CHAPTER 12

Point-to-Point Access: PPP

Review Questions

1. PPP is designed for users who need a point-to-point connection.
2.
   a. Idle state: The link is not being used.
   b. Establishing state: Options are negotiated between the communicating parties.
   c. Authentication state: The identification of the user is verified.
   d. Networking state: Control and user data are exchanged.
   e. Terminating state: The link is disconnected.
3. Link Control Protocol, Password Authentication Protocol or Challenge Handshake Authentication Protocol, and Network Control Protocol.
4. The value of the protocol field defines the protocol stack.
5. The HDLC format of a U-frame is used for the control field in a PPP frame. The frame has no sequence numbers and there is no error or flow control.
6. The purpose of the LCP is establishing, maintaining, configuring, and terminating links between two communicating parties.
7. LCP packets are encapsulated in the payload field of a PPP frame, whose protocol field value is then set to $C021_{16}$ to indicate that it's carrying the LCP packet.
8.
   a. Configuration packets are used to negotiate options between the two ends.
   b. Link termination packets are used to disconnect the link.
   c. Link monitoring and debugging packets are used for checking the code and protocol of the frame, and for monitoring the link.
9. Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).
10. PAP is a simple procedure with two steps. First the user sends an authentication identification and password; then the system checks their validity and grants or denies connection. The main deficiency of this protocol is the lack of security.

11. CHAP is a three-way authentication protocol. The system sends the user a challenge packet with a challenge value. The user applies a predefined function to the challenge value and sends the result back to the system. The system checks the result by doing the same computations with the user's password and challenge value and grants or denies access depending on the result. CHAP is a more secure protocol than PAP.
12. CHAP and PAP packets are encapsulated in the payload field of the PPP frame The value of the protocol field of the PPP frame indicates that it's carrying the PAP (when set to $C023_{16}$) or CHAP packet (set to $C223_{16}$).
13. NCP is a set of protocols which allows the encapsulation of data coming from network layer protocols in the PPP frame.
14. IPCP is one of the NCP protocols consisting of a set of packets for establishing and terminating a network layer connection for PPP.

Multiple-Choice Questions

15. c
16. a
17. b
18. d
19. c
20. b
21. a
22. d
23. d
24. b
25. b
26. b
27. d
28. c

Exercises

29. flag = 7E; address = FF; control = C0
30. See Table 12.1.

Table 12.1 *Exercise 30*

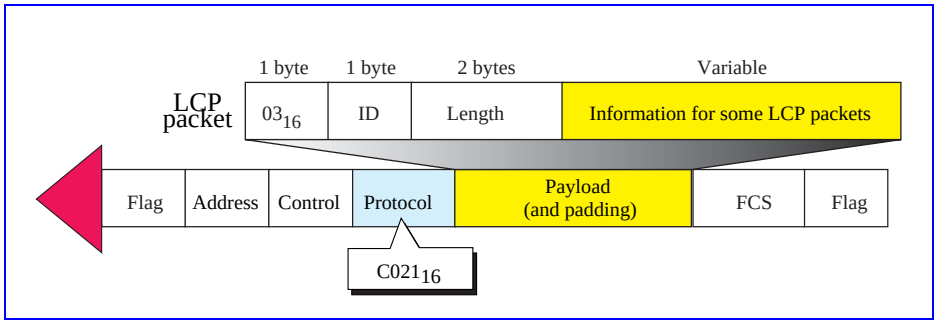
Field	*HDLC*	*PPP*
Flag	01111110	01111110
Address	Address of secondary station	11111111
Control	One or two bytes	11000000
Protocol	----------	One or two bytes

Table 12.1 *Exercise 30*

Field	*HDLC*	*PPP*
Information	Data and padding	Data and padding
FCS	Two or four bytes	Two or four bytes

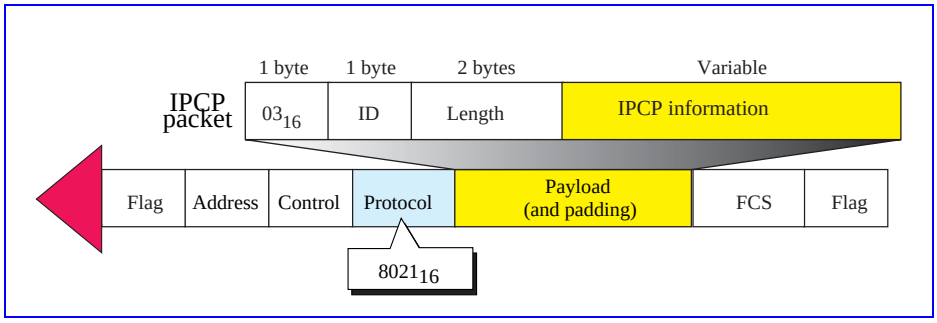
31. The protocol is the Link Control Protocol carrying a terminate-request packet.
32. The protocol is the Link Control Protocol carrying a echo-request packet. The ID of the packet is 11_{16} and the length is 0014_{16}, which means 20 bytes.
33. See Figure 12.1.

Figure 12.1 *Exercise 33*



34. See Figure 12.2.

Figure 12.2 *Exercise 34*



35. The protocol fields and the payload fields are different.
36. Echo request: 09 01 0009 48454C4C4F
    PPP frame: 7E FF C0 C021 09 01 0009 48454C4C4F (FCS) 7E
37. Echo reply: 0A 01 0009 48454C4C4F
    PPP frame: 7E FF C0 C021 0A 01 0009 48454C4C4F (FCS) 7E
38. Authenticate request: 01 01 0014 08 464F524F555A414E 06 373937393739
    PPP Frame:
    7E FF C0 C023 01 01 0014 08 464F524F555A414E 06 373937393739 (FCS) 7E

39. Authenticate ack: 02 01 0014 08 464F524F555A414E
PPP Frame: 7E FF C0 C023 02 01 0014 08 464F524F555A414E (FCS) 7E
40. Challenge: 01 01 0009 04 A4253616 (We used no challenge name)
PPP Frame: 7E FF C0 C223 01 01 0009 04 A4253616 (FCS) 7E
41. Response: 02 01 0009 04 6163524A (We used no response name)
PPP Frame: 7E FF C0 C223 02 01 0009 04 6163524A (FCS) 7E
42. 36364C3C
43. The negotiation was successful, connection is established, the next state is either authentication or networking.
44. The connection is in the establishing state; one of the sides should revise the options.
45. Networking state.
46.

7E FF C0 CO21 (Configure-request, LCP) (FCS) 7E
7E FF C0 C021 (Configure-ack, LCP) (FCS) 7E
7E FF C0 C023 (Authenticate-request, PAP) (FCS) 7E
7E FF C0 C023 (Authenticate-ack, PAP) (FCS) 7E
7E FF C0 8021 (Configure-request, IPCP) (FCS) 7E
7E FF C0 8021 (Configure-ack, IPCP) (FCS) 7E
7E FF C0 0021 (Data, IP) (FCS) 7E
...
7E FF C0 0021 (Data, IP) (FCS) 7E
7E FF C0 8021 (Terminate-request, IPCP) (FCS) 7E
7E FF C0 8021 (Terminate-ack, IPCP) (FCS) 7E
7E FF C0 C021 (Terminate-request, LCP) (FCS) 7E
7E FF C0 C021 (Terminate-ack, LCP) (FCS) 7E