

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.

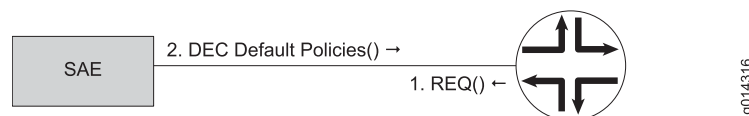
Like a subscriber with PPP access, a subscriber with DHCP access can have several accounts. The subscriber logs in to the different accounts at different times. This setup allows subscribers access to different sets of subscriptions. It supports a household in which different members share the same computer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

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 1 on page 1 shows this interaction.

Figure 1: 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.

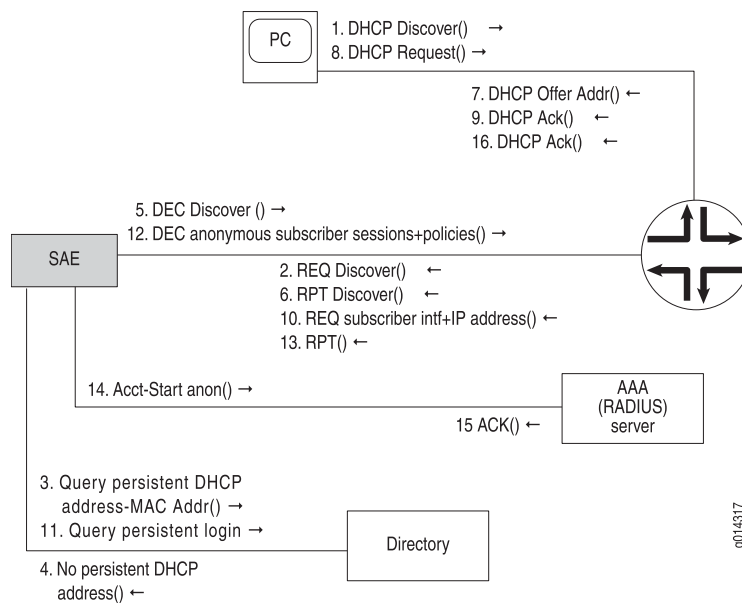
The first time a subscriber's network device starts, the router assigns an IP address to it. This address allows the subscriber access only to the SAE. The router provides this IP address for a short period of time called the lease time. After the lease time is over, the router provides a permanent IP 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 2 on page 2 shows the interactions that take place when a DHCP subscriber starts a network device.

Figure 2: 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:

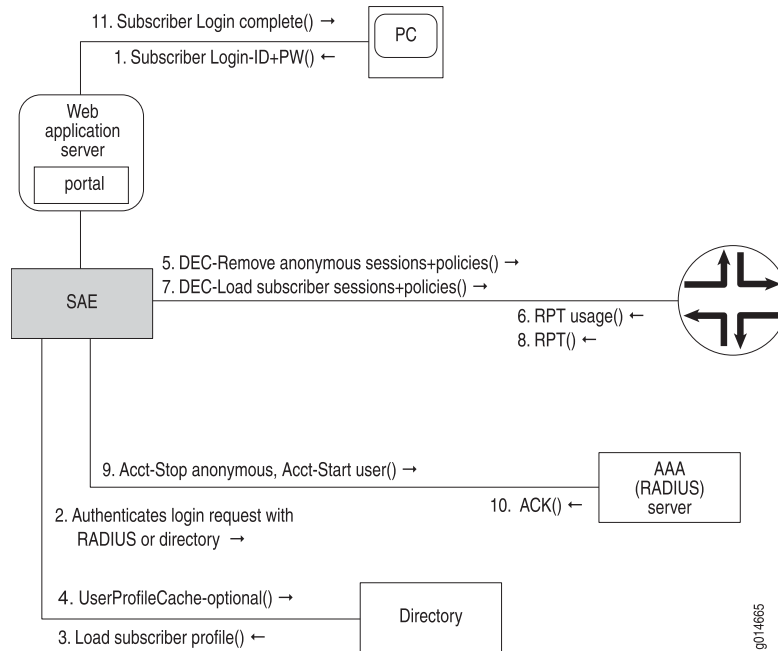
1. The DHCP client in the subscriber's network device broadcasts a discover message to the router.
2. The router acts on the discover message by sending a COPS request (REQ) message to the SAE, indicating that an IP address is about to be assigned by the local DHCP server on the local router. This request 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.)
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 3 on page 4 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 3: DHCP Subscriber Login



