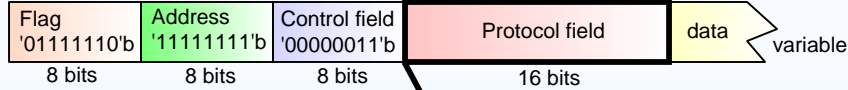


Authentication Protocols - PAP / CHAP

(Using Password and Challenge-Handshake Authentication Protocols with PPP Encapsulation)

HDLC-framed PPP packet has the following structure:



x'c023' Password Authentication protocol
x'c223' Challenge Handshake Authentication protocol

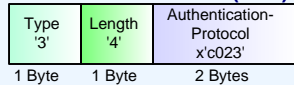
RFC 1994
August 1996

In order to establish communications over a point-to-point link, a peer must first send LCP packets to configure the data link during the link establishment phase. After the link has been established, PPP provides for an authentication phase before proceeding to the Network-Layer Protocol phase.

Password Authentication Protocol (PAP)

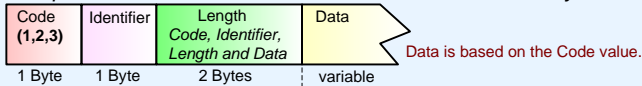
PAP uses clear text (unencrypted) password authentication. There is no protection from playback or repeated trial & error requests. Uses a two-way handshake to verify the identity of the remote peer.

Optional Point-to-Point Protocol (PPP) Link Control Protocol (LCP) Data Packet



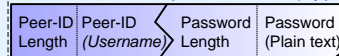
PAP Packet Layout

encapsulated in the Information field of a PPP Data Link Layer frame



- 1 - Authenticate-Request
- 2 - Authenticate-Acknowledgement
- 3 - Authenticate-Nak negative acknowledge

Authenticate-Request Packet (Type 1)



Authenticate-Ack Packet (Type 2)



Authenticate-Nak Packet (Type 3)



The Peer-ID field is zero or more octets and indicates the name of the peer to be authenticated

The message field is intended to be human readable, and MUST NOT affect operation of the protocol.

It is recommended that the message content be ASCII characters and 126 decimal characters.

Type	Configuration Option
1	Maximum-Receive-Unit
2	Async-Control-Character-Map
3	Authentication-Protocol
4	Quality-Protocol
5	Magic-Number
6	RESERVED
7	Protocol-Field-Compression
8	Address-and-Control-Field-Compression
9	FCS-Alternatives
10	Self-Describing-Pad
11	Numbered-Mode
12	Multi-Link-Procedure
13	Callback
14	Connect-Time
15	Compound-Frames
16	Nominal-Data-Encapsulation
17	Multilink-MRRU
18	Multilink-Share-Number
19	Multilink-Share-Number
20	...
21	...

Challenge-Handshake Authentication Protocol (CHAP)

CHAP requires a challenge-response handshake. Used to Periodically verify the identity of the remote peer.

Optional Point-to-Point Protocol (PPP) Link Control Protocol (LCP) Data Packet

Type

Copyright © IT charts.com