

Virtual Private Networks

FEUP

MPR

Type of VPNs

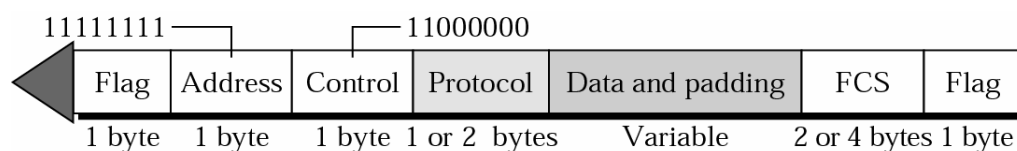
- ◆ Secure VPNs
 - » Built by customers
 - » Constructed using encryption
 - » PPP, PPTP, L2TP, IPSec

- ◆ Trusted VPNs
 - » Built by ISP, which provides and maintains the circuits integrity
 - » Layer 2 frames over MPLS, VLANs

PPP – Point-to-Point Protocol

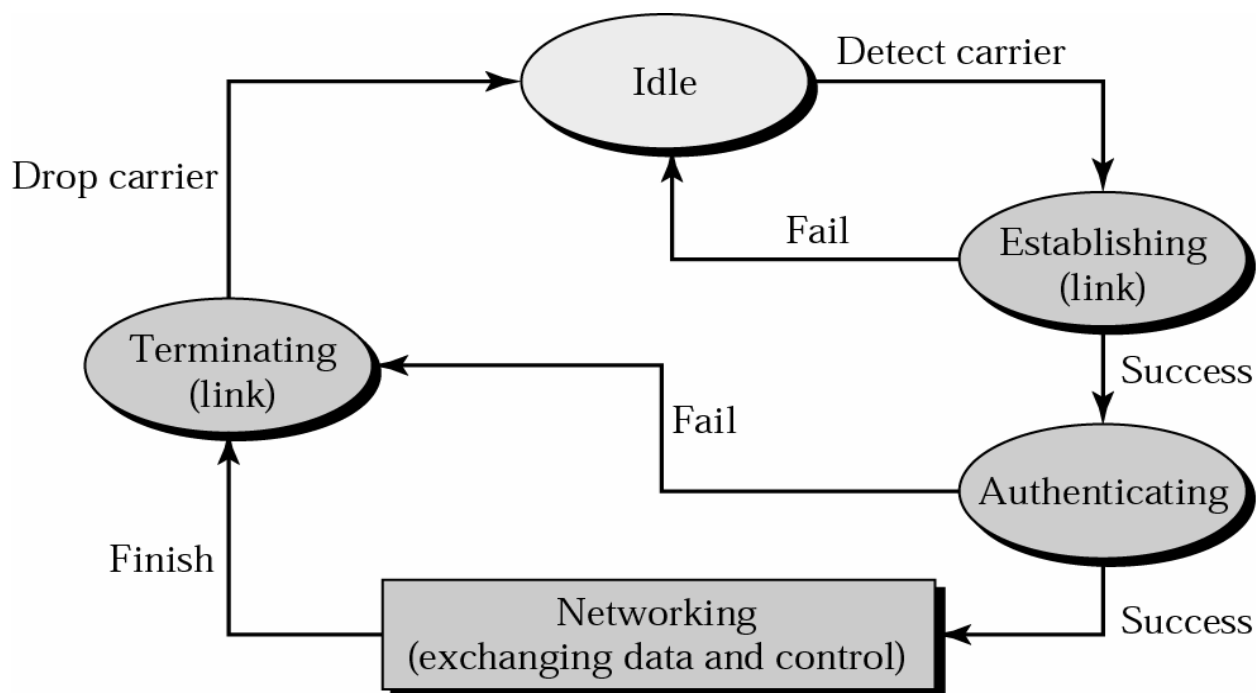
Point-to-Point Protocol

- ◆ PPP - The Point-to-Point Protocol
 - RFC 1661, RFC 2153
- ◆ Method for transporting datagrams over point-to-point links
- ◆ 3 main components
 - » method for encapsulating multi-protocol datagrams
 - » LCP - Link Control Protocol
 - establishing, configuring, testing the data-link connection
 - » Family of NCP - Network Control Protocols
 - establishing, configuring different network-layer protocols

