PPP Authentication Protocols

Windows Server 2003 and Windows XP support the following PPP authentication protocols:

PAP or Password Authentication Protocol

The oldest forms of authentication schemes used where the user credential are sent in plain text. This is not the securest form of passing authentication credentials as anybody can use a third party sniffer program and capture these clear text username and password as they are unencrypted. The next thing that would happens is the news of a server being compromised due to intruder attack. Avoid using PAP as much as you can.

CHAP or Challenge-Handshake Authentication Protocol

CHAP is better than PAP as its uses encrypted authentication mechanism which would protect the username and password from being sent if the destination NAS server does not support this authentication method. Basically, the actual password will not be transmitted over the network, instead when the basic PPP connection is established, the NAS server sends a challenge phrase associated with a Session ID to the remote client. Then the remote client uses a specific MD5 (message digest version 4) hash algorithm to answer the challenge string with the username and an answer to the hash challenge with its username, network ID and password. The username will still be sent in plain text though.

CHAP is definitely a better choice than PAP where the password is sent in clear-text. But in CHAP the password is mixed up in hash form as an answer to the challenge string sent by the NAS server. Once the answer to the hash challenge is received the NAS server which already know the password, authenticates the user immediately. CHAP keeping sending challenges for the user to reply and verify its identity several times during the connection making it a more secure connection

from any intrusion. The advantage CHAP carries over PAP is the way a user is authenticated over a dial-up or direct PPP connection.

MS-CHAP or Microsoft Challenge-Handshake Authentication Protocol

MSCHAP is an encrypted authentication mechanism which works very similar to CHAP. We have seen in CHAP, where a NAS server sends a challenge to the client consisting of a Session ID and a hash challenge string. The remote client then, returns back the challenge with the session ID and MD4 based hashed answer. The introduction of MD4 gave an extra level of security where the clear-text was replaced with the hash passwords. MS-CHAP gave more attributes to the secure transmission of password over the wire by adding more error code aware attributes like, password expired code, next level of encryption between client and server allowing user to change there password while connected to the NAS server or during authentication process. The additional encryption between client and server is supported by using an encryption key to support data encryption by MPPE (Microsoft Point to Point Encryption).

MS-CHAP v2 or Microsoft Challenge Handshake Authentication Protocol Version 2

The newer version of MS-CHAP was introduced some after the older one giving it a name MS-CHAP V2. The encryption authentication mechanism was updated with much stronger security specifically when the username and password can now be exchanged along with determination of encryption keys. Initially the NAS server attempts to send the session ID and challenge to the remote client. The remote client uses the hash algorithm to reply back to NAS server's challenge string along with the supported encryption type, the session ID, its own peer challenge and the user password. In next step, the NAS server verifies client's information and responds with the another ID specifying the reason if this connection was a success or failure based upon the information like the negotiated encryption type, Peer challenge response, and decision on the NAS server challenge (the password client has provided).

The remote client verifies this information with the one it sent before and connects to the NAS server. If for some reason the authentication response was ot correct, the remote client will terminate the connection. Therefore, it's a behavior where the both client and server authenticate each other mutually. Also, there are two type of encryption keys used, one of sending the data and the other one receiving the data.

EAP or Extensible Authentication Protocol

EAP was lately introduced as the newest PPP authentication protocol with MS CHAP V2 based features. During the authentication phase EAP is not in the picture! That's the biggest difference between EAP and other methods. EAP does not perform any sort of authentication, it in-fact only negotiates the actual EAP type and the user authentication is done by the Domain controller which hold the user database or a RADIUS (Remote Dial-in User Service) which works are an agent to get user credentials verified against a Domain Controller.

Until MS-CHAP V2, this authentication was happening only at the NAS server with the user database but with EAP, it's against a central user database holder or a Domain Controller only.

EAP is a new PPP authentication protocol that allows for an arbitrary authentication method. Once the user is connected over PPP, NAS server immediately collects the user credentials and sends them over to a RADIUS or Domain Controller for verification.

Source: http://www.tech-faq.com/ppp-authentication-protocols.html