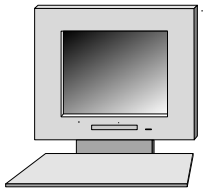

1. Hello

Random: ServerChallenge (16 Bytes)

2. ServerChallenge

Random: ClientChallenge (16 Bytes)
ChallengeHash =
SHA-1(ClientChallenge | ServerChallenge | Username)
NTHash = MD4(Password)
PaddedNTHash = NTHash | 0x00 00 00 00 00
ClientResponse = $DES_{PaddedNTHash[0,...,6]}$(ChallengeHash[0,..7]) |
$DES_{PaddedNTHash[7,...,13]}$(ChallengeHash[0,..7]) |
$DES_{PaddedNTHash[14,...,20]}$(ChallengeHash[0,..7])

3. ClientResponse, ClientChallenge

NTHashHash = MD4(NTHash)
Digest = SHA-1(NTHashHash | ClientResponse | const)
ServerResponse = (Digest | ClientChallenge | padding)

4. ServerResponse