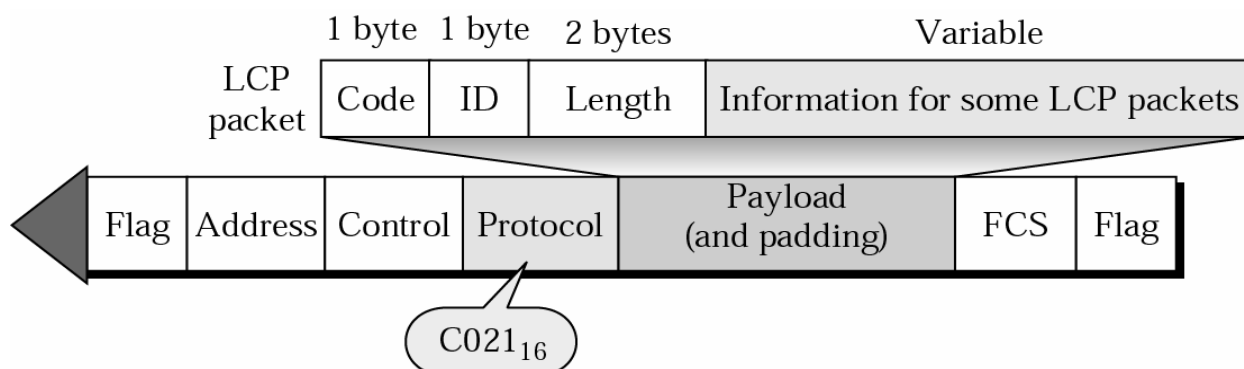


Flag: start/end of frame (01111110); **Address:** broadcast address; **Protocol:** protocol encapsulated

Transition States



LCP Packet in a Frame



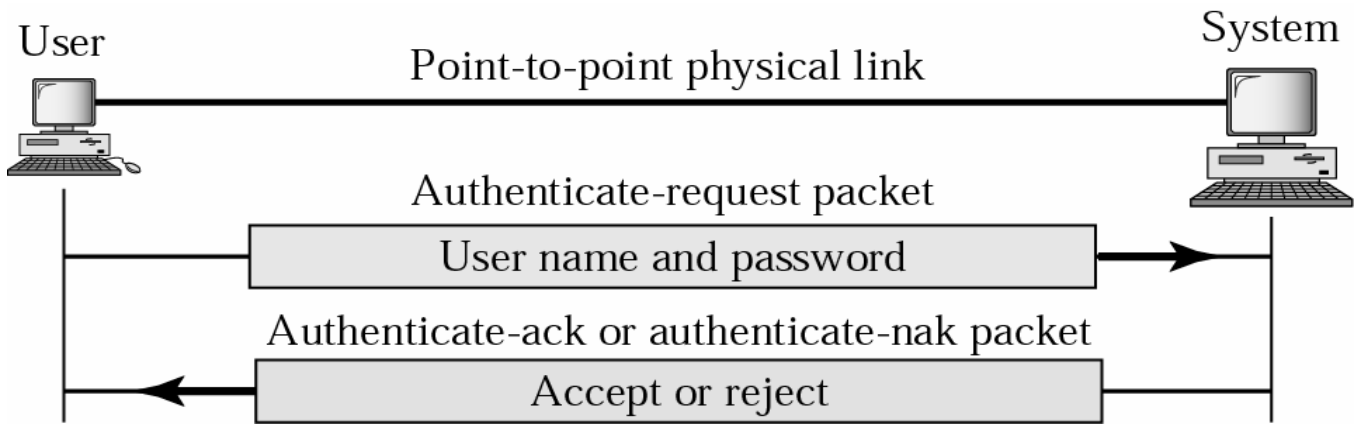
LCP Packet and Codes

Code 0x	Packet Type	Description
01	Configure-request	Contains the list of proposed options and their values
02	Configure-ack	Accepts all options proposed
03	Configure-nak	Announces that some options are not acceptable
04	Configure-reject	Announces that some options are not recognized
05	Terminate-request	Requests to shut down the line
06	Terminate-ack	Accepts the shut down request
07	Code-reject	Announces an unknown code
08	Protocol-reject	Announces an unknown protocol
09	Echo-request	A type of hello message to check if the other end is alive
0A	Echo-reply	The response to the echo-request message
0B	Discard-request	A request to discard the packet

