



SNS COLLEGE OF ENGINEERING



Kurumbapalayam(Po), Coimbatore – 641 107

Accredited by NAAC-UGC with 'A' Grade

Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

Department of Information Technology

Course Name – 19IT401 Computer Networks

II Year / IV Semester

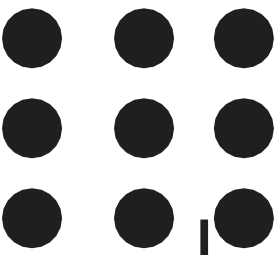
Unit 2 – Link Layer

Topic 3- PPP





PPP



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

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.

Authentication is also provided in the protocol, but it is optional. The new version of PPP, called Multilink PPP, provides connections over multiple links.

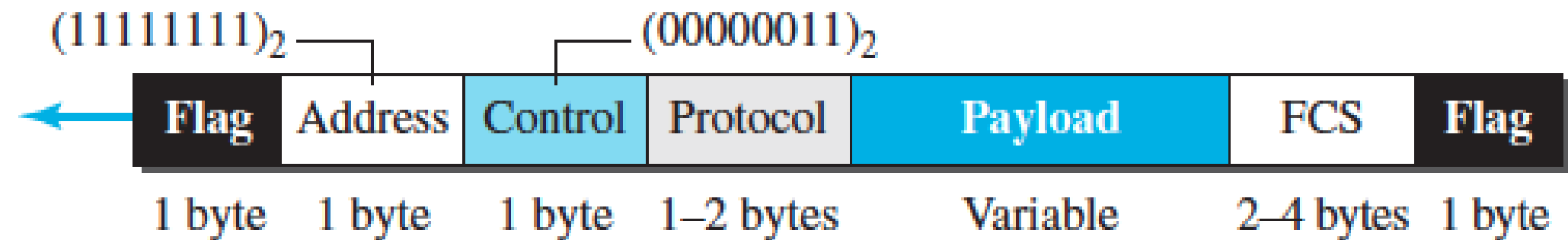
One interesting feature of PPP is that it provides network address configuration.

PPP

Framing

PPP uses a character-oriented (or byte-oriented) frame.

Frame Format



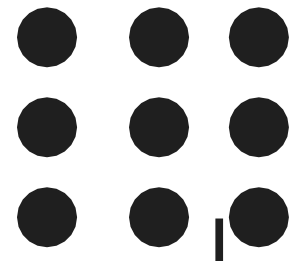
Address - The address field in this protocol is a constant value and set to 11111111 (broadcast address).

Control - This field is set to the constant value 00000011 (imitating unnumbered frames in HDLC).

Protocol - The protocol field defines what is being carried in the data field: either user data or other information.

Payload field - This field carries either the user data or other information. The data field is a sequence of bytes with the default of a maximum of 1500 bytes; but this can be changed during negotiation.

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



PPP

Multiplexing

Although 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).

Legend

LCP: Link control protocol
 AP: Authentication protocol
 NCP: Network control protocol

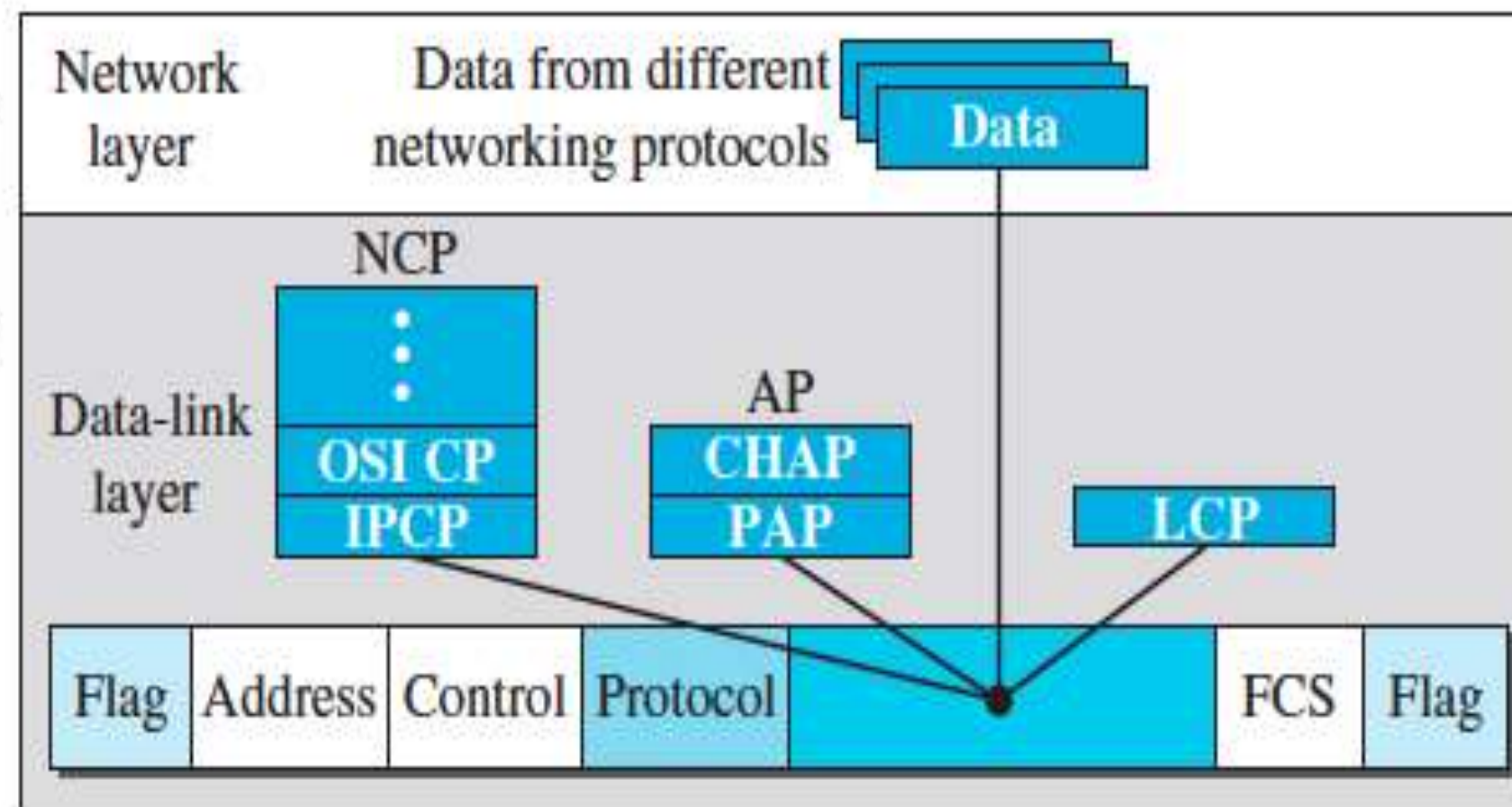
Protocol values:

