

Chapter 17

Services in 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. The chapter contains the following sections:

- Overview of a Wireless Roaming Environment on page 257
- Managing Subscribers for a Wireless Location on page 258

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-fi-ally.com/opensection/wispr.asp>

Subscriber Access in a Wireless Roaming Environment

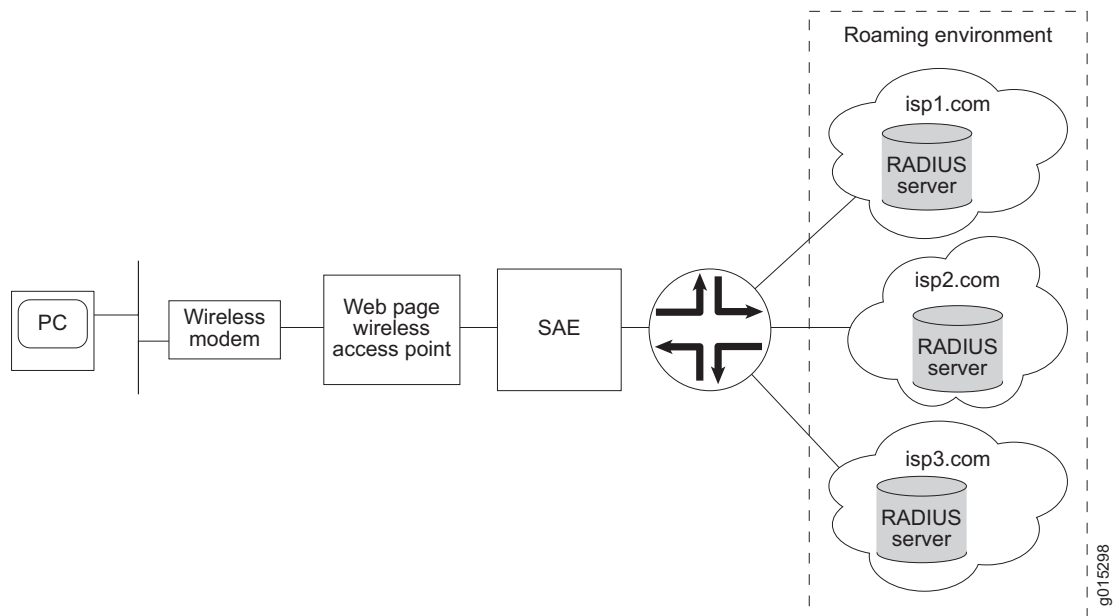
When subscribers log in to a wireless location that has a roaming agreement with other locations, the following sequence of events occurs:

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

Figure 51: Subscriber Access to a Wireless Roaming Group



Managing Subscribers for a Wireless Location

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

1. Configure RADIUS authentication for users who connect from a wireless location.
2. Create subscriber access to an ISP.
3. Create Web access.
4. Verify idle timeout properties for the SAE.

The following sections describe how to perform these tasks.

Configuring RADIUS Authentication

To 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 SDX 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 259.

For information about creating a custom plug-in, see *SAE CORBA Plug-In Service Provider Interface (SPI)* in the SDX 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-fi.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 *SDX Components Guide, Vol. 1, Chapter 5, Configuring Authorization and Accounting Plug-Ins*.

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 JUNOS 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 SDX 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 SDX 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 SDX 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 30 shows the packet types associated with each attribute.

Table 30: Packet Types for RADIUS Attributes

RADIUS Attribute	Associated RADIUS Packet Definition
<code>vendor-specific.WISPr.Location-ID</code>	<code>RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Location-ID</code>
<code>vendor-specific.WISPr.Redirection-URL</code>	<code>RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Redirection-URL</code>
<code>vendor-specific.WISPr.Logoff-URL</code>	<code>RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Logoff-URL</code>
<code>vendor-specific.WISPr.Bandwidth-Max-Up</code>	<code>RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Bandwidth-Max-Up</code>
<code>vendor-specific.WISPr.Maximum-Max-Down</code>	<code>RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Maximum-Max-Down</code>
<code>vendor-specific.WISPr.Location-Name</code>	<code>RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Location-Name</code>
<code>vendor-specific.WISPr.Session-Terminate-Time</code>	<code>RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Session-Terminate-Time</code>
<code>vendor-specific.WISPr.Session-Terminate-End-Of-Day</code>	<code>RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Session-Terminate-End-Of-Day</code>
<code>vendor-specific.WISPr.Billing-Class-Of-Service</code>	<code>RadiusPacket.stdAuth.auth.vendor-specific.WISPr.Billing-Class-Of-Service</code>

