POINT-TO-POINT PROTOCOL (PPP)

- One of the most common protocols for point-to-point access is the **Point-to-Point Protocol (PPP).**

Services:

Services Provided by PPP

- PPP defines the format of the frame to be exchanged between devices. It also defines how two devices can negotiate the establishment of the link and the exchange of data.
- The new version of PPP, called ***Multilink*** *PPP,* provides connections over multiple links.

Services Not Provided by PPP

- PPP does not provide flow control.

Framing:

Flag:A PPP frame starts and ends with a 1-byte flag with the bit pattern 01111110.

Address: The address field in this protocol is a constant value and set to 11111111 (broadcast address).

Control: This field is set to the constant value 00000011.

Protocol: The protocol field defines what is being carried in the data field: either user data or other information. This field is by default 2 bytes long, but the two parties can agree to use only 1 byte.

Payload field: This field carries either the user data or other information.

FCS: The frame check sequence (FCS) is simply a 2-byte or 4-byte standard CRC.

Byte Stuffing:

- Since PPP is a byte-oriented protocol, the flag in PPP is a byte that needs to be escaped whenever it appears in the data section of the frame.
- The escape byte is 01111101,which means that every time the flag like pattern appears in the data, this extra byte is stuffed to tell the receiver that the next byte is not a flag.

Transition Phases:

- A PPP connection goes through phases which can be shown in a transition phase diagram. The transition diagram, which is an FSM, starts with the ***dead*** state.
- In this state, there is no active carrier and the line is quiet. When one of the two nodes starts the communication, the connection goes into the ***establish*** state.

- In this state, options are negotiated between the two parties. If the two parties agree that they need authentication then the system needs to do authentication otherwise, the parties can simply start communication.
- The link-control protocol packets, discussed shortly, are used for this purpose. Several packets may be exchanged here.
- Data transfer takes place in the ***open*** state. When a connection reaches this state, the exchange of data packets can be started.
- The connection remains in this state until one of the endpoints wants to terminate the connection. In this case, the system goes to the ***terminate*** state. The system remains in this state until the carrier is dropped, which moves the system to the ***dead*** state again.

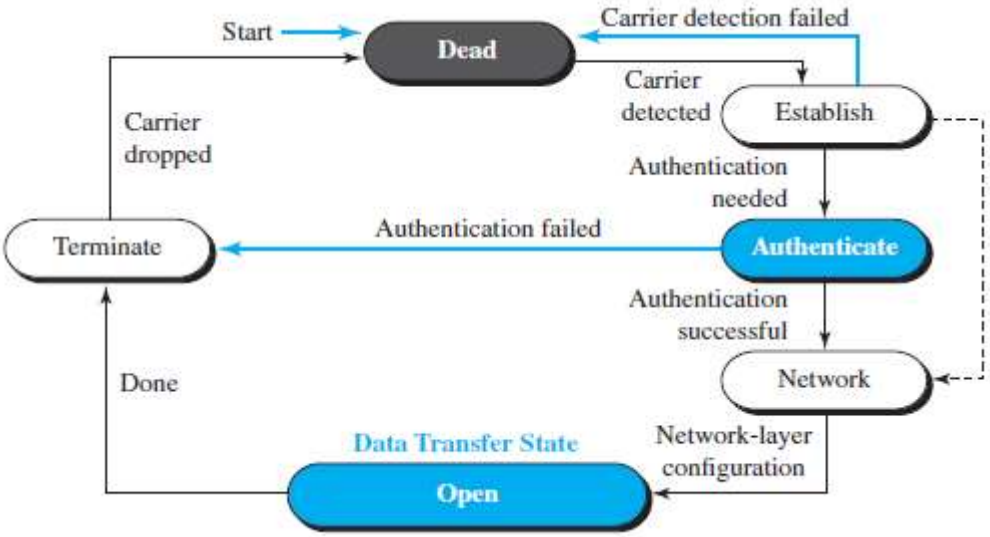

Fig: Transition phases

Multiplexing:

- PPP is a link-layer protocol, it uses another set of protocols to establish the link, authenticate the parties involved, and carry the network-layer data.
- Three sets of protocols are defined to make PPP powerful: The Link Control Protocol (LCP), two Authentication Protocols (APs), and several Network Control Protocols (NCPs).

Link Control Protocol:

- The **Link Control Protocol (LCP)** is responsible for establishing, maintaining, configuring ,and terminating links. It also provides negotiation mechanisms to set options between the two endpoints.