LCP: 0xC021

AP: 0xC023 and 0xC223

NCP: 0x8021 and

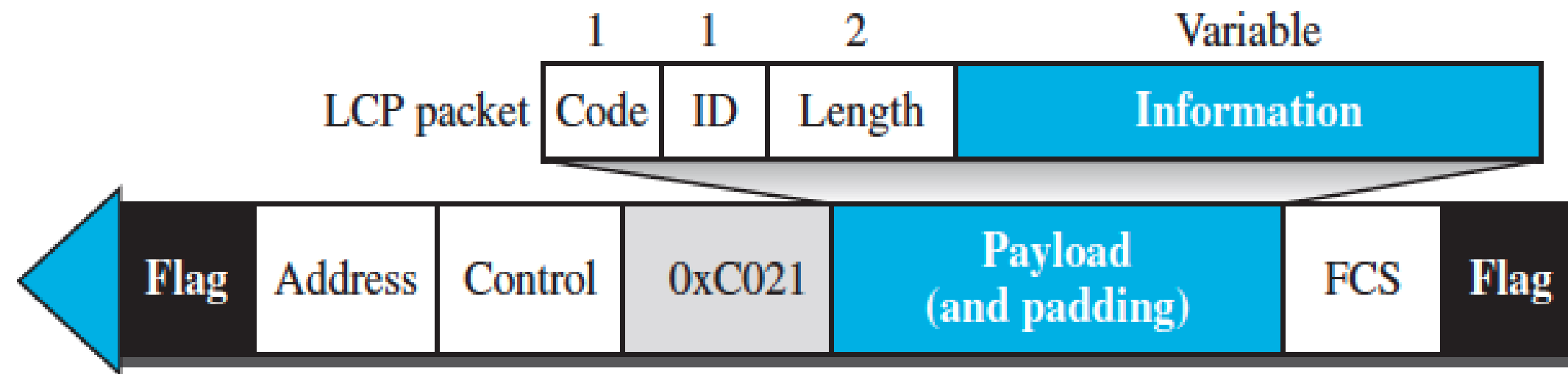
Data: 0x0021 and



PPP

Link Control Protocol

The Link Control Protocol (LCP) is responsible for establishing, maintaining, configuring, and terminating links.



The code field defines the type of LCP packet. There are 11 types of 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.



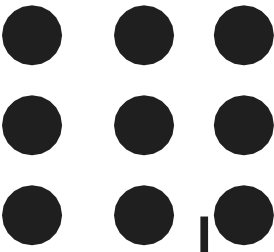
PPP

Link Control Protocol.

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



PPP



Authentication Protocols

Authentication plays a very important role in PPP because PPP is designed for use over dial-up links where verification of user identity is necessary.

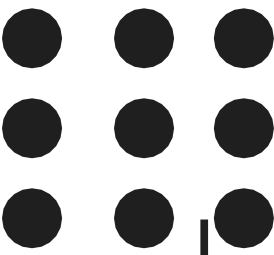
Authentication means validating the identity of a user who needs to access a set of resources.

PPP has created two protocols for authentication:

- Password Authentication Protocol and
- Challenge Handshake Authentication Protocol.



PPP



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.

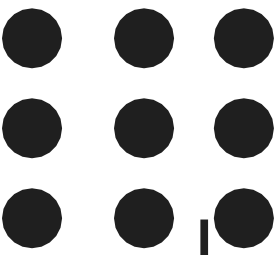
When a PPP frame is carrying any PAP packets, the value of the protocol field is 0xC023.

The three PAP packets are

- authenticate-request - used by the user to send the user name and password
- authenticate-ack - used by the system to allow access
- authenticate-nak - used by the system to deny access



PPP



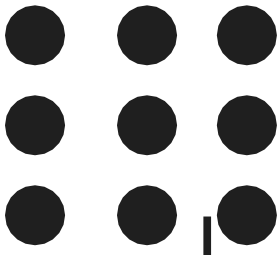
CHAP

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.



PPP



Network Control Protocols

PPP is a multiple-network-layer protocol.

IPCP

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



THANK YOU