Some Options and Their Values

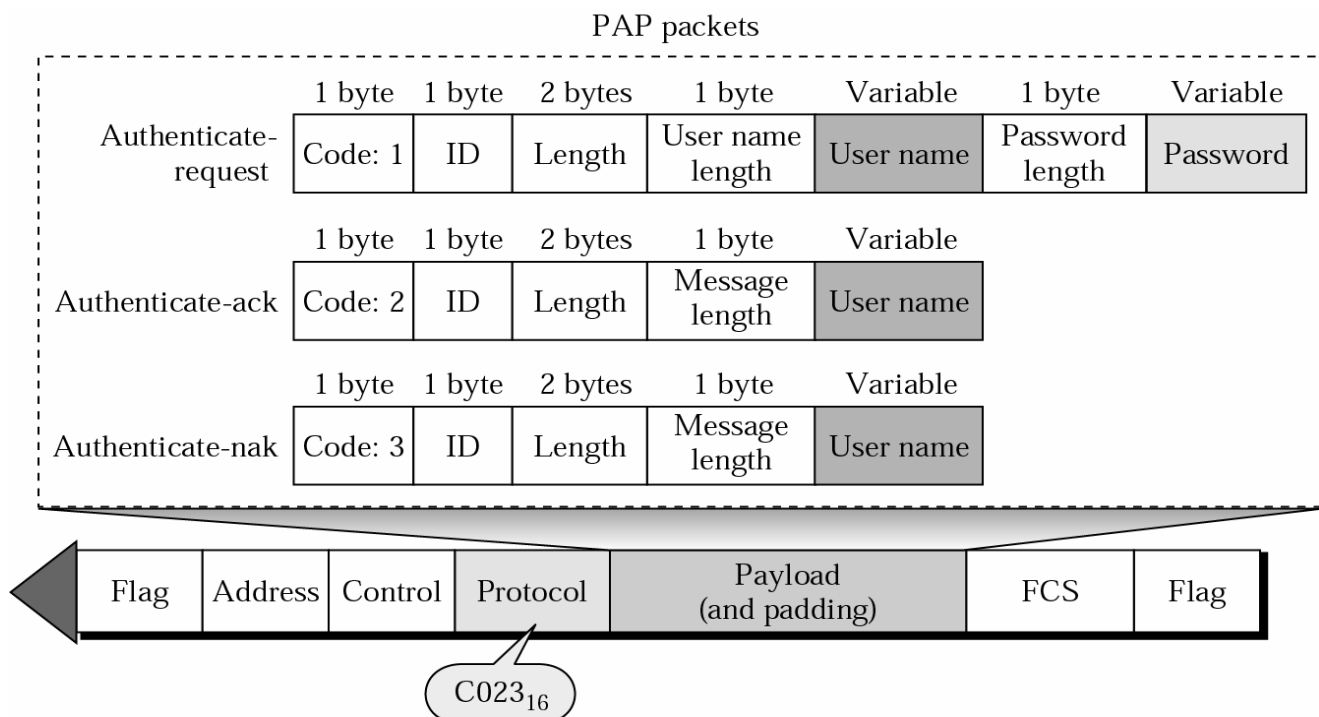
Option	Example Values
Maximum receive unit	1500
Authentication protocol	None, PAP, CHAP

PAP – Password Authentication Protocol



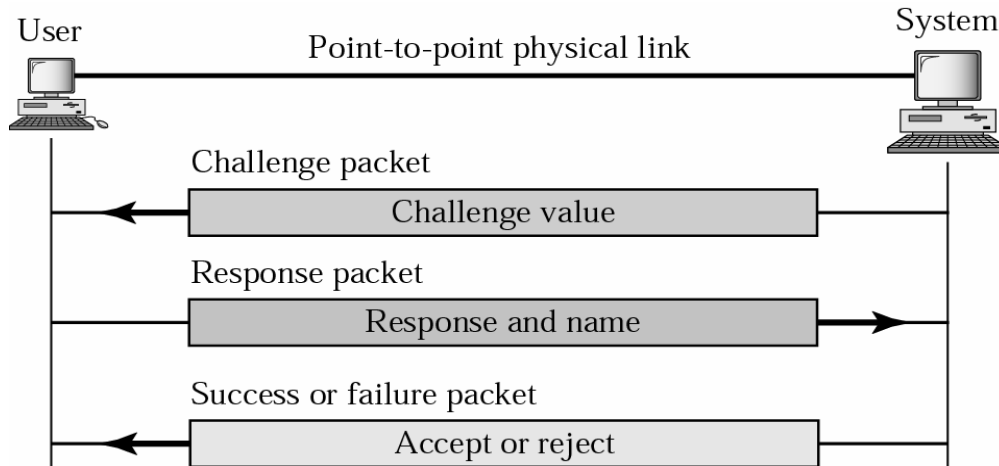
Poor Security: Usernames and Passwords sent in the clear