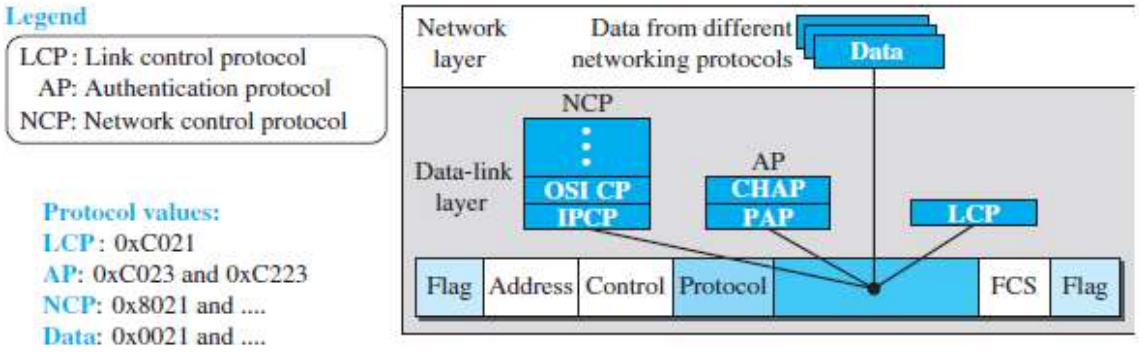

Fig: Multiplexing in PPP

- All LCP packets are carried in the payload field of the PPP frame with the protocolfield set to C021 in hexadecimal.

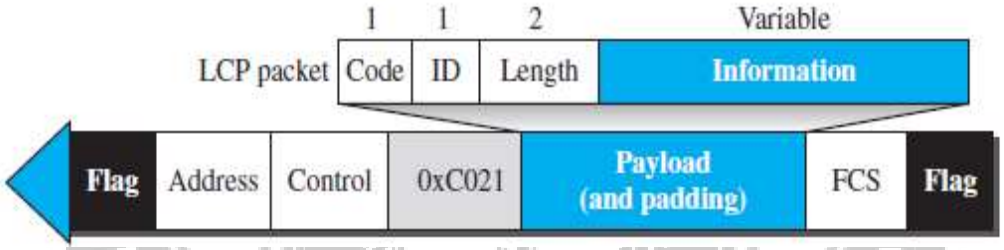

Fig: LCP packet encapsulated in a frame.

LCP packets:

- There are three categories of packets. The first category, comprising the first four packet types, is used for link configuration during the establish phase.
- The second category, comprising packet types 5 and 6, is used for link termination during the termination phase. The last five packets are used for link monitoring and debugging.
- The ID field holds a value that matches a request with a reply.
- The length field defines the length of the entire LCP packet. The information field contains information, such as options, needed for some LCP packets.

Table: LCP packets

Code	Packet Type	Description
0x01	Configure-request	Contains the list of proposed options and their values
0x02	Configure-ack	Accept all options proposed
0x03	Configure-nak	Announces that some options are not acceptable
0x04	Configurw-reject	Announces that some options are not recognized

0x05	Terminate-request	Request to shut down the line
0x06	Terminate-ack	Accept the shutdown request
0x07	Code-reject	Announces an unknown code
0x08	Protocol-reject	Announces an unknown protocol
0x09	Echo-request	A type of hello message to check if the other end is alive
0x0A	Echo-reply	The response to the echo-request message
0x0B	Discard-request	A request to discard the packet

Authentication Protocols:

- Authentication plays a very important role in PPP because PPP is designed for use overdial-up links where verification of user identity is necessary.
- Authentication means validating the identity of a user who needs to access a set of resources. PPP has created two protocols for authentication: Password Authentication Protocol and Challenge Handshake Authentication Protocol.

PAP:

- The **Password Authentication Protocol (PAP)** is a simple authentication procedure with a two-step process:

a. The user who wants to access a system sends an authentication identification(usually the user name) and a password.

b. The system checks the validity of the identification and password and either accepts or denies connection.

CHAP:

- The **Challenge Handshake Authentication Protocol (CHAP)** is a three-way handshaking authentication protocol that provides greater security than PAP. In this method, the password is kept secret; it is never sent online.

a. The system sends the user a challenge packet containing a challenge value, usually a few bytes.

b. The user applies a predefined function that takes the challenge value and the user's own password and creates a result. The user sends the result in the response packet to the system.

c. The system does the same. It applies the same function to the password of the user (known to the system) and the challenge value to create a result. If the result created is the same as the result sent in the response packet, access is granted; otherwise, it is denied. CHAP is more secure than PAP.

Network Control Protocols:

IPCP:

- One NCP protocol is the **Internet Protocol Control Protocol (IPCP).** This protocol configures the link used to carry IP packets in the Internet.

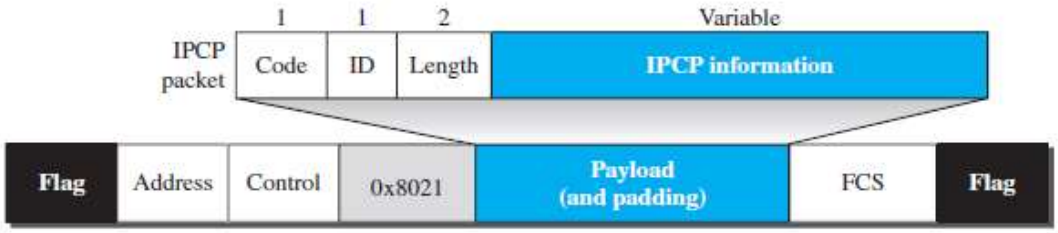

Fig: IPCP packet encapsulated in PPP frame

Table Code value for IPCP packets:

Code	IPCP Packet
0x01	Configure-request
0x02	Configure-ack
0x03	Configure-nak
0x04	Confugure-reject
0x05	Configure-request
0x06	Terminate-ack
0x07	Code-reject