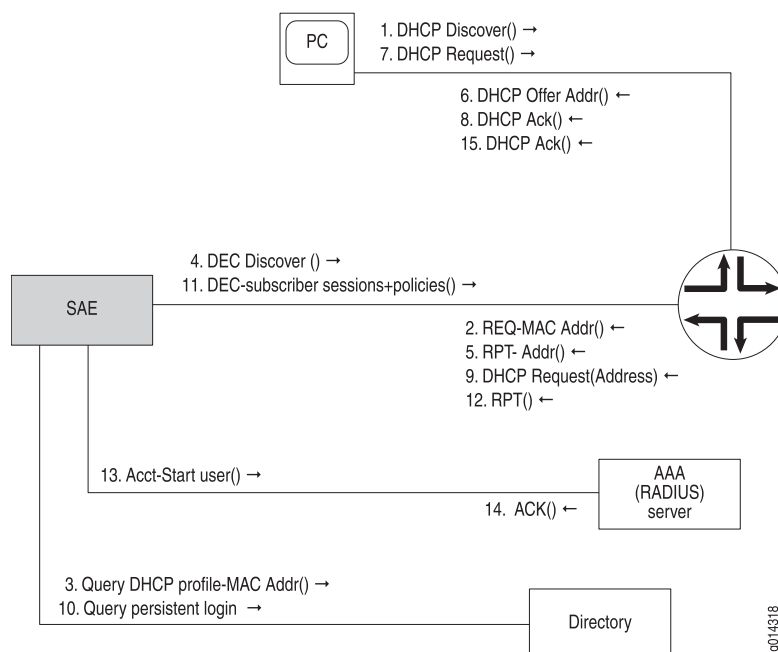
The sequence is as follows:

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 4 on page 5 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 4: Persistent DHCP Subscriber Login



The login sequence is as follows:

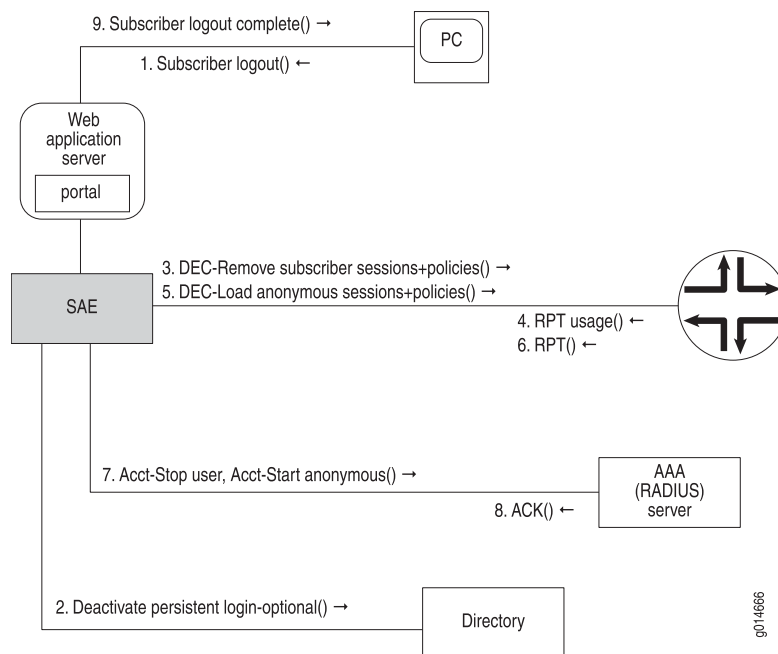
1. The DHCP client in the subscriber's network device sends a discover message to the router.
2. The router sends a COPS request (REQ) message to the SAE, informing the SAE that the router has received a DHCP discover request. The message includes the MAC address of the subscriber's network device and 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 5 on page 6 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 5: 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.