PAP Packets



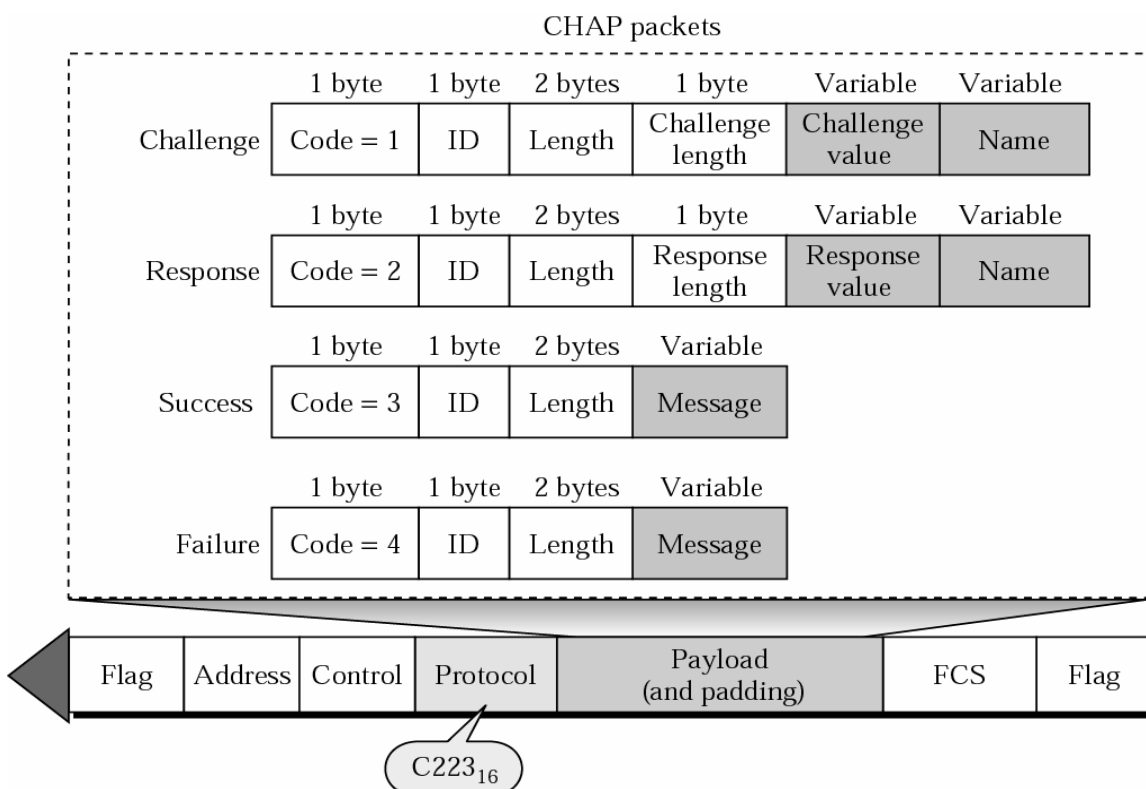
Challenge Handshake Authentication Protocol (CHAP) VPN 11

- ◆ System computes hash of challenge message plus secret
MD5
- ◆ If equals the response message, authentication is successful



