Chapter 3

Subscriber Logins and Service Activation

This chapter gives an overview of how different types of subscribers log in to the network and how services and subscribers are activated. Topics include:

Overview of Login Events and Processes

Because of the different ways that residential and enterprise subscribers connect, the login interactions between the components differ according to the type of subscriber. Because residential customers can connect by PPP, DHCP, or static IP addresses, the interactions between the SRC components differ according to the method of connection that a residential subscriber uses. However, there is only one type of login interaction—the subscriber interface login interaction—for enterprise subscribers.

Logins to plug-ins can occur during the login to the SAE or during the activation of subscriptions. For these processes, many of the interactions between the SRC components are the same regardless of the type of subscriber and the type of connection.

Login Events

Each login process begins with a login event, as described in Table 9.

Table 9: Login Events

Login Event	Event Is Triggered When	SAE Response
AUTHINTF	An interface responds to authentication, such as authentication for a PPP session. (Supported on JUNOSe routers.)	Invokes subscriber classification script, creates subscriber session.
INTF	An interface comes up and the interface classifier script determines that the SAE should manage the interface, unless the interface comes up as a result of an authenticated PPP session. (Supported on JUNOS routing platform and JUNOSe routers.)	Invokes subscriber classification script, creates subscriber session.
ADDR	A subscriber obtains an unauthenticated IP address from the router through DHCP. (Supported on JUNOSe routers.)	Invokes subscriber classification script, creates subscriber session.
AUTHADDR	A subscriber obtains an authenticated IP address from the router through DHCP. (Supported on JUNOSe routers.)	Invokes subscriber classification script, creates subscriber session.
PORTAL	The portal API is invoked by a JSP Web page to log in a subscriber. (Supported on JUNOS routing platform and JUNOSe routers.)	Authenticate subscriber, invokes subscriber classification script, creates subscriber session.
ASSIGNEDIP	An application accesses a subscriber object for an assigned IP subscriber that is not currently loaded into memory.	Invoke subscriber classification script, creates subscriber session.

Summary of the Login Process

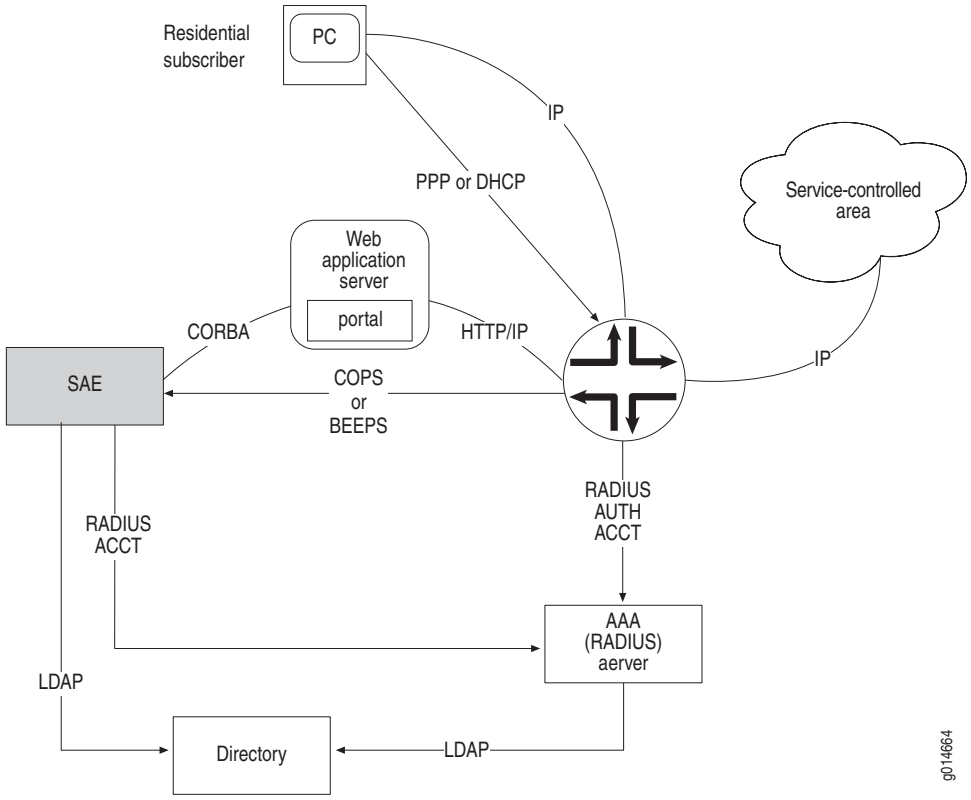
The SAE login process is summarized in the steps below. If any of the steps fail, the login process stops, and no subscriber session is created.

1. A login event occurs (see Table 9) and triggers the login process.
2. In case of a portal login, the SAE invokes the authentication plug-ins to authenticate the request.
3. The SAE invokes the subscriber classification script and provides to the script details about the login event (for example, interface name, subscriber IP address if available, login name if available, and login event type).
4. The script sends an LDAP query that uniquely identifies a subscriber entry in the directory to the SAE.
5. The SAE loads the subscriber entry from the directory and uses the entry to create a subscriber session in memory.
6. The SAE queries all configured authorization plug-ins about whether it should allow the login.
7. The SAE completes the login process by activating the subscriber's activate-on-login subscriptions.

Residential Subscriber Login and Processes

This section focuses on residential subscriber configurations involving authenticated PPP, DHCP, and static IP. The PPP, DHCP, and static IP cases are distinguished by the type and configuration of the networking software on the network device used to access the router. Figure 4 shows how residential subscribers connect to SRC components.

Figure 4: Components Involved in Subscription Activation



The residential subscriber's network device (such as a computer, cellular telephone, or set-top box) connects through a layer 2 connection to the router. The network device is configured for network access with PPP or DHCP.

The router and the SAE use a RADIUS server for authentication, accounting, and optionally IP address allocation. The router can also locally manage the allocation of IP addresses to residential subscribers' PCs. A directory supporting LDAP holds the database of subscriber, service, and subscription information. Both the SAE and the RADIUS server use the directory.

Once connected to the network, the subscriber's network device exchanges IP data packets with resources in a service-controlled area. From the service provider's perspective, the resource to which access is controlled may be the network itself or content servers in the network.

The SAE manages the subscriber's IP interface on the router to control the level of access that the subscriber gets to the service-controlled area. The level of access can be anything from viewing a portal page that allows the subscriber to select a service to varying the network access speed. The subscriber can actively and instantly request access to the service-controlled area by selecting items on Web pages generated by the SAE. Selecting these items triggers the SAE to instantly reconfigure the subscriber's IP interface on the router.

The SAE communicates with JUNOSe routers through COPS messages.

The SAE communicates with JUNOS routing platforms through BEEP messages.

PPP Subscriber Login and Service Activation

PPP subscribers access the network by using either special PPP or PPP over Ethernet software on their network access device. PPP access provides a means to configure the subscriber's network access device with several network parameters, including an IP address and a channel for transporting IP packets between the subscriber's network device and the router.