Creating Subscriber Access to an ISP

An access service lets subscribers connect to an ISP. The policies associated with the access service should specify a JUNOS policing or JUNOSe rate-limiting policy to set the maximum bandwidth at which a subscriber can send traffic, and the maximum bandwidth at which 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 an access service to the ISP:

1. In SDX Admin, create the access service.

See *SDX Objects Guide, Chapter 1, Managing Services*.

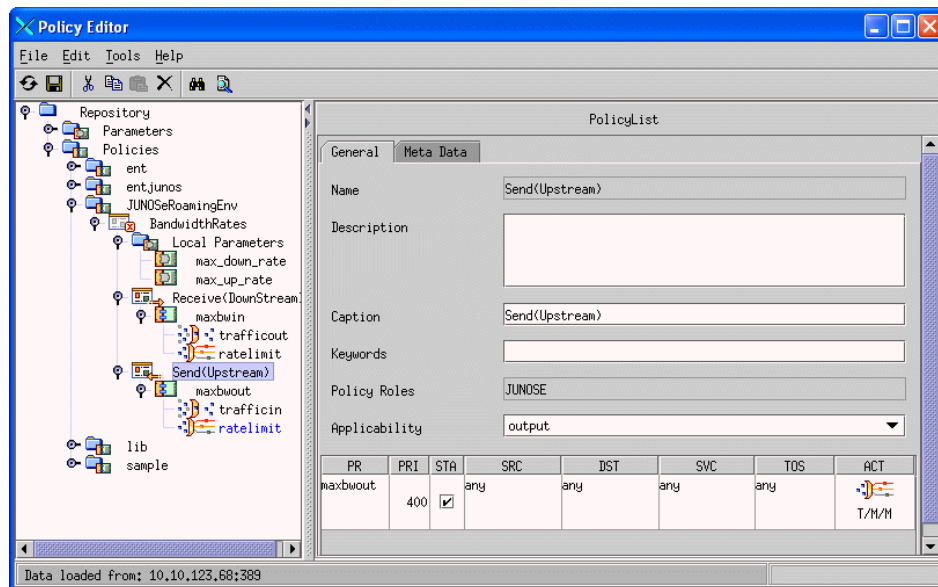
2. In Policy Editor, create a policy group that sets the maximum bandwidth at which a subscriber can send traffic, and the maximum bandwidth at which a subscriber can receive traffic. Use parameters to set these values.

See *SDX Objects Guide, Chapter 8, Configuring and Managing Policies* and *SDX Objects Guide, Chapter 10, Parameter Value Acquisition*.

The example in Figure 52 on page 263 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 52: Sample Rate-Limiting Policies with Bandwidth Parameters



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 residential service selection portal. A captive portal page receives and manages redirected Web requests. For information about residential portals and captive portal pages, see *SDX Components Guide, Vol. 2, Chapter 1, Overview of the Residential 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 SDX 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>

Verifying Idle Timeout Properties for the SAE

Review the following configuration properties to ensure that the settings are consistent with the requirements for your environment:

- Idle Timeout
- Adjust Session Time

To review idle timeout settings from SDX Configuration Editor:

1. In the navigation pane, expand SAE, and click a configuration object.
2. In the content pane, click the Miscellaneous tab.
3. Verify the setting for Idle Timeout(s).

This value may be set in the service definition for the access service, or by the ISP in a RADIUS authorization response.

An interval up to 5 minutes is typically recommended for the idle timeout. For the SDX software, the recommended minimum is 15 minutes.

4. In the Miscellaneous pane, expand Idle Timeout, and review the setting for Adjust Session Time. See the field description below.

Adjust Session Time

- Whether or not, when an idle timeout terminates a session, the session time reported in the accounting message is reduced by the idle time. This way the session time is accurately reported to avoid overcharges for the session.
- Value
 - True—Reduces the session time by the amount of time specified by Idle Timeout
 - False—Does not reduce the session time by the amount of time specified by Idle Timeout
- Default—True
- Property name—`AccountingMgr.adjustSessionTime`