Point-to-Point Protocol (PPP)

PPP is the most commonly used data link protocol. It is used to connect the Home PC to the server of ISP via a modem.

• This protocol offers several facilities:

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

2. It defines link control protocol (LCP) for:-

(a) Establishing the link between two devices.

(b) Maintaining this established link.

(c) Configuring this link.

(d) Terminating this link after the transfer.

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

4. PPP provides error detection.

5. PPP allows the IP address to be assigned at the connection time i.e. dynamically. Thus a temporary IP address can be assigned to each host.

7. PPP provides multiple network layer services supporting a variety of network layer protocol. For this PPP uses a protocol called NCP (Network Control Protocol).

8. It also defines how two devices can authenticate each other.

PPP Frame Format

The frame format of PPP resembles HDLC frame. Its various fields are:

Flag	Address		Control			Flag
01111110	11111111	00000011	Protocol	Data	FCS	01111110
1 byte	1 byte	1 byte	1 or 2 byte	Variable	2 or 4 byte	

PPP frame Format

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

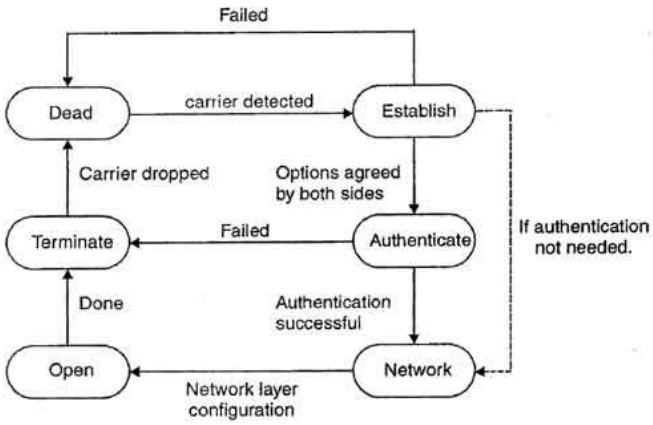
2. **Address field**: This field is of 1 byte and is always 11111111. This address is the broadcast address *i.e.* all the stations accept this frame.

3. **Control field**: This field is also of 1 byte. This field uses the format of the U-frame (unnumbered) in HDLC. 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.

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

5. **Data 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.

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



Transition phases

Transition Phases in PPP

The PPP connection goes through different states as shown in fig.

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

1. Link Control Protocol

• It is responsible for establishing, maintaining, configuring and terminating the link.

• It provides negotiation mechanism to set options between two endpoints.

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

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

1. **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.

2. **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.

3. **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 protocols help to validate the identity of a user who needs to access the resources.

There are two authentication protocols:

1. Password Authentication Protocols (PAP) 2. Challenge Handshake Authentication Protocol (CHAP)

1. PAP (Password Authentication Protocol)
This protocol provides two step authentication procedures:
Step 1: User name and password is provided by the user who wants to access a system.
Step 2: The system checks the validity of user name and password and either accepts or denies the connection.
1. **Authenticate-request**: used to send user name & password.
2. **Authenticate-ack**: used by system to allow the access.
3. **Authenticate-nak**: used by system to deny the access.

2. CHAP (Challenge Handshake Authentication Protocol)
• It provides more security than PAP.
• In this method, password is kept secret, it is never sent on-line.
• It is a three-way handshaking 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.

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.