HDLC and PPP

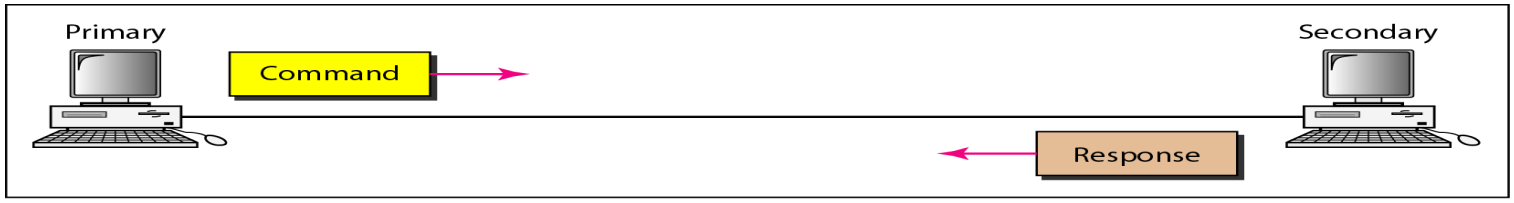
High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point-to-point and multipoint links. It implements the ARQ mechanisms.

HDLC

Configuration and Transfer Modes

- HDLC provides two common transfer modes:
  - Normal Response Mode
  - Asynchronous Balanced Mode

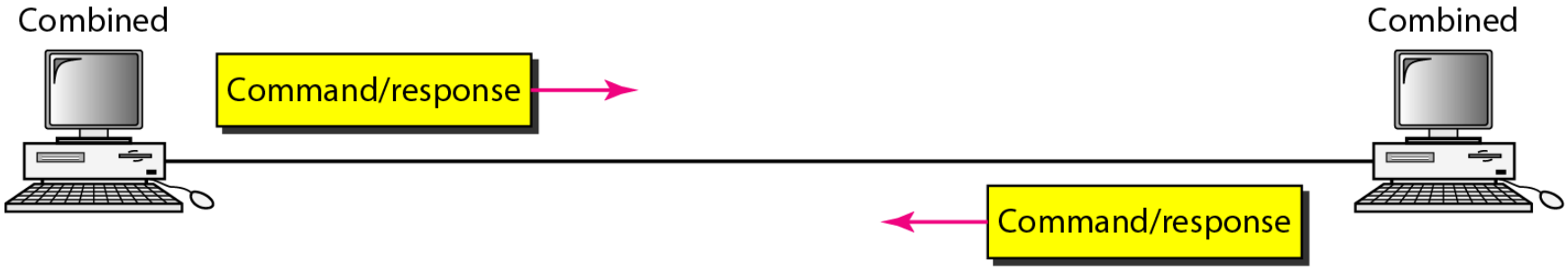
- Normal Response Mode
  - We have one **primary station** and multiple **secondary stations**.
  - Primary station can send commands and a secondary station can only respond.
  - NRM is used for both point-to-point and multipoint links.



a. Point-to-point

b. Multipoint

Asynchronous Balanced Mode (ABM)