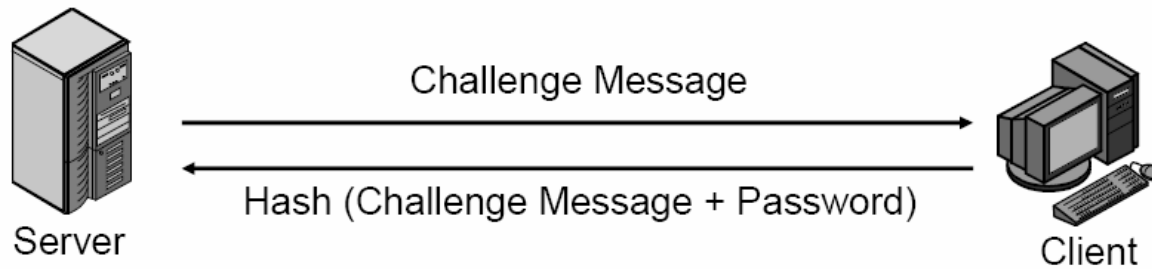
VPN 12

CHAP Packets



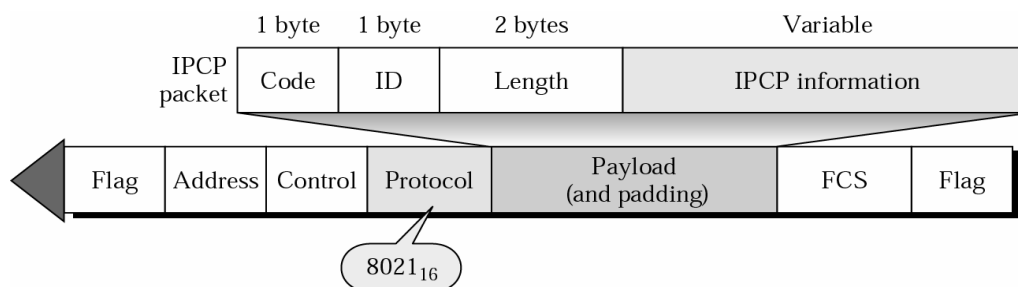
MS-CHAP Authentication

- ◆ CHAP but with password as the secret
- ◆ Widely used allows password authentication



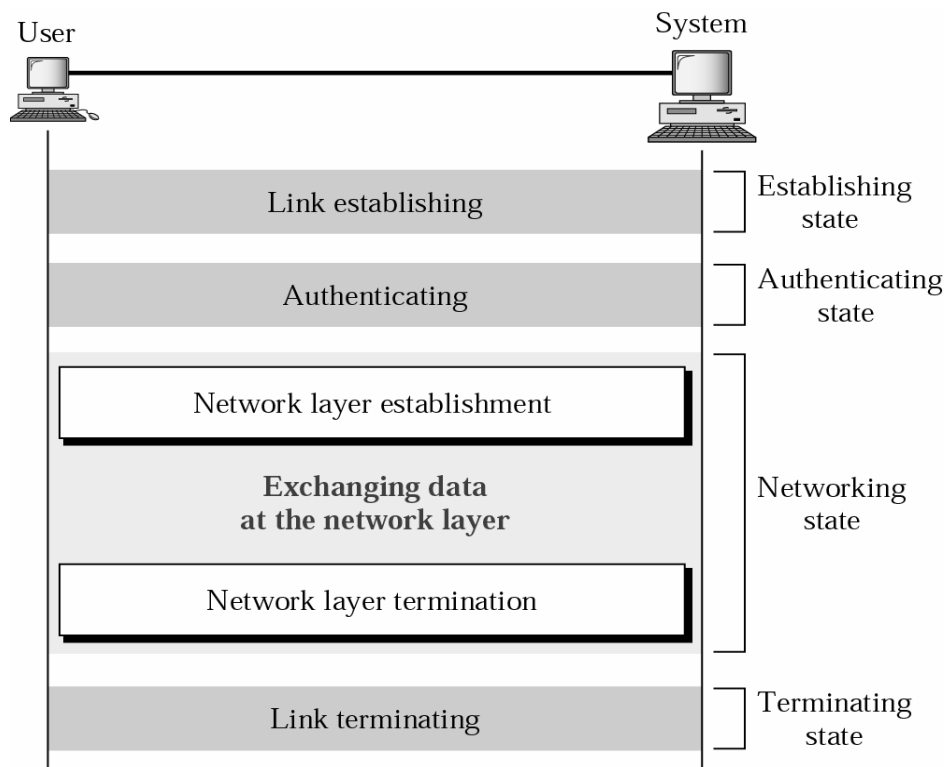
IPCP Packet encapsulated in PPP Frame

VPN 14



Code	IPCP Packet
01	Configure-request
02	Configure-ack
03	Configure-nak
04	Configure-reject
05	Terminate-request
06	Terminate-ack
07	Code-reject