For subscribers with PPP access, logging in to the network consists of starting the PPP client, and logging out consists of stopping it. On PPP login, the router authenticates the subscriber as normal with a message to a RADIUS server. The router then notifies the SAE that there is a new IP interface on the router. The message to the SAE includes information such as the subscriber's IP address (if assigned by the router or RADIUS server), PPP login ID, and router interface ID. Using this information, the SAE retrieves the information to construct the default policies. The SAE then activates subscription policies, which are downloaded to the router and applied to the subscriber's network interface.

Subscribers can log in to the system with different accounts to different retail Internet service providers (ISPs). Subscribers use a different login ID for each account.

PPP requires special software on a network access device. The PPP software must be installed and maintained by the subscriber. The software can interfere with other applications.

Web Login for PPP Subscribers

In a PPP session, an IP address and a subscriber profile are authenticated at the same time. However, for some applications a split of subscriber profile and PPP session is useful; for example:

- Generic PPP account—An ISP could offer generic PPP login names and passwords for everybody and use Web-based login to identify subscribers.
- Device-based PPP—A PPP login may be used between a digital subscriber line (DSL) access device and a router. In this case a PPP login does not correspond to a subscriber session.
- Subaccounts with different services.

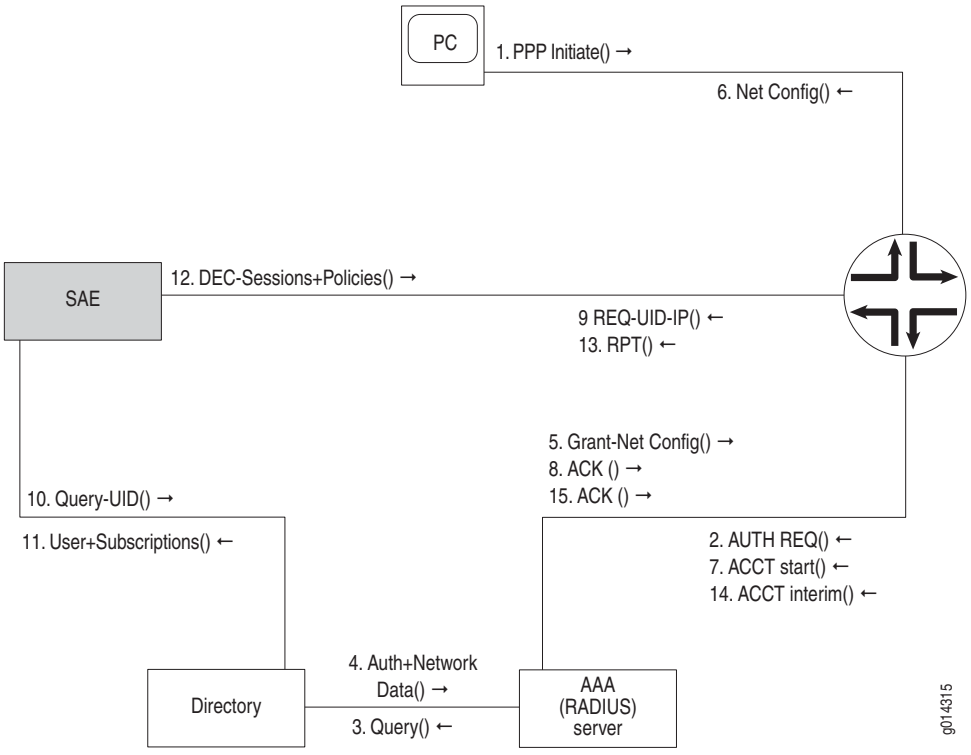
As a consequence, the Service Selection Portal (SSP) API allows creation of a Web application that:

- Allows PPP subscribers to log out—When the PPP subscriber logs out, the current subscriber session is closed, all active services are deactivated, and accounting records are generated. The unauthenticated subscriber entry is then associated with the IP address of the subscriber. This process is similar to a DHCP logout.
- Forces an unauthenticated PPP subscriber (that is, a PPP subscriber account that is bound to the unauthenticated subscriber entry or to an anonymous subscriber entry) to log in—The subscriber provides a username, realm (domain), and password. Authentication is processed in the same way as a DHCP login.

PPP Login Interactions

Figure 5 shows the interactions that take place during a PPP login.

Figure 5: PPP Login Interactions



The login sequence is as follows:

1. The subscriber initiates a PPP login by starting a PPP client on his or her network device.
2. The router sends an authentication request to the RADIUS server.
3. The RADIUS server sends a user ID query to the directory.

4. The directory responds with the data (IP address for the subscriber's network device) needed to authenticate the login, and then completes the configurations of the interface on the router and on the subscriber's network device.

5. If the authentication succeeds, the RADIUS server responds to the router with a grant message, including the network configuration parameters.

6. The configurations of the PPP and IP interfaces on the router and subscriber's network device are completed.

7. The router sends an accounting start message to the RADIUS server, indicating that a subscriber session has started.

8. The RADIUS server acknowledges the accounting start message.

9. The router sends a COPS or BEEP request message to the SAE. The message includes the user ID and the IP address assigned to the IP interface on the subscriber's network device. The SAE associates the subscriber's IP address with the subscriber session so that it can associate later requests from the subscriber with this session by looking at the source IP address of the request.

10. The SAE uses the subscriber ID to look up the subscriber's data in the directory.

11. The directory responds with data about the subscriber and the associated subscriptions. This data specifies which subscriptions should be automatically activated.

12. The SAE sends a series of decision (DEC) messages to the router. These messages tell the router to attach default policies and policies for automatically activated subscriptions to the subscriber's interface. They also tell the router to store subscriber and service sessions so that if the SAE fails, the subscriber can continue using his or her active subscriptions. If the SAE fails, the router connects to a backup SAE that synchronizes all session information and then takes over management of active subscribers on the router. During the synchronization process, active sessions are not affected.

13. The router acknowledges the decision messages with a report (RPT) message.

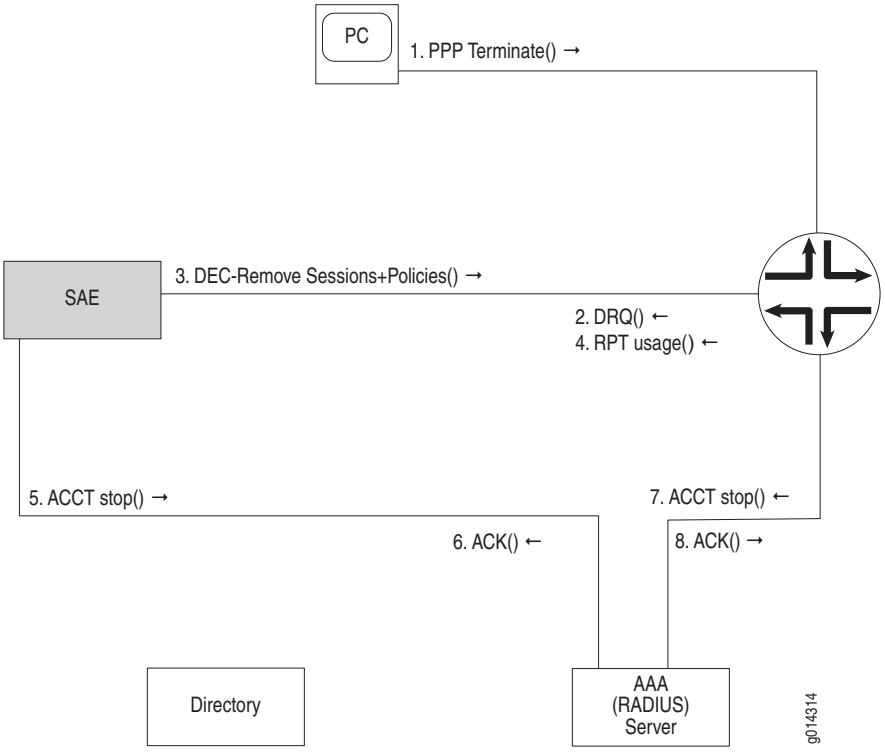
14. If interim accounting is enabled, the router periodically sends an accounting request to the RADIUS server to store an interim accounting record.

