RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Billing-Class-Of-Service

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 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 *SRC-PE Services and Policies Guide, Chapter 1, Managing Services with the 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.

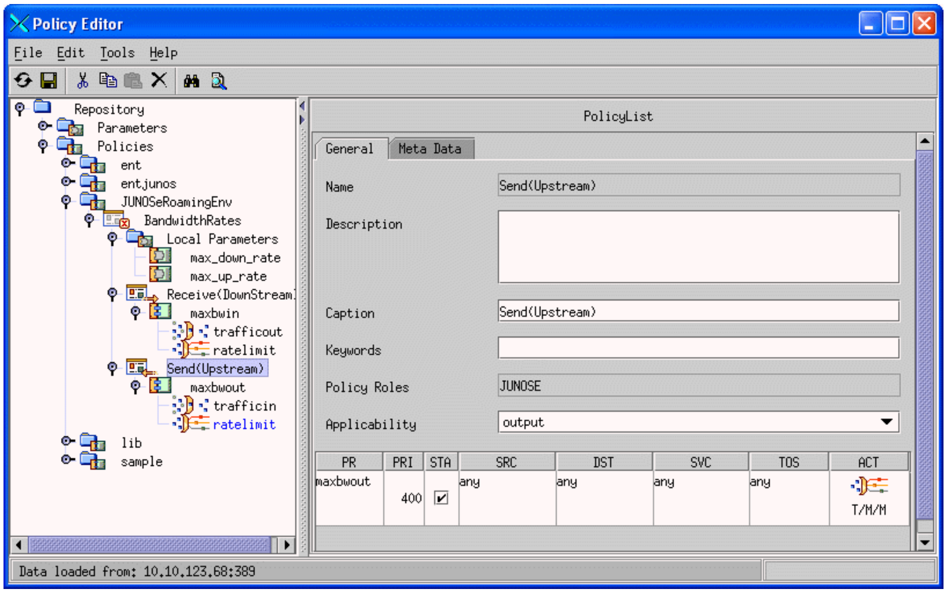
   To configure policies with Policy Editor, see *SRC-PE Services and Policies Guide, Chapter 11, Configuring and Managing Policies with Policy Editor* and *SRC-PE Services and Policies Guide, Chapter 14, Defining and Acquiring Values for Parameters*.

   To configure policies with the SRC CLI, see *SRC-PE Services and Policies Guide, Chapter 10, Configuring and Managing Policies with the SRC CLI* and *SRC-PE Services and Policies Guide, Chapter 9, Configuring Local and Global Parameters with the SRC CLI*.

The example in Figure 5 on page 27 shows 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

Figure 5: Sample Rate-Limiting Policies with Bandwidth Parameters



Name: Send(Upstream)

Description:

Caption: Send(Upstream)

Keywords:

Policy Roles: JUNOSE

Applicability: output

PR	PRI	STA	SRC	DST	SVC	TOS	ACT
maxbwout	400	☑	any	any	any	any	T/M/M

Data loaded from: 10.10.123.68:389

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

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 in the SRC software distribution in the folder *SDK/doc/idl* or on the Juniper Networks Web site at

http://www.juniper.net/techpubs/software/management/sdx/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 messaged 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:

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

Related Topics

- *JUNOS System Basics Configuration Guide*

  http://www.juniper.net/techpubs/software/junos/junos84/swconfig84-system-basics/swconfig84-system-basics.pdf

- *JUNOSe Broadband Access Configuration Guide*

  http://www.juniper.net/techpubs/software/erx/junose82/bookpdfs/swconfig-broadband.pdf