CSS2C08

COMPUTER NETWORKS

MODULE 4

1. **LINK LAYER SERVICES**

2. **ERROR DETECTION AND CORRECTION**

3. **MULTIPLE ACCESS PROTOCOLS**

4. **LAN ADDRESS**

5. **ARP**

6. **ETHERNET**

7. **HUBS ,BRIDGES and SWITCHES**

8. **WIRELESS LINKS**
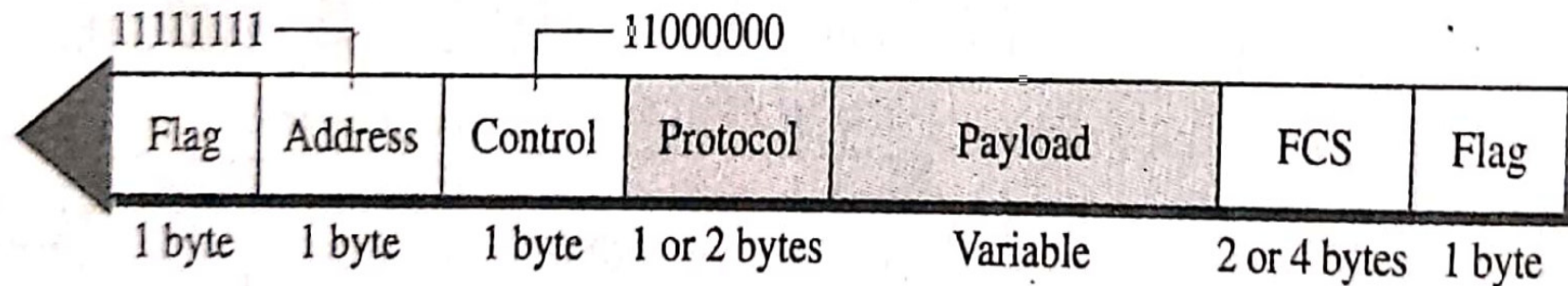
9. **PPP**

10. **ATM**

Point to point protocol(PPP)

➢ Point - to - Point Protocol (PPP) is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers.

➢ It is a byte - oriented protocol that is widely used in broadband communications having heavy loads and high speeds.

➢ It is used to connect the Home PC to the server of ISP via a modem.

➢ **PPP provides several services:**

1. PPP defines the format of the frame to be exchanged between devices.

2. PPP defines how two devices can negotiate the establishment of the link and the exchange of data.

3. PPP defines how network layer data are encapsulated in the data link frame.

4. PPP defines how two devices can authenticate each other.

5. PPP provides multiple network layer services supporting a variety of network layer protocols.

6. PPP provides connections over multiple links.

7. PPP provides network address configuration. This is particularly useful when a home user needs a temporary network address to connect to the Internet.

➤ PPP Frame Format:

```
11111111 ──────┐         ┌────── 11000000
```

Flag	Address	Control	Protocol	Payload	FCS	Flag
1 byte	1 byte	1 byte	1 or 2 bytes	Variable	2 or 4 bytes	1 byte

❖ **Flag field**: Flag field marks the beginning and end of the PPP frame. Flag byte is 01111110. (1 byte).

❖ **Address field**: This field is of 1 byte and is always 11111111. This address is the broadcast address *i.e.* all the stations accept this frame.

❖ **Control field**: This field is also of 1 byte. The value is always 00000011 to show that the frame does not contain any sequence numbers and there is no flow control or error control.

❖ **Protocol field**: This field specifies the kind of packet in the data field *i.e.* what is being carried in data field.

❖ **Payload field**: Its length is variable. If the length is not negotiated using LCP during line set up, a default length of 1500 bytes is used. It carries user data or other information.

❖ **FCS field**: The frame checks sequence. It is either of 2 bytes or 4 bytes. It contains the checksum.

