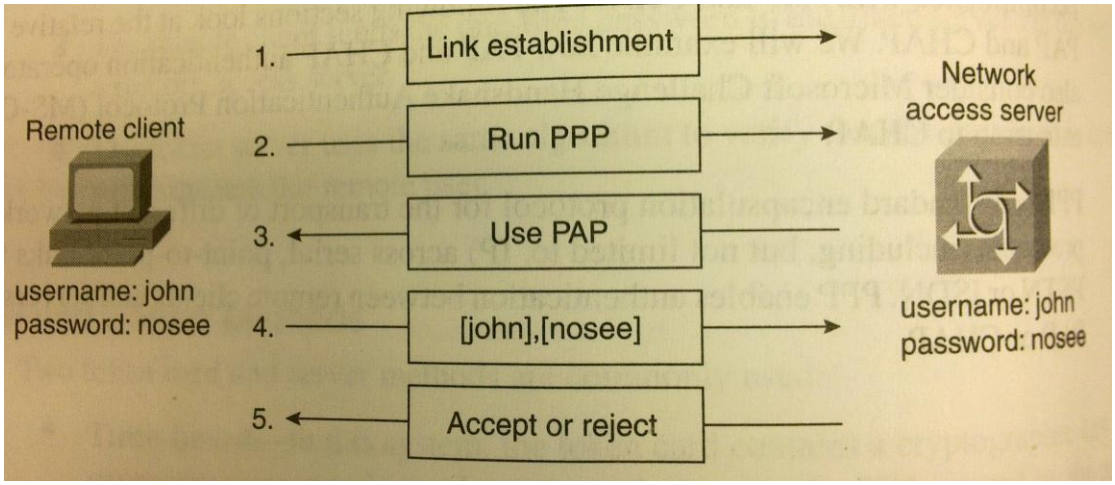
PAP authentication over PPP

PAP authentication, which uses PPP, provides a simple way for the remote client to establish its identity: a two-way handshake (see Figure 1). The handshake is done only after initial PPP link establishment. After the link establishment phase is complete, a username/password pair is repeatedly sent by the peer to the authenticator until authentication is acknowledged or the connection is terminated. Here are the messages exchanged during PAP authentication:

1 The remote client establishes the dialup link.
2 The remote client tells the network access server that it is running PPP.
3 The network access server, configured to use PAP, notifies the remote client to use PAP in this session.
4 The remote client sends the username and password in PAP format.
5 The network access server compares the username and password to that stored in its database and accepts or rejects the username and password entered.



PAP is not a strong authentication method. The username and password are sent in clear text across the link. A protocol analyzer could be used to easily capture the password in an eavesdropping attack. PAP offers no protection from playback or repeated trial-and-error attacks. The peer is in control of the frequency and timing of the attempts. PAP provides a level of security similar to the usual user at the remote host.