Example



PPP Encryption

- ◆ IETF specifies DES and 3DES for PPP encryption
- ◆ Original PPP frame encrypted and placed in a new PPP frame with plaintext headers



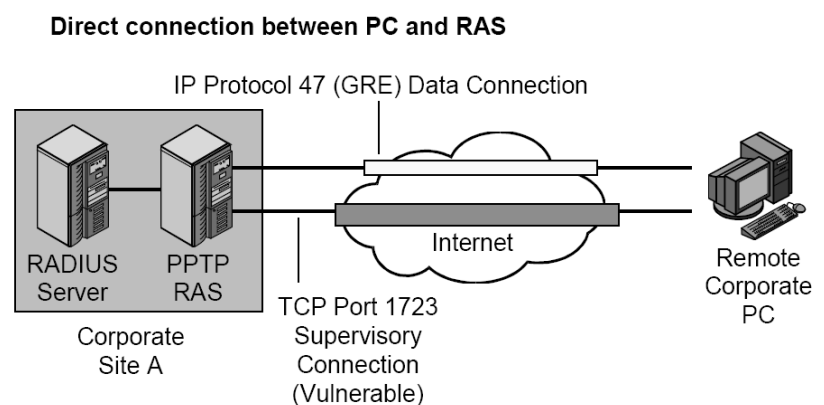
- ◆ Microsoft uses Microsoft Point-to-Point Encryption (MPPE)

PPTP – Point-to-Point Tunnelling Protocol

PPTP - Point-to-Point Tunneling Protocol VPN 18

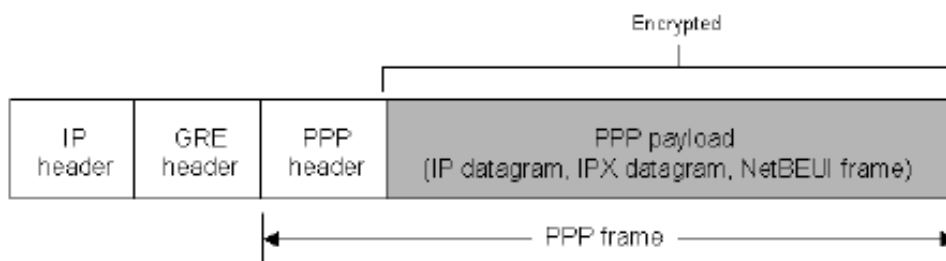
- ◆ Point-to-Point Tunneling Protocol (PPTP) [RFC 2637]
 - » Mainly implemented and used by Microsoft
 - » Extension of PPP
 - » Tunneling of PPP datagrams over IP networks

- ◆ Use of 2 connections
 - » Control connection
 - » Tunnel connection



PPTP

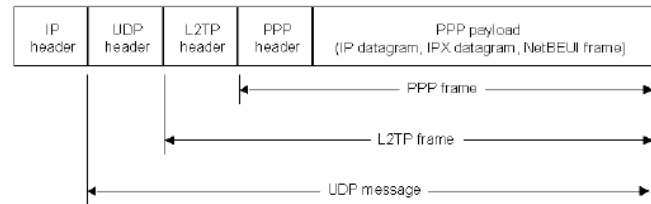
- Tunneling places the PPP frame in an IP packet
 - Encryption and authentication possible, as in PPP
 - GRE, Generic Routing Encapsulation for traffic tunneling
RFC 1701, RFC 2784



L2TP – Layer 2 Tunnelling Protocol

L2TP

- Layer 2 Tunneling Protocol
 - RFC 2661
- No control channel



- User
 - Makes dial-up/PPP to local access concentrator
 - Local phone calls
 - Access concentrator redirects PPP frames to ISP via internet
 - PPP/L2TP/UDP/IP frame from Access Concentrator to ISP
 - Multiplexing of individual PPP sessions
- Can be combined with IPSec