➤ Transition Phases in PPP :

❖ A PPP connection goes through phases which can be shown in a transition phase diagram .
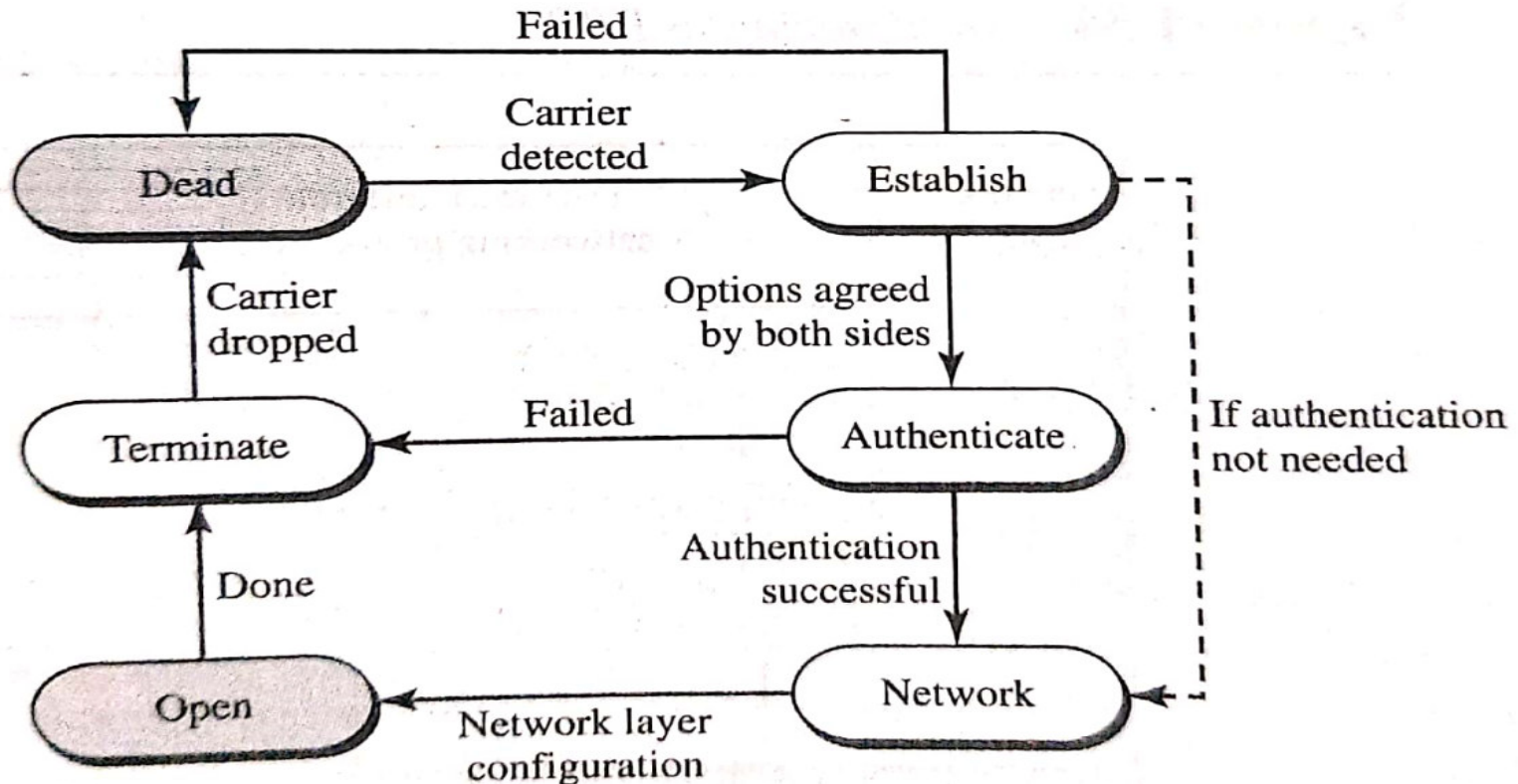
1. **Dead**: In dead phase the link is not used. There is no active carrier and the line is quiet.

2. **Establish**: Connection goes into this phase when one of the nodes start communication. In this phase, two parties negotiate the options. If negotiation is successful, the system goes into authentication phase or directly to networking phase. LCP packets are used for this purpose.