15. The RADIUS server sends an acknowledge message to the router, acknowledging the receipt of the interim accounting record.

PPP Logout Interactions

Figure 6 shows the interactions that take place when a subscriber logs out of a PPP session.

Figure 6: PPP Logout



The logout sequence is as follows:

1. The subscriber triggers his or her PPP software to close the PPP session with the router.

2. The router sends a COPS or BEEP delete request (DRQ) message, informing the SAE that the subscriber's IP interface is being shut down.

3. The SAE responds with decision (DEC) messages, requesting the router to remove the default and active subscription policies and sessions for the subscriber.

4. The router responds with a report (RPT) message that includes the usage data for the subscriptions that were just deactivated.

5. The SAE sends an accounting stop message to the RADIUS server, indicating that a service session has stopped. The stop message includes the usage data. (For information about service sessions, see *Subscriptions and Activations* on page 33.)

6. The RADIUS server acknowledges the accounting stop request.

7. The router sends an accounting stop message to the RADIUS server, indicating that a subscriber session has stopped.

8. The RADIUS server acknowledges the accounting stop request.

DHCP Subscriber Login and Service Activation

The DHCP system uses Ethernet to send data between a network device and the router. The DHCP client is built into the operating system. DHCP subscribers log in to the SAE to identify themselves, get personalized services, and select the retail ISP they want to use. Anonymous subscribers can log in to the SAE to view their account and subscription information.

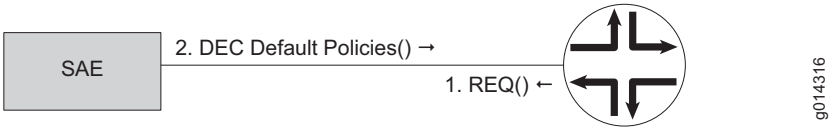
Like a subscriber with PPP access, a subscriber with DHCP access can have several accounts. The subscriber logs in to the different accounts at different times. This setup allows subscribers access to different sets of subscriptions. It supports a household in which different members share the same computer but subscribe to different services. Members of the household can get different bills for the services they use.

Subscribers can create a persistent login. In this case, the SAE stores the MAC address of the network device, along with the subscriber ID and password. This way, the network device is logged in to the subscriber account every time the device is started. Using the SAE core API, one can provide a check box on the portal page that allows the subscriber to create a persistent login. See *Persistent DHCP Subscriber Login Interactions* on page 26.

Interface Startup

An IP interface for DHCP subscribers can come up on the router without subscribers explicitly triggering its creation by logging in. When an interface comes up, the SAE runs an interface classifier script to determine whether it should manage the interface and, if so, which default policies to apply to the interface. Thus, for DHCP subscribers, default policies are applied as soon as the IP interface on the router comes up independently of any subscriber login. Figure 7 shows this interaction.

Figure 7: DHCP Interface Startup



The startup sequence is as follows:

1. When the IP interface on the router comes up, the router sends a COPS request (REQ) to the SAE to let it know that the new interface exists.

2. The SAE runs an interface classification script to determine whether it should manage the new interface. If the SAE manages the interface, then the SAE downloads the default policies for the interface on the router.

Initial Login

When a DHCP subscriber starts a network device for the first time, the SAE has no information about who the subscriber is and what subscriptions the subscriber has. The SAE assigns default policies and an unauthenticated subscriber profile to the subscriber. The unauthenticated subscriber profile gives the subscriber access to services that are available without authentication.

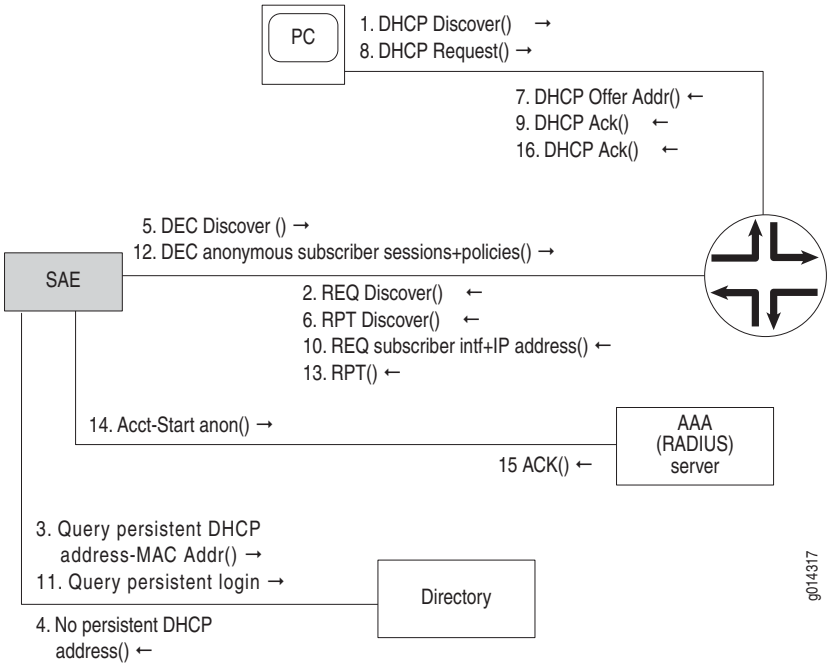
The first time a subscriber's network device starts, the router assigns an IP address to it. This address allows the subscriber access only to the SAE. The router provides this IP address for a short period of time called the lease time. After the lease time is over, the router provides a permanent IP address.

The system builds SAE applications to allow subscribers to register with the network if they are first-time subscribers of the network.

Initial DHCP Login Interactions

Figure 8 shows the interactions that take place when a DHCP subscriber starts a network device.

Figure 8: DHCP Subscriber Initial Login



For this example, we assume that the directory responses show that there are no persistent subscriber logins. The startup sequence is as follows:

1. The DHCP client in the subscriber's network device broadcasts a discover message to the router.

2. The router acts on the discover message by sending a COPS request (REQ) message to the SAE, indicating that an IP address is about to be assigned by the local DHCP server on the local router. This request includes the MAC address of the subscriber's network device and the DHCP options sent by the client.

3. The SAE queries the directory to detect any persistent DHCP address assignments associated with the subscriber's network device. Persistent DHCP address assignments are indexed by the MAC address of the device from which they originate.

4. The directory responds with an indication that there are no persistent DHCP address assignments associated with the subscriber's network device.

5. The SAE responds to the router with a COPS decision (DEC) message, requesting the router to assign an unauthenticated address to the subscriber device.

