

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.

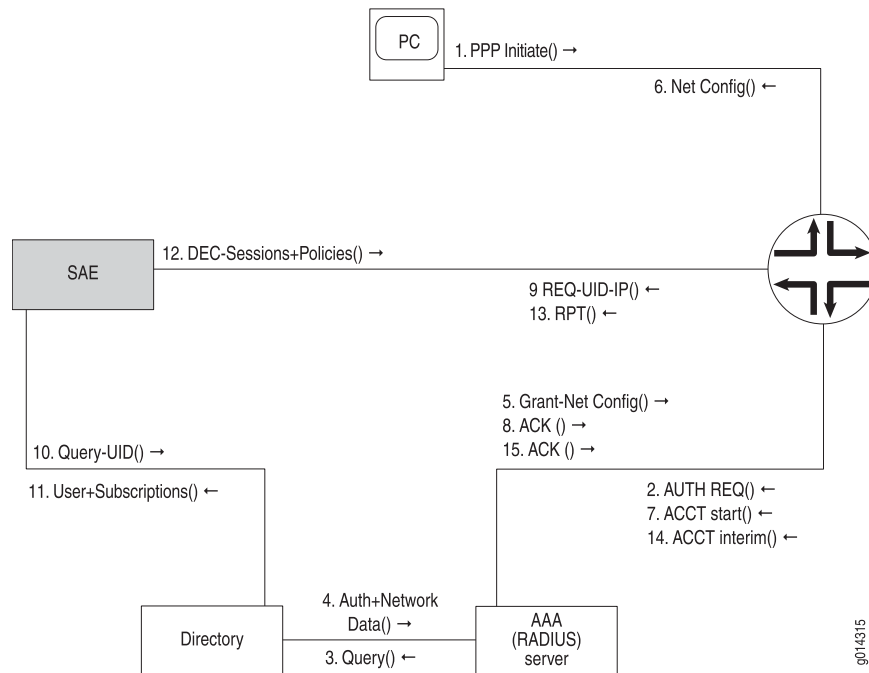
As a consequence, the Service Selection Portal (SSP) API allows creation of a Web application that:

- 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 1 on page 2 shows the interactions that take place during a PPP login.

Figure 1: 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

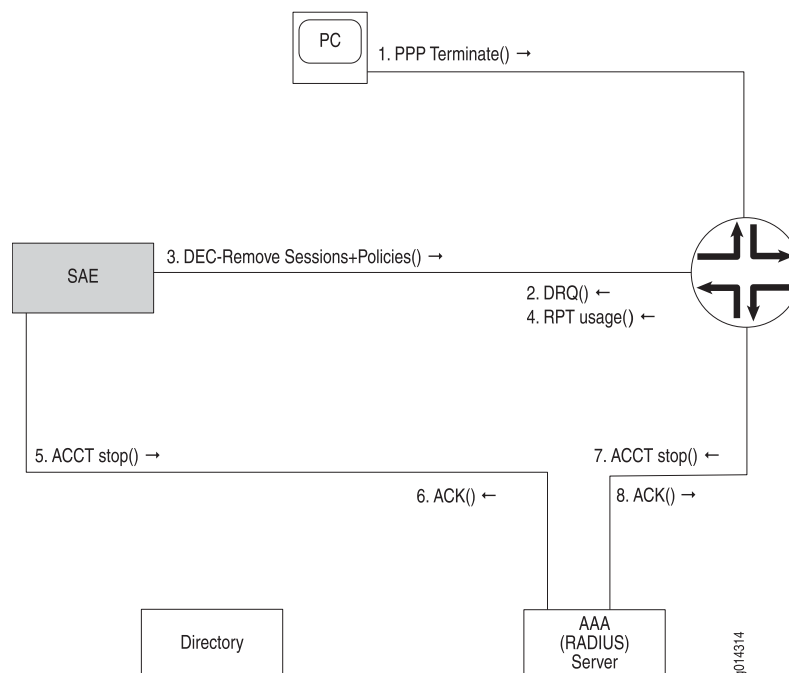
the subscriber session so that it can associate later requests from the subscriber with this session by looking at the source IP address of the request.

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 2 on page 3 shows the interactions that take place when a subscriber logs out of a PPP session.

Figure 2: 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.)
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.