3. **Authenticate**: This phase is optional. The two nodes may decide during the establishment phase, not to skip this phase. However if they decide to proceed with authentication, they send several authentication packets. If the result is successful, the connection goes to the networking phase; otherwise, it goes to the termination phase.
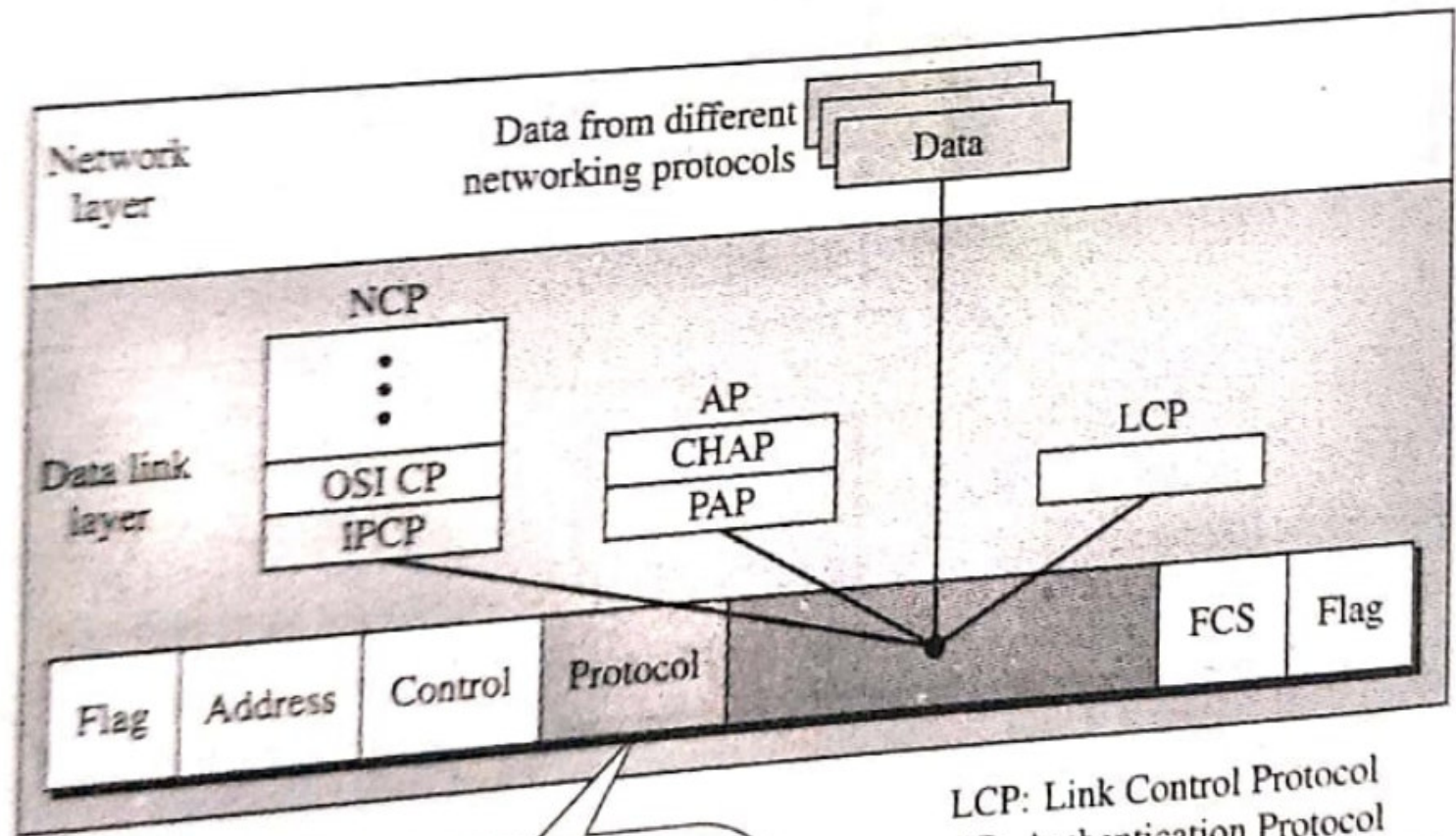
4. **Network**: In network phase, negotiation for the network layer protocols takes place. PPP specifies that two nodes establish a network layer agreement before data at the network layer can be exchanged. This is because PPP supports several protocols at network layer. If a node is running multiple protocols simultaneously at the network layer, the receiving node needs to know which protocol will receive the data.