6. The router acknowledges the address assignment decision message with a COPS report (RPT) message.

7. The router allocates and offers an IP address to the subscriber's network device.

8. The network device sends a request for the address that the router offered.

9. The router acknowledges the address request.

10. The router sends a COPS request message that includes the subscriber's interface and the assigned IP address.

11. The SAE looks up persistent logins or runs the subscriber classification script and creates a subscriber session based on the loaded subscriber profile.

12. The SAE downloads sessions for the newly logged in unauthenticated subscriber and the policies for the subscriptions that this subscriber account has configured for automatic activation. (Identification of which unauthenticated subscriber account to use is configurable in the SAE and is a function of attributes found in the original COPS request message of Step 2.)

13. The router stores the sessions, applies the policies to the subscriber's IP interface, and then acknowledges the decision with a COPS report.

14. If accounting is configured for the subscriptions, the SAE sends an accounting start message to the RADIUS server.

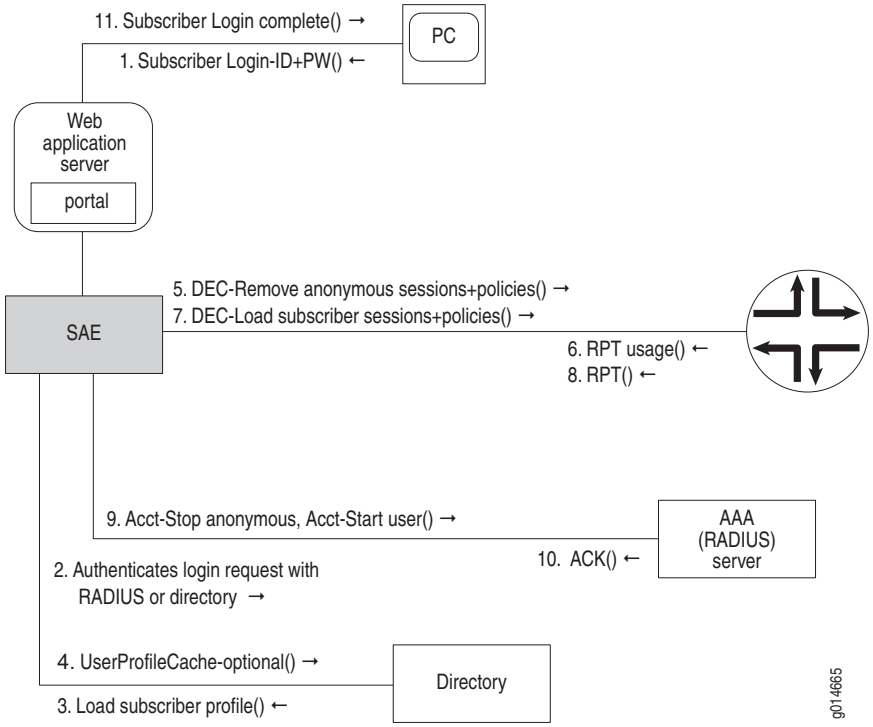
15. The RADIUS server acknowledges the accounting message.

16. The DHCP server on the router acknowledges the DHCP renew request.

DHCP Login to Subscriber Account Interactions

Figure 9 shows the interactions that take place when a DHCP subscriber logs in to a subscriber account. The account changes from an anonymous subscriber to an authenticated subscriber with personalized subscriptions.

Figure 9: DHCP Subscriber Login



The sequence is as follows:

1. The subscriber's network device sends a request to the SAE to log in to the subscriber account with the subscriber ID and password (PW).

2. The SAE authenticates the request using the configured authentication plug-in.

3. If authentication is successful, SAE loads a subscriber profile from the directory.

4. If this is a persistent login, the SAE creates an entry in the directory in the userProfileCache object. The entry is keyed to the network device's MAC address and associates the MAC address with the subscriber ID and password. The next time the subscriber starts the device, the system automatically logs in the subscriber's account.

5. The SAE sends a COPS decision (DEC) message, instructing the router to deactivate the policies and sessions associated with the active subscriptions.

6. The router acknowledges the COPS decision message with a COPS report (RPT) message that includes usage information for the active subscriptions.

7. The SAE sends a COPS decision message to load sessions and policies for the automatically activated subscriptions for the new subscriber account.

8. The router acknowledges these decisions with COPS report messages.

9. The SAE sends the RADIUS server accounting stop messages for the subscriptions that were deactivated, and accounting start messages for the subscriptions that were activated.

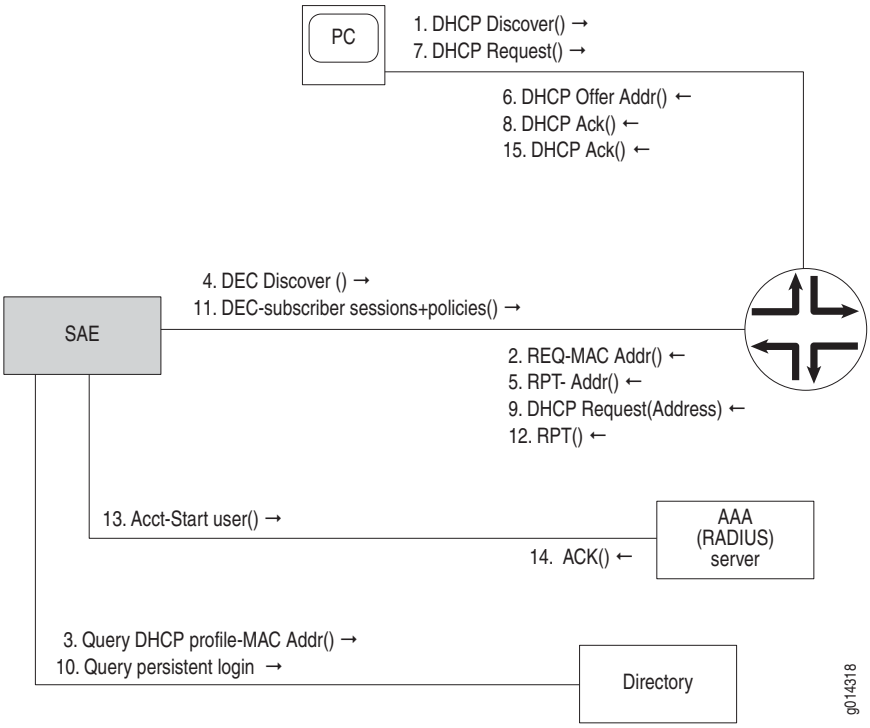
10. The RADIUS server acknowledges the accounting messages.

11. The SAE responds to the subscriber's original request with a login successful message. A typical application would return a Web page that gives the subscriber the ability to activate and deactivate subscriptions.

Persistent DHCP Subscriber Login Interactions

Figure 10 shows the interactions that take place when a DHCP subscriber starts a device on the network after having previously been logged in as a persistent subscriber.

Figure 10: Persistent DHCP Subscriber Login



The login sequence is as follows:

1. The DHCP client in the subscriber's network device sends a discover message to the router.

2. The router sends a COPS request (REQ) message to the SAE, informing the SAE that the router has received a DHCP discover request. The message includes the MAC address of the subscriber's network device and the DHCP options sent with the discover request.

