

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

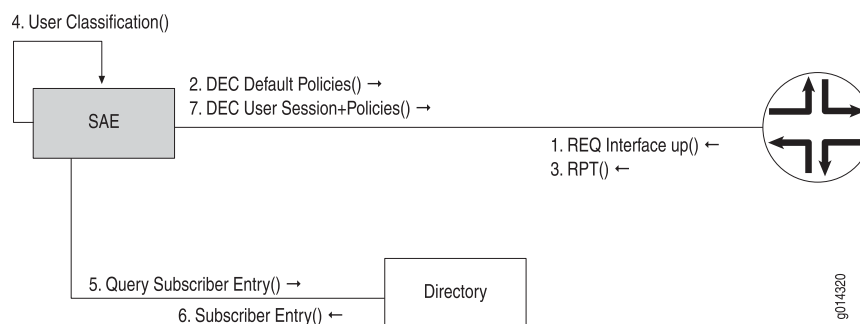
See Figure 1 on page 1.

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 1: Static IP Subscriber Login



Subscriber IP Address Not Known

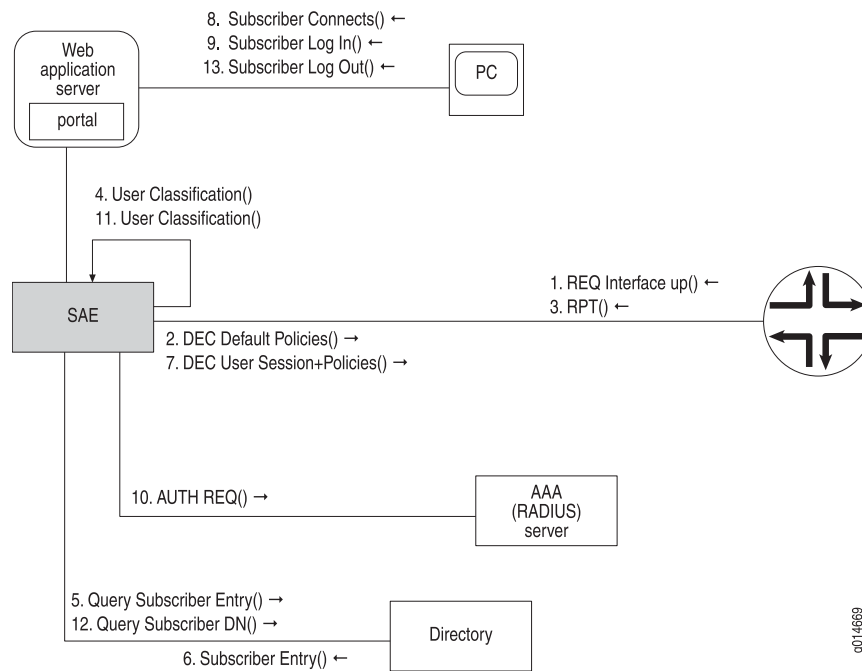
See Figure 2 on page 3.

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 2: Subscriber IP Address Not Known



- Related Topics**
- Overview of Subscribers
 - Overview of Classification Scripts
 - Classifying Interfaces (SRC CLI)
 - Allowing Multiple Logins from the Same IP Address