5. **Open**: In this phase, data transfer takes place. The connection remains in this phase until one of the endpoints wants to end the connection.

6. **Terminate**: In this phase connection is terminated.

➤ **Point-to-point protocol Stack**

❖ PPP uses several other protocols to establish link, authenticate users and to carry the network layer data.

❖ The various protocols used are:

1. Link Control Protocol

2. Authentication Protocol

3. Network Control Protocol

Network layer

Data from different networking protocols

Data

Data link layer

NCP

⋮

OSI CP

IPCP

AP

CHAP

PAP

LCP

FCS | Flag

Flag | Address | Control | Protocol

LCP: 0xC021
AP: 0xC023 and 0xC223
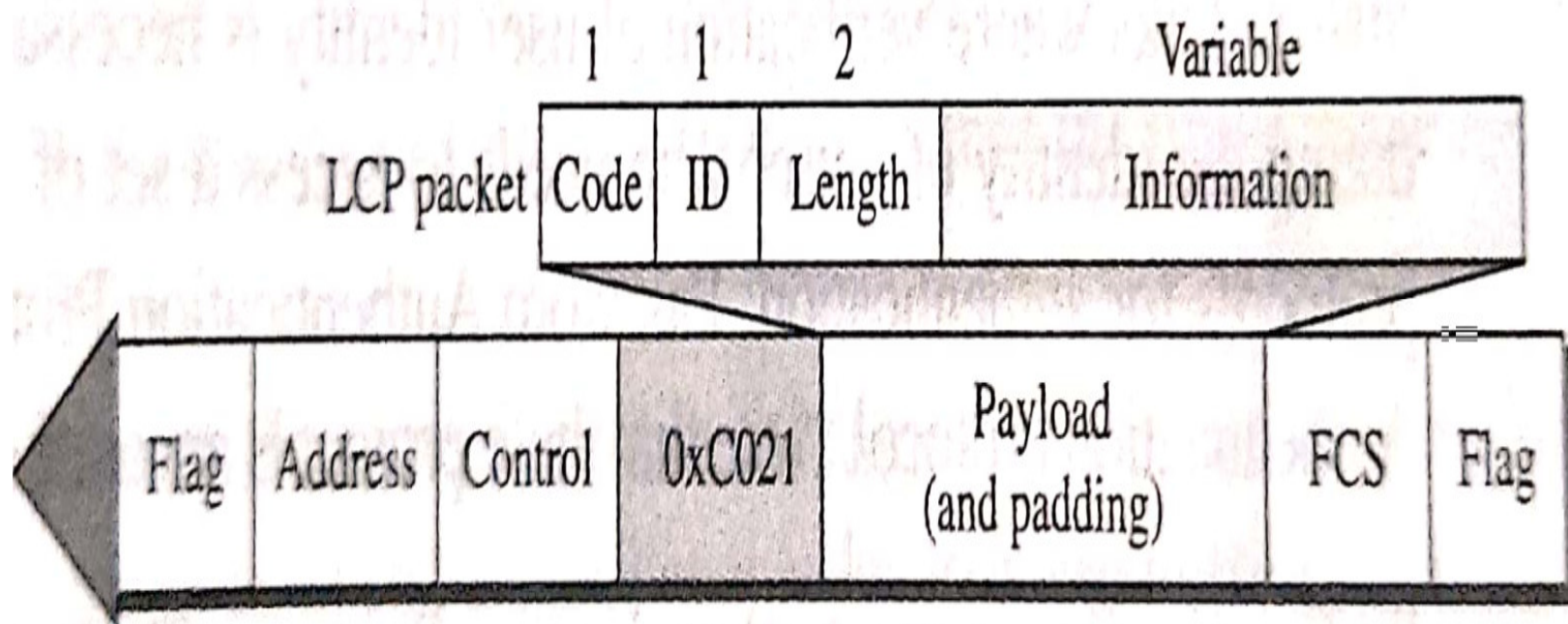NCP: 0x8021 and ....
Data: 0x0021 and ....