3. The SAE queries the directory for a DHCP profile associated with the MAC address of the subscriber's network device.

4. The SAE sends the router a COPS decision (DEC) message, instructing the router to assign an IP address to the subscriber's network access device based on the information stored in the DHCP profile.

5. The router acknowledges the address assignment decision message with a COPS report (RPT) message.

6. The router allocates and offers an IP address to the subscriber's network access device.

7. The subscriber's network access device sends a request message to the router, requesting the address that was offered.

8. The router acknowledges the address request.

9. The router sends a COPS request message to the SAE that includes the subscriber's interface and the assigned IP address.

10. The SAE queries the directory for persistent logins, and the directory responds with the subscriber account information for the persistent login, including the subscriptions that are to be automatically activated.

11. The SAE starts the subscriber session and downloads session data for the subscriber account and the policies for the subscriptions that this subscriber account has configured for automatic activation.

12. The router stores the session data and applies the policies to the subscriber's IP interface. The router then acknowledges the decision message with a COPS report message.

13. If accounting is configured for the automatically activated subscriptions, then the SAE sends an accounting start message to the RADIUS server.

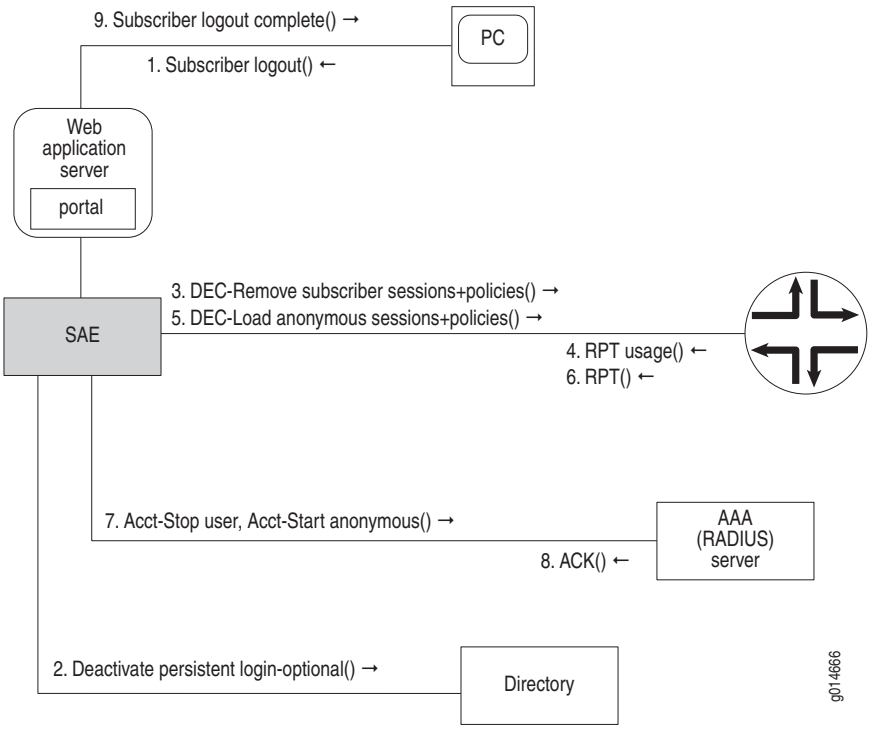
14. The RADIUS server acknowledges the accounting start message.

15. The router acknowledges the DHCP request messages with a DHCP acknowledge message.

DHCP Subscriber Logout Interactions

Figure 11 shows the interactions that take place when a DHCP subscriber logs out of a subscriber account. The account changes from an authenticated subscriber to an anonymous subscriber with generic subscriptions and limited access.

Figure 11: DHCP Subscriber Logout



The logout sequence is as follows:

1. The subscriber's network device sends a request to the SAE to log out of its current subscriber session.

2. The subscriber may request to deactivate persistent login. If the subscriber deactivates persistent login, the SAE deletes the entry in the directory. If the subscriber does not deactivate the persistent login, then the account is automatically logged in the next time the same network device is started.

3. The SAE sends a COPS decision (DEC) message to the router, instructing the router to remove the sessions and policies associated with the active subscriptions.

4. The router responds with a COPS report (RPT) message that includes the usage information for the deactivated subscriptions.

5. The SAE sends a COPS decision message to add sessions and policies for the automatically activated subscriptions for the anonymous account to which the subscriber has switched.

6. The router acknowledges the COPS decision message by sending a COPS report message to the SAE.

7. The SAE sends the RADIUS server accounting stop messages for the subscriptions that were deactivated, and accounting start messages for the subscriptions that were activated.

8. The RADIUS server acknowledges these accounting messages.

9. The SAE responds to the subscriber's logout request, showing that the logout is complete.

Static IP Subscribers

The SAE supports residential subscribers who use statically assigned IP addresses. Statically assigned means that the network does not create events that contain information about the IP address of the subscriber. The SAE can handle the case in which a router interface is dedicated to one subscriber. This subscriber can be a single PC or multiple PCs that are managed by the same household.

Single PC, IP Address Known

See Figure 12.

1. When the interface dedicated to the subscriber comes up, the router sends a COPS or BEEP request (REQ) message to the SAE. The SAE calls the interface classification script to determine whether the interface is being managed and which default policies are applied.

2. The SAE sends a decision (DEC) message to the router, requesting that the router attach the selected default policies.

3. The router acknowledges the decision message with a report message.

4. The SAE calls the subscriber classification script to determine whether a subscriber session needs to be started. The subscriber classification script responds with an LDAP query.

5. The SAE uses the LDAP query to look up a subscriber entry in the directory.

6. The directory responds with data about the subscriber and the associated subscriptions. The IP address assigned to the subscriber can be part of the data returned from the directory. If the IP address cannot be stored in the directory, it is also possible to integrate the SAE with an external data source (for example, a database maintained by an existing provisioning system), to look up the IP address of the subscriber.

   As in the PPP case, the SAE associates the subscriber session with the IP address so it can handle later requests by looking up the source IP address of the HTTP request.

7. The SAE sends decision messages that install policies for automatically activated subscriptions.

Figure 12: Static IP Subscriber Login

Subscriber IP Address Not Known

See Figure 13.

1. When the interface dedicated to the subscriber comes up, the router sends a BEEP or COPS request (REQ) message to the SAE. The SAE calls the interface classification script to determine whether the interface is being managed and which default policies are applied.

2. The SAE sends a decision (DEC) message to the router, requesting that the router attach the selected default policies.

3. The router acknowledges the decision message with a report (RPT) message.

4. The SAE invokes the subscriber classification script to determine whether a subscriber session needs to be started. The subscriber classification script responds with an LDAP query.

5. The SAE uses the LDAP query to look up a subscriber entry in the directory.

6. The directory responds with data about the subscriber and the associated subscriptions.

   The SAE associates the subscriber session with the DN of the subscriber entry so that later requests can be handled. One consequence of associating the subscriber entry with the DN is that it is not possible to have more than one subscriber session for a single DN active at the same time.

7. The SAE sends decision messages that install policies for automatically activated subscriptions.

8. The subscriber connects to the portal. Because the IP address of the subscriber is not associated with a subscriber session, a login page is displayed instead.

