DHCP Authentication Process

This section illustrates the DHCP authentication process. As illustrated in Figure 32.1, the DHCP authentication process begins when a DHCP client attempts to connect to the network. The member DHCP server checks if the MAC address of the DHCP client matches a MAC address in the guest or authenticated MAC address filters. If the member does not find a match, it assigns an IP address from the quarantine range to the DHCP client. When the client tries to access a web site, it is redirected to the captive portal page.

Figure 32.1 Stage 1: Quarantining an Unauthenticated DHCP Client

![Diagram showing Stage 1: Quarantining an Unauthenticated DHCP Client]

Note that the quarantine range in Figure 32.1 contains MAC address filters to deny leases in the quarantine range to DHCP clients with MAC addresses that match those in the Guest and Authenticated MAC address filters. When the client connects to the captive portal IP address through its web browser, the user can register and continue the authentication process to obtain an IP address from the authenticated DHCP range, or register as a guest and obtain an IP address from the guest DHCP range.

If the user chooses to continue the authentication process, as shown in Figure 32.2, the member authenticates the user with the authentication service that you configured, which can be RADIUS, LDAP, or AD.

Figure 32.2 Stage 2a: Authenticating the User
After the client successfully passes the authentication stage, the appliance stores the MAC address of the client in the MAC address filter for the authenticated range. When the client tries to renew its IP address, it receives a new IP address from the authenticated DHCP range.

Note that if the MAC address filter has an expiration period, the member automatically deletes expired MAC addresses from the filter. Therefore, if a DHCP client tries to renew its IP address after the expiration period, the client is redirected to the captive portal because its MAC address is no longer in the MAC address filter. For more information, see Defining MAC Address Filters.

If the user chooses to sign in as a guest, as shown in Figure 32.3, the user can fill in the guest registration page provided by the captive portal.

Figure 32.3 Stage 2b: Registering as a Guest
After the user signs in as a guest, the appliance stores the MAC address of the client in the MAC address filter for the guest range. When the DHCP client tries to renew its IP address, it receives a new IP address from the guest DHCP range, unless the MAC address of the client expired and was removed from the filter. In this case, the DHCP client is redirected to the captive portal.

The quarantined DHCP client connects to the captive portal.

The user chooses to register as a guest, so the server displays the guest registration page. The user enters information on the guest registration page.

The member adds the MAC address of the client to the MAC address filter for the authenticated range and assigns the client system an IP address in the authenticated range.

After the user signs in as a guest, the appliance stores the MAC address of the client in the MAC address filter for the guest range. When the DHCP client tries to renew its IP address, it receives a new IP address from the guest DHCP range, unless the MAC address of the client expired and was removed from the filter. In this case, the DHCP client is redirected to the captive portal.