LCP: Link Control Protocol
AP: Authentication Protocol
NCP: Network Control Protocol

1. 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.

❖ All LCP packets are carried in the data field of the PPP frame

❖ The presence of a value $C021_{16}$ in the protocol field of PPP frame indicates that LCP packet is present in the data field.

❖ The various fields present in LCP packet are:

1. **Code**: 1 byte-specifies the type of LCP packet.

2. **ID**: 1 byte-holds a value used to match a request with the reply.

3. **Length**: 2 byte-specifies the length of entire LCP packet.

4. **Information**: Contains extra information required for some LCP packet.

	1	1	2	Variable
LCP packet	Code	ID	Length	Information

Flag	Address	Control	0xC021	Payload (and padding)	FCS	Flag

❖ There are eleven different type of LCP packets. These are categorized in three groups:

a) **Configuration packet**: These are used to negotiate options between the two ends. For example: configure-request, configure-ack, configure-nak, configure-reject are some configuration packets.

b) **Link termination packets**: These are used to disconnect the link between two end points. For example: terminate-request, terminate-ack, are some link termination packets.

c) **Link monitoring and debugging packets**: These are used to monitor and debug the links. For example: code-reject, protocol-reject, echo-request, echo-reply and discard-request are some link monitoring and debugging packets.

2. Authentication Protocol

❖ Authentication means validating the identity of a user who needs to access a set of resources.

❖ PPP has created two protocols for authentication:

a) Password Authentication Protocol and

b) Challenge Handshake Authentication Protocol.

a) Password Authentication Protocol(PAP):

❖ This protocol provides two step authentication procedures:

1. User name and password is provided by the user who wants to access a system.

2. The system checks the validity of user name and password and either accepts or denies the connection.

❖ PAP packets are also carried in the data field of PPP frames. The presence of PAP packet is identified by the value $C023_{16}$ in the protocol field of PPP frame.

❖ There are three PAP packets.

  ❖ **Authenticate-request**: used to send user name & password.

  ❖ **Authenticate-ack**: used by system to allow the access.

  ❖ **Authenticate-nak**: used by system to deny the access

System

Authenticate-request →

← Authenticate-ack or authenticate-nak

PAP packets
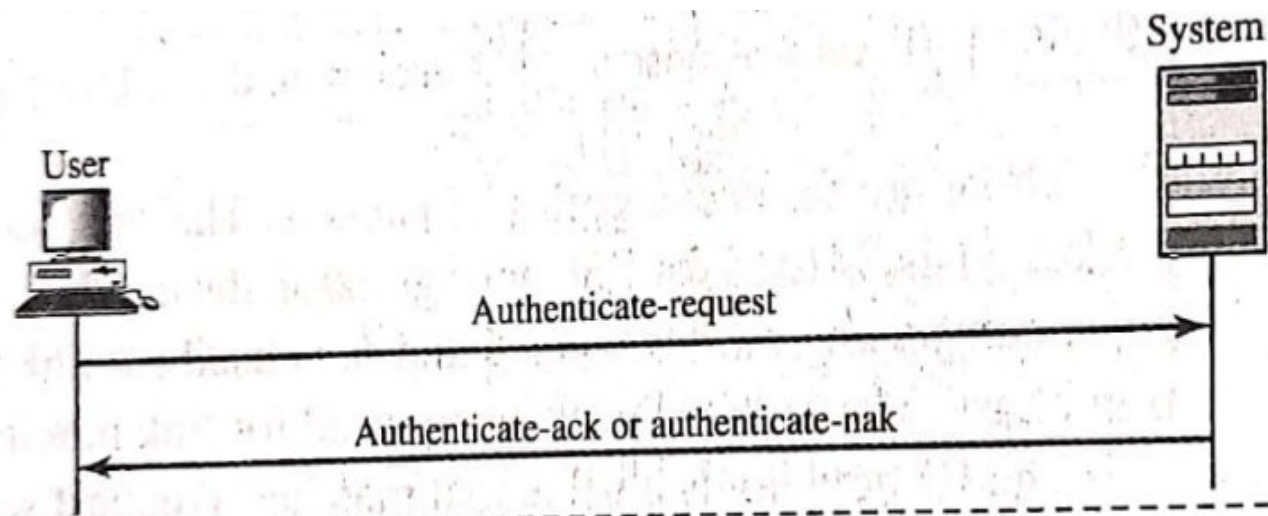
	1	1	2	1	Variable	1	Variable
Authenticate-request	Code: 1	ID	Length	User name length	User name	Password length	Password
Authenticate-ack	Code: 2	ID	Length	Message length	User name		
Authenticate-nak	Code: 3	ID	Length	Message length	User name		