9. The subscriber provides a username and password.

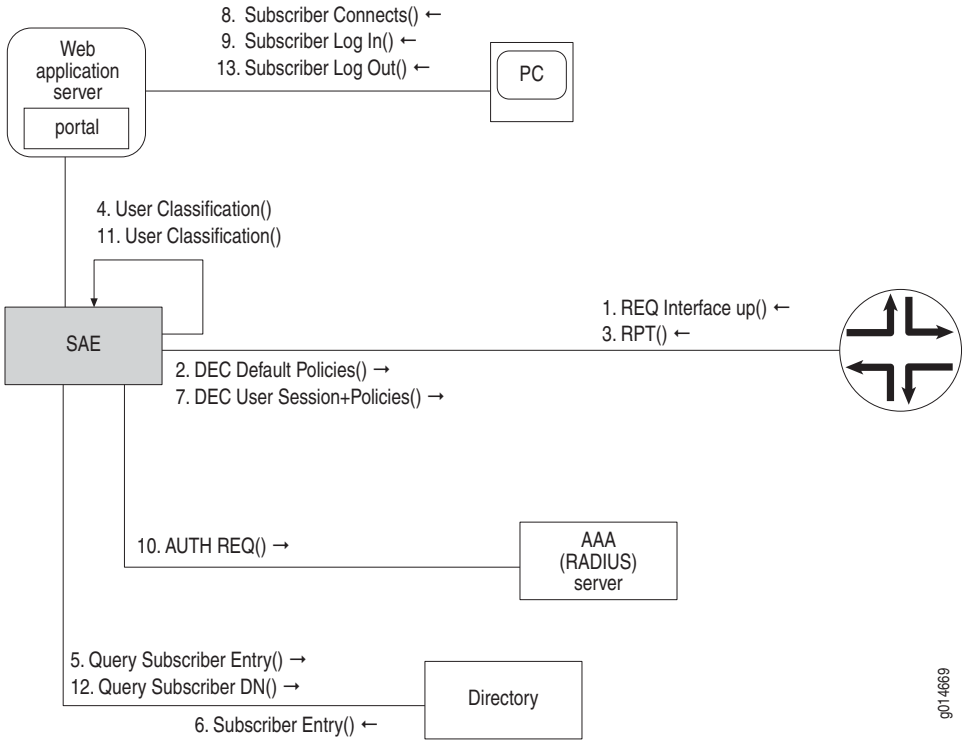
10. The SAE authenticates the request (for example, by using the RADIUS authentication plug-in) and calls the subscriber classification script.

11. The subscriber classification script returns an LDAP query. The SAE uses the query to look up the DN of the subscriber entry in the directory.

12. The SAE uses the DN returned from the directory to find a subscriber session and associates it with the IP address of the HTTP request. The SAE handles subsequent accesses to the portal by looking up the IP address of the HTTP request.

13. The subscriber logs out from the SAE. The SAE does not change the subscriber session associated with the DN of the subscriber, but removes the association of the subscriber IP address with the subscriber session.

Figure 13: Subscriber IP Address Not Known



Enterprise Subscriber Login Process

Enterprise subscribers may connect through any access method. Any of the events described in Table 9 on page 16 can initiate an enterprise login.

Interface Startup

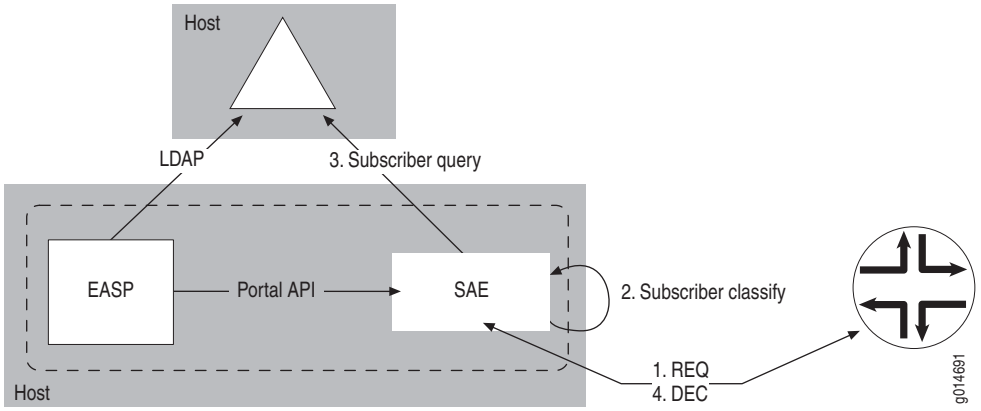
When a router interface comes up, the router sends a message to the SAE with information about that interface.

The SAE classifies the subscriber to determine the default interface policies. An SAE subscriber classification rule matches the attributes of the interface and describes how to formulate an LDAP query that retrieves the access entry in the directory that corresponds to the router interface.

Based on the response from the directory, the SAE creates a subscriber session and associates it with the DN of the access entry in the directory. The SAE then sends the router a message to install all the policies for subscriptions for the access line that are set to administratively active.

Figure 14 shows the stages involved in activating an enterprise subscriber session.

Figure 14: Enterprise Subscriber Session Activation



Subscriptions and Activations

Each subscriber purchases a set of services; this purchase is known as a subscription. Information about the subscriptions is stored in the directory and is used by a residential service selection portal application to generate controls that enable the subscriber to:

- Activate and deactivate subscriptions.
- Subscribe to services.
- Configure subscriptions to be automatically activated.

The service selection application can be either a Web application or an API. When the service selection application is a Web application, the controls are Web pages with buttons and links to click on (see Figure 15 and Figure 16). However, the service selection application provides an open API that makes it possible to build applications that are controlled by mechanisms other than Web pages. For instance, customers can build service selection applications that are controlled by applications running in the system tray area of the Windows task bar. This deployment consolidates the control of subscribers' active network services and the speed of their Internet connection, along with their control of other aspects of their PC, such as the clock settings and audio volumes.

