CHAP authentication over PPP

CHAP is a stronger authentication method than PAP because the user’s actual password never crosses the communications channel. CHAP uses a three-way handshake to verify the identity of the peer. The handshake is done upon initial link establishment, and it may be repeated periodically thereafter to ensure the identity of the peer. The CHAP initiation sequence and three-way handshake occur as follows and as illustrated in Figure 1:

(1) The PPP link is established after dialup. The network access server is configured to support PPP and CHAP.

(2) The network access server tells the remote client to use CHAP.

(3) The remote client responds with an OK.

(4) The three-way handshake occurs as follows:

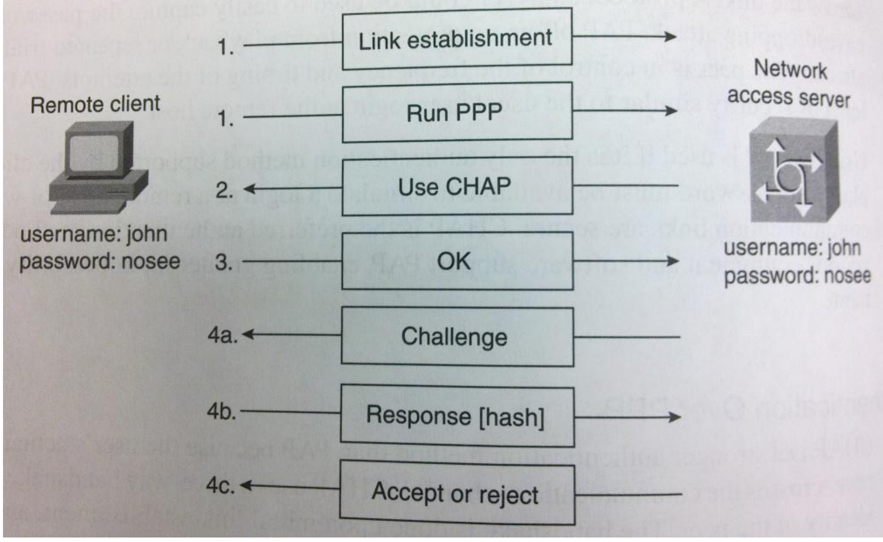
  a. The network access server sends a challenge message to the remote client.

  b. The remote client replies with a one-way hash value.

  c. The network access server processes the received hash value. If it matches the station’s own calculation, authentication is acknowledged. Passwords are not sent over the link.

CHAP periodically verifies the identity of the remote client by using a three-way handshake. The network access server sends a challenge message to the remote node. The remote nodes responds with a value calculated using a one-way hash function (typically MD5). The network access server checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged. Otherwise, the connection is terminated immediately.

Figure 1



CHAP authentication depends on a “secret” know only to the authenticator and the remote client. The secret is not send over the link. Although the authentication is only one-way, by negotiating CHAP in both directions, the same secret set may easily be used for mutual authentication.