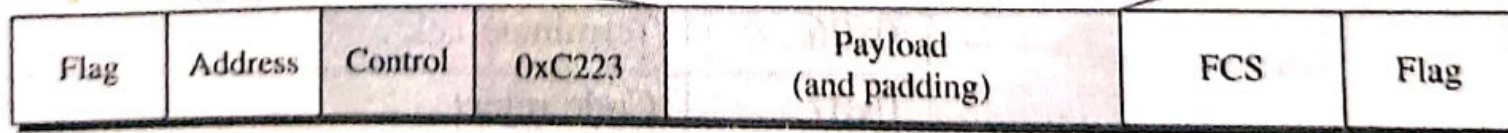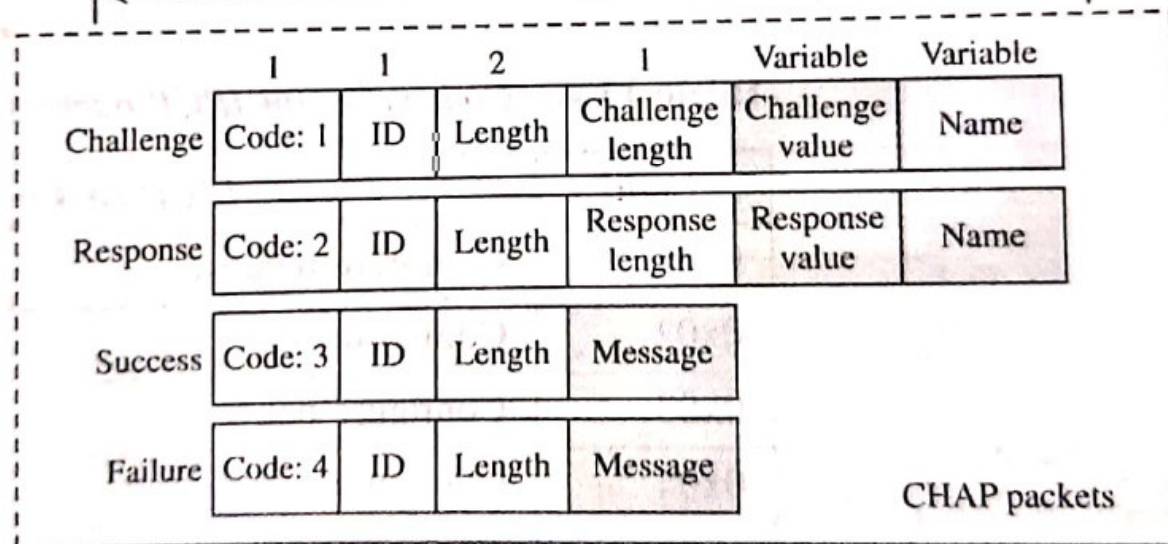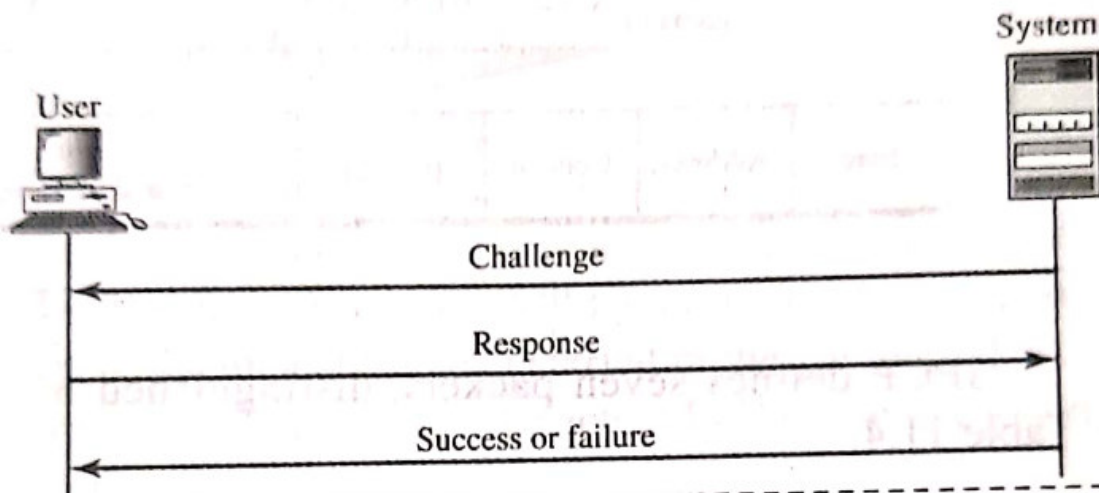| Flag	Address	Control	C023₁₆	Payload (and padding)	FCS	Flag
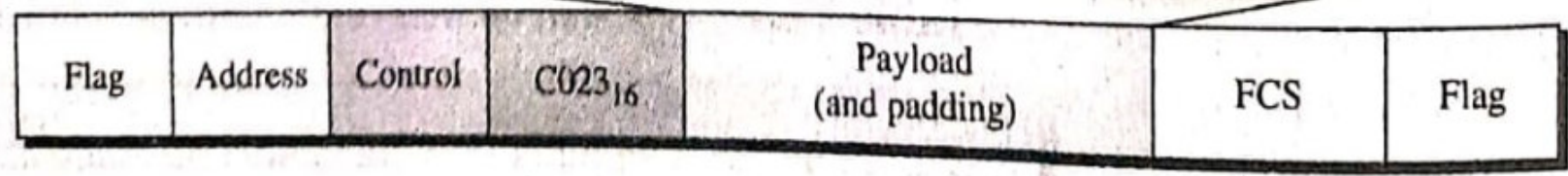
b) CHAP (Challenge Handshake Authentication Protocol)