Figure 15: Service Activation Page

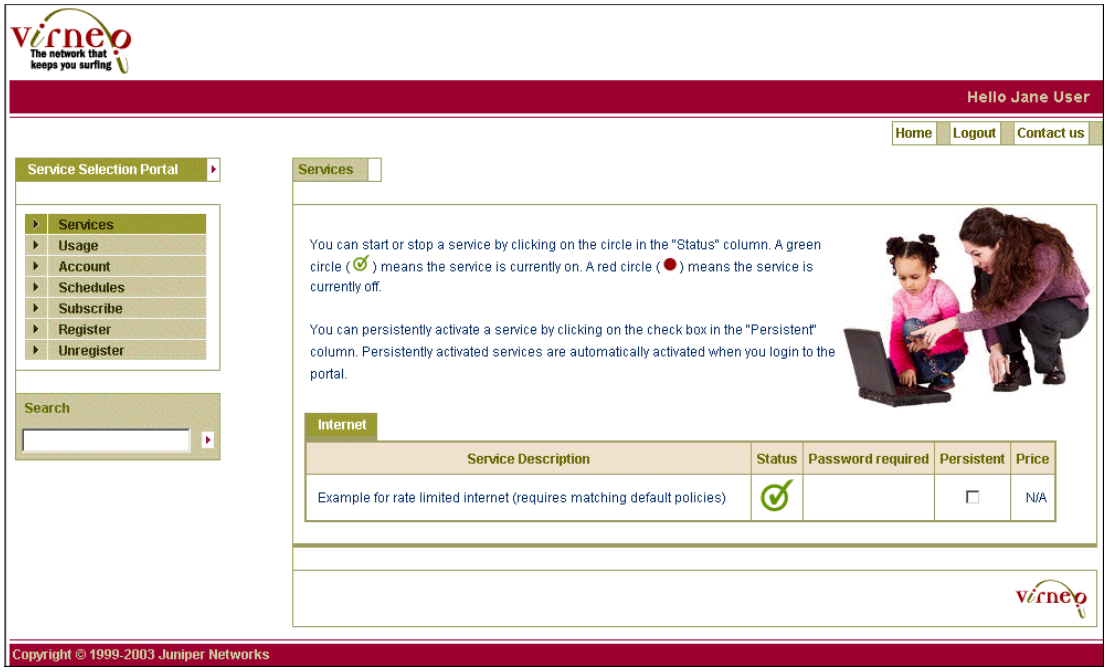
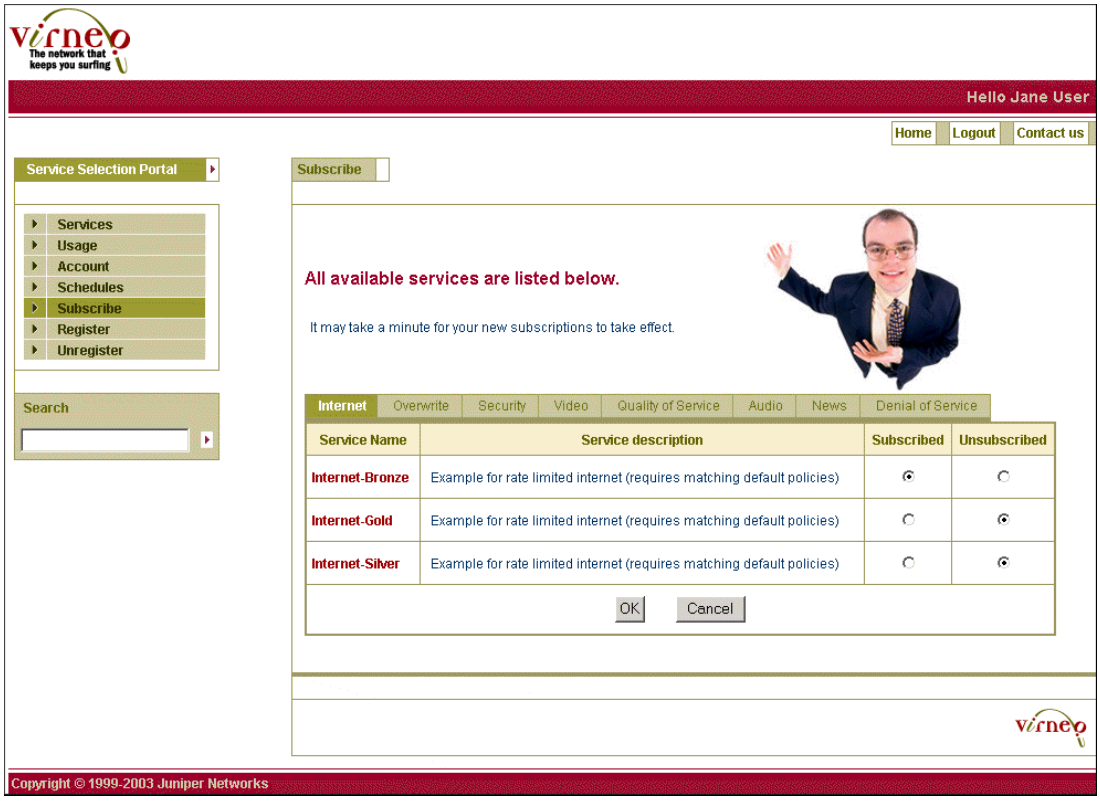


Figure 16: Subscription Activation Page

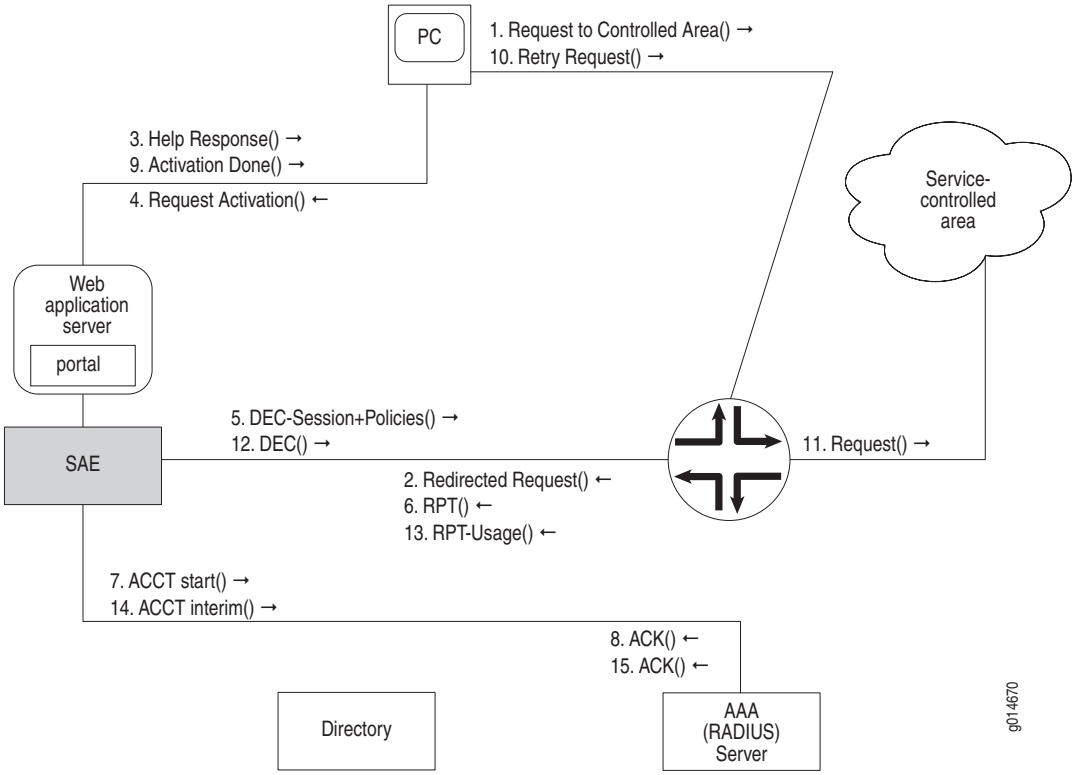


Many of the activation and deactivation interactions work in the same way, whether the subscriber is a residential subscriber or an enterprise subscriber. However, some interactions apply only to enterprise subscribers (see *Enterprise-Specific Remote Session Activation* on page 38).

Subscription Activation Interactions

Clicking a button on the Web page to activate a service session causes the SAE to download the policies associated with the service to the subscriber's IP interface on the router. Figure 17 shows the interactions among the components shown in Figure 4 on page 17 during the activation process. This scenario assumes that the subscriber has already logged in.

Figure 17: Subscription Activation



The activation sequence is as follows:

1. Before the subscription is activated, the subscriber makes a request to the corresponding subscription resource in the service-controlled area.

