# 3. Find and document as much as possible for the VPN authentication protocols: PAP/CHAP/MS-CHAP/MS-CHAPV2.

## 1. PAP (Password Authentication Protocol):

A password authentication protocol (uncapitalized) is an authentication protocol that uses a password.

PAP is used by Point to Point Protocol to validate users before allowing them access to server resources. Almost all network operating system remote servers support PAP.

PAP transmits unencrypted ASCII passwords over the network and is therefore considered insecure. It is used as a last resort when the remote server does not support a stronger authentication protocol, like CHAP or EAP (while the last is actually a framework).

Working cycle

Client sends username and password

Server sends authentication-ack (if credentials are OK) or authentication-nak (otherwise)

PAP Packets

Description

PAP packet embedded in a PPP frame. The protocol field has a value of C023 (hex).

## 2. CHAP (Challenge-Handshaking Authentication Protocol):

In computing, the Challenge-Handshake Authentication Protocol (CHAP) authenticates a user or network host to an authenticating entity. That entity may be, for example, an Internet service provider. CHAP is specified in RFC 1994.

CHAP provides protection against replay attacks by the peer through the use of an incrementally changing identifier and of a variable challenge-value. CHAP requires that both the client and server know the plaintext of the secret, although it is never sent over the network. The MS-CHAP variant does not require either peer to know the plaintext, but has been broken.[1] Thus, CHAP provides better security as compared to Password Authentication Protocol (PAP).

Working cycle

CHAP is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake. This happens at the time of establishing the initial link (LCP), and may happen again at any time afterwards. The verification is based on a shared secret (such as the client user's password).[2]

After the completion of the link establishment phase, the authenticator sends a "challenge" message to the peer.

The peer responds with a value calculated using a one-way hash function on the challenge and the secret combined.

The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator acknowledges the authentication; otherwise it should terminate the connection.

The ID chosen for the random challenge is also used in the corresponding response, success, and failure packets. A new challenge with a new ID must be different from the last challenge with another ID. If the success or failure is lost, the same response can be sent again, and it triggers the same success or failure indication. For MD5 as hash the response value is MD5(ID||secret||challenge), the MD5 for the concatenation of ID, secret, and challenge.

## 3. MS-CHAP (Microsoft version of Challenge-Handshaking Authentication Protocol):

MS-CHAP is the Microsoft version of the Challenge-Handshake Authentication Protocol, CHAP. The protocol exists in two versions, MS-CHAPv1 (defined in RFC 2433) and MS-CHAPv2 (defined in RFC 2759). MS-CHAPv2 was introduced with Windows NT 4.0 SP4 and was added to Windows 98 in the "Windows 98 Dial-Up Networking Security Upgrade Release" and Windows 95 in the "Dial Up Networking 1.3 Performance & Security Update for MS Windows 95" upgrade. Windows Vista dropped support for MS-CHAPv1.

MS-CHAP is used as one authentication option in Microsoft's implementation of the PPTP protocol for virtual private networks. It is also used as an authentication option with RADIUS servers which are used for WiFi security using the WPA-Enterprise protocol. It is further used as the main authentication option of the Protected Extensible Authentication Protocol (PEAP).

Compared with CHAP, MS-CHAP:

is enabled by negotiating CHAP Algorithm 0x80 (0x81 for MS-CHAPv2) in LCP option 3, Authentication Protocol

provides an authenticator-controlled password change mechanism

provides an authenticator-controlled authentication retry mechanism

defines failure codes returned in the Failure packet message field

MS-CHAPv2 provides mutual authentication between peers by piggybacking a peer challenge on the Response packet and an authenticator response on the Success packet.

## 4. MS-CHAPv2 (Microsoft version2 of Challenge-Handshaking Authentication Protocol):

Windows 2000 includes support for Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) that provides stronger security for remote access connections. MS-CHAP v2 offers the additional security features:

LAN Manager encoding of responses and password changes is no longer supported.

Two-way authentication verifies the identity of both sides of the connection. The remote access client authenticates against the remote access server and the remote access server authenticates against the remote access client. Two-way authentication, also known as mutual authentication, ensures that the remote access client is dialing into a remote access server that has access to the user's password. Mutual authentication provides protection against remote server impersonation.

Separate cryptographic keys are generated for transmitted and received data.

The cryptographic keys are based on the user's password and the arbitrary challenge string. Each time the user connects with the same password, a different cryptographic key is used.

The use of MS-CHAP v2 is negotiated during LCP negotiation by specifying the authentication protocol LCP option (type 3), the authentication protocol 0xC2-23, and the algorithm 0x81. Once LCP negotiation is complete, MS-CHAP messages use the PPP protocol ID of 0xC2-23.

MS-CHAP v2 authentication is an exchange of three messages:

The remote access server sends an MS-CHAP v2 Challenge message to the remote access client that consists of a session identifier and an arbitrary challenge string.

The remote access client sends an MS-CHAP v2 Response message that contains:

The user name.

An arbitrary peer challenge string.

An Secure Hash Algorithim (SHA) hash of the received challenge string, the peer challenge string, the session identifier, and the MD4-hashed version of the user's password.

The remote access server checks the MS-CHAP v2 Response message from the client and sends back an MS-CHAP v2 Response message containing:

An indication of the success or failure of the connection attempt.

An authenticated response based on the sent challenge string, the peer challenge string, the client's encrypted response, and the user's password.

The remote access client verifies the authentication response and if it is correct, uses the connection. If the authentication response is not correct, the remote access client terminates the connection.