❖ It provides more security than PAP. In this method, the password is kept secret; it is never sent online.

❖ It is a three-way hand-shaking authentication protocol

1. System sends, a challenge packet to the user. This packet contains a value, usually a few bytes.

2. Using a predefined function, a user combines this challenge value with the user password and sends the resultant packet back to the system.

3. System then applies the same function to the password of the user and challenge value and creates a result. If result is same as the result sent in the response packet, access is granted, otherwise, it is denied.

❖**There are 4 types of CHAP packets:**

1. **Challenge**-used by system to send challenge value.

2. **Response**-used by the user to return the result of the calculation.

3. **Success**-used by system to allow access to the system.

4. **Failure**-used by the system to deny access to the system.

User

System

Challenge

Response

Success or failure

		1	1	2	1	Variable	Variable
Challenge	Code: 1	ID	Length	Challenge length	Challenge value	Name	
Response	Code: 2	ID	Length	Response length	Response value	Name	
Success	Code: 3	ID	Length	Message			
Failure	Code: 4	ID	Length	Message			

CHAP packets

Flag	Address	Control	0xC223	Payload (and padding)	FCS	Flag

3. Network Control Protocol (NCP):

❖ After establishing the link and authenticating the user, PPP connects to the network layer. This connection is established by NCP. Therefore NCP is a set of control protocols that allow the encapsulation of the data coming from network layer. After the network layer configuration is done by one of the NCP protocols, the users can exchange data from the network layer.

❖ PPP can carry a network layer data packet from protocols defined by the Internet, DECNET, Apple Talk, Novell, OSI, Xerox and so on. None of the NCP packets carry networks layer data. They just configure the link at the network layer for the incoming data.