2. A default policy that matches the request on the router causes the router to redirect the request to the SAE.

3. The SAE responds to the request with a help desk Web page, requesting that the subscriber activate the subscription before trying to access the resource.

4. The subscriber clicks a button on the service selection portal Web page, requesting the activation of the subscription.

5. The SAE sends a COPS or BEEP decision (DEC) message to the router, requesting the installation of policies for the subscription on the subscriber's IP interface on the router, as well as service session information.

   At start time, the SAE loads all services and policy templates from the directory. At activation time, the policy templates for the service are instantiated with values that are determined at activation, such as the subscriber's IP address. The router stores session information so that if the SAE fails, the subscriber can continue using his or her active subscriptions. If the SAE fails, the router connects to a backup SAE. The backup SAE synchronizes all session information and then takes over management of all active subscribers on the router.

6. The router responds with a report (RPT) message acknowledging the decision message.

7. The SAE sends an accounting start message to the RADIUS server.

8. The RADIUS server acknowledges the accounting start message.

9. The SAE responds to the subscriber's activation request, indicating that the subscription is active.

10. The subscriber may now retry the request for access to the controlled resource.

11. This time, the request to the controlled resource matches the policy from the newly activated subscription, so the router allows the request to be routed normally. Depending on the policy, the router may also apply QoS processing.

12. If interim accounting is enabled, the SAE periodically sends a decision message requesting usage data.

13. The router responds with a report message that contains usage data for the subscription. The usage data consists of the number of bytes and packets that the policies processed for the subscription.

14. The SAE stores the usage data in interim accounting records in the RADIUS server.

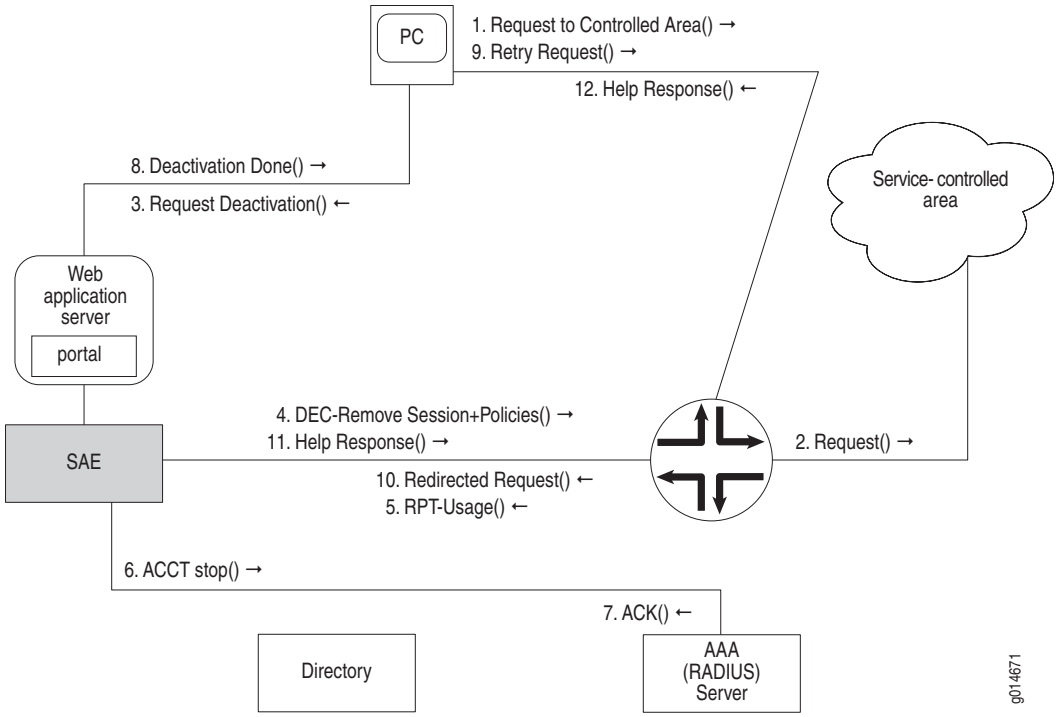
15. The RADIUS server acknowledges the interim accounting record.

Subscription Deactivation Interactions

Clicking a button on the Web page to deactivate a service causes the SAE to request that the router remove the policies for the service from the subscriber's IP interface on the router.

Figure 18 shows the interactions among the components shown in Figure 4 on page 17 during the subscription deactivation process. This scenario assumes that the subscriber has already logged in.

Figure 18: Subscription Deactivation



The deactivation sequence is as follows:

1. The subscriber sends a request to deactivate a subscription to a resource in the service-controlled area.

2. The request matches a policy that allows the request to be forwarded to the resource in the service-controlled area.

3. The subscriber clicks on a field on a Web page to request that the SAE deactivate the subscription.

4. As a result, the SAE sends a COPS or BEEP decision (DEC) message to the router to remove policies for the subscription from the subscriber interface and the service session from memory.

5. The router acknowledges the decision message with a report (RPT) message that contains service usage. The usage is the number of bytes and packets that the policies processed for the subscription.

6. An accounting stop record that includes the subscription usage information is written in the RADIUS server.

7. The RADIUS server acknowledges the accounting message.

8. The SAE sends a message to the subscriber, informing the subscriber that the subscription has been deactivated.

9. Because the policy for the subscription was removed from the subscriber interface on the router, any request for access is directed to the SAE.

10. The subscriber may now retry to request access to the controlled resource.

11. As was the case before the subscription was activated, the SAE generates a help desk Web page response that is relayed to the subscriber.

Automatic Activation at Login

An activate-on-login subscription is a subscription that is configured to start every time the subscriber logs in.

A manual subscription is a subscription that is configured to start only by an action from the subscriber.

For example, residential subscriber Elizabeth has designated her high-speed subscription to automatically activate every time she logs in. On the other hand, her video subscription is not activated unless she activates it by clicking a button on a portal page. It is possible to integrate the SAE with a video-on-demand server so that the video service is automatically activated when Elizabeth logs in. This type of configuration ensures access to the server and to QoS for the video stream. When the video stream is finished, the video-on-demand server triggers the SAE to stop the video service.

Residential subscriber Robert is interested in streaming audio. He sets his subscriptions so that regular-speed service, along with his subscription to an audio service, is automatically activated every time he logs in.

Enterprise-Specific Remote Session Activation

When a subscription is set for automatic activation through the Web interface, a service session request message is sent from the manager's PC to the Enterprise Manager Portal. The Enterprise Manager Portal writes this request to the directory, and the directory eventing system (DES) notifies the SAE affected by this request of the directory event. The SAE then sends a COPS or BEEP decision message to the router to download the policies for the activated subscription.

The enterprise manager must explicitly request feedback to see whether the session succeeded and what the operational values for the service parameters actually are. To do this, the enterprise manager sends a feedback request to the Enterprise Manager Portal. To process this request, the Enterprise Manager Portal sends a feedback request to the remote SAE managing the access through CORBA and returns the response to the enterprise manager's browser.

Figure 19 shows the sequence of messaging events that occur between the manager PC, the Enterprise Manager Portal, the master and shadow directories, the remote SAE, and the router.

Figure 19: Remote Session Activation Sequence