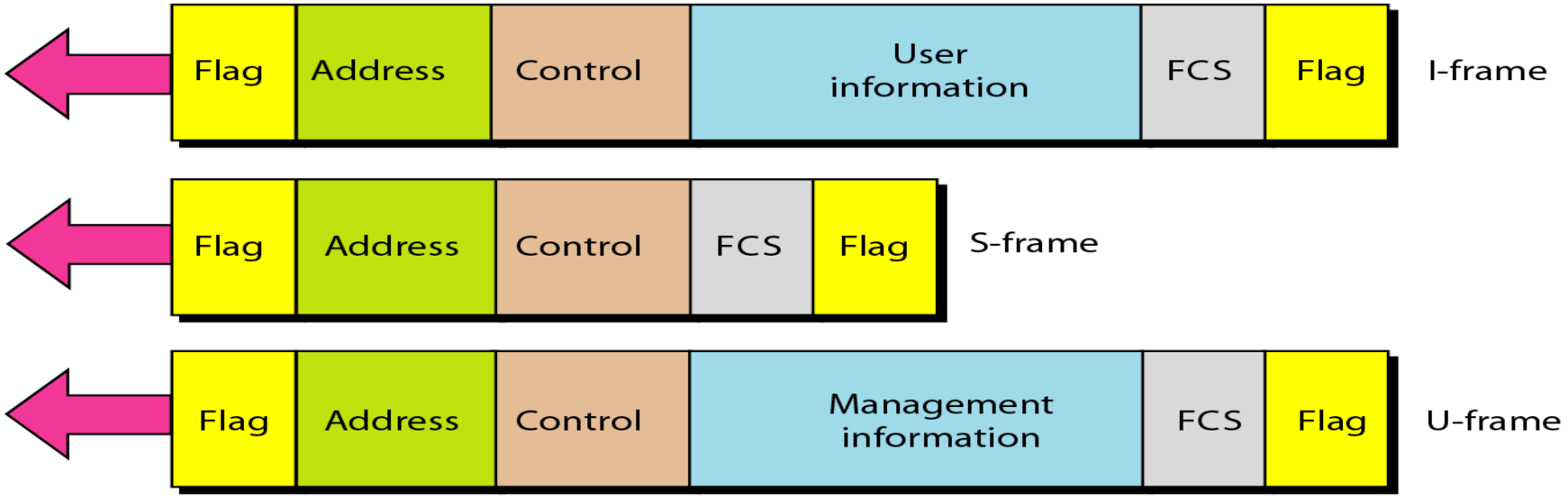


- Asynchronous Balanced Mode (ABM)
  - Configuration is balanced.
  - The link is point-to-point
  - Each station can function as primary and secondary.

HDLC Frames

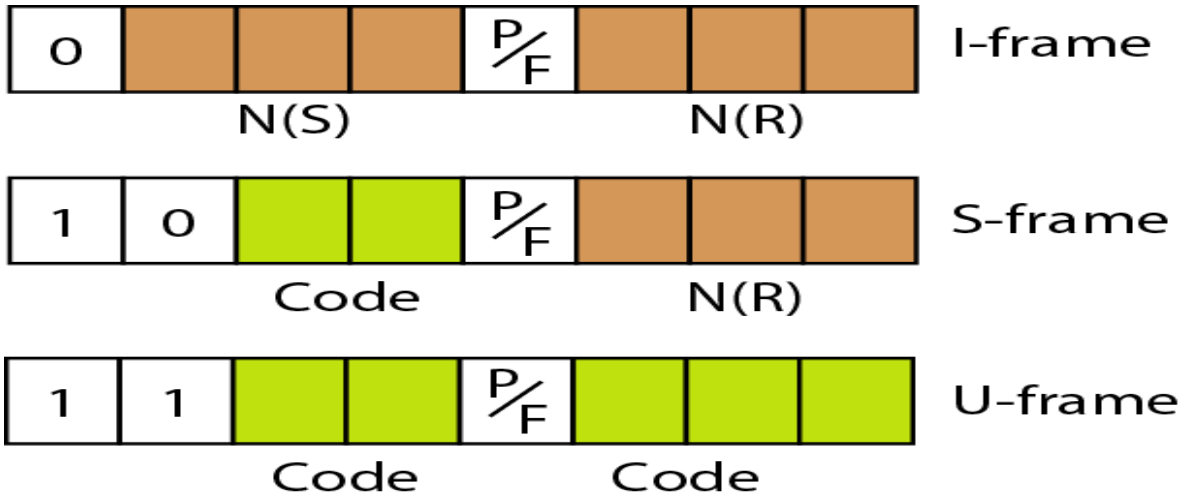
- HDLC defines three types of frames:
  - Information frames (I-frames): to transport user data and control information relating to user data (piggybacking).
  - Supervisory frames (S-frames): to transport control information
  - Unnumbered frames (U-frames): reserved for system management.
- In multiple frame transmission, the ending flag of one frame can serve as the beginning flag of the next frame.

HDLC frames



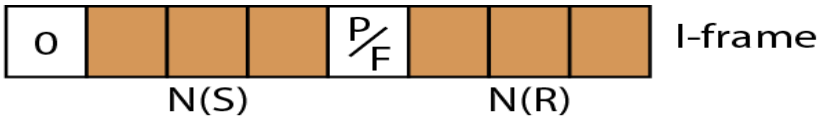
- Flag: 01111110
- Address: address of the secondary station.
- Control: flow or error control. 1- or 2- byte segment.
- Information: user's data from the netwrk layer or management information.
- FCS: Frame check sequence (FCS) in the HDLC error detection field.

Control field format for the different frame types



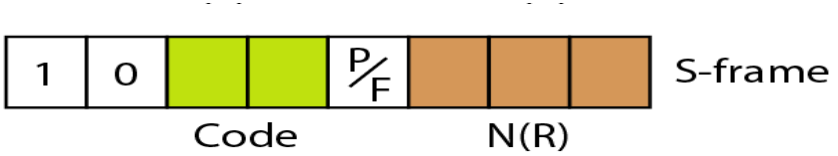
- Determines the type of the frame and defines its functionality.

Control field for I-frame



- **I-frames** are used to carry user data from the network layer. In addition they include flow and error control information
- The first bit (**0**) indicates an I-frame
- The next 3 bits **N(S)**, defines the sequence number of the frame.
- The last 3 bits **N(R)**, corresponds to the acknowledgement number when piggybacking is used.
- Poll or Final **(P/F) bit**: Poll means the frame is sent by a primary station to a secondary station. Final is the opposite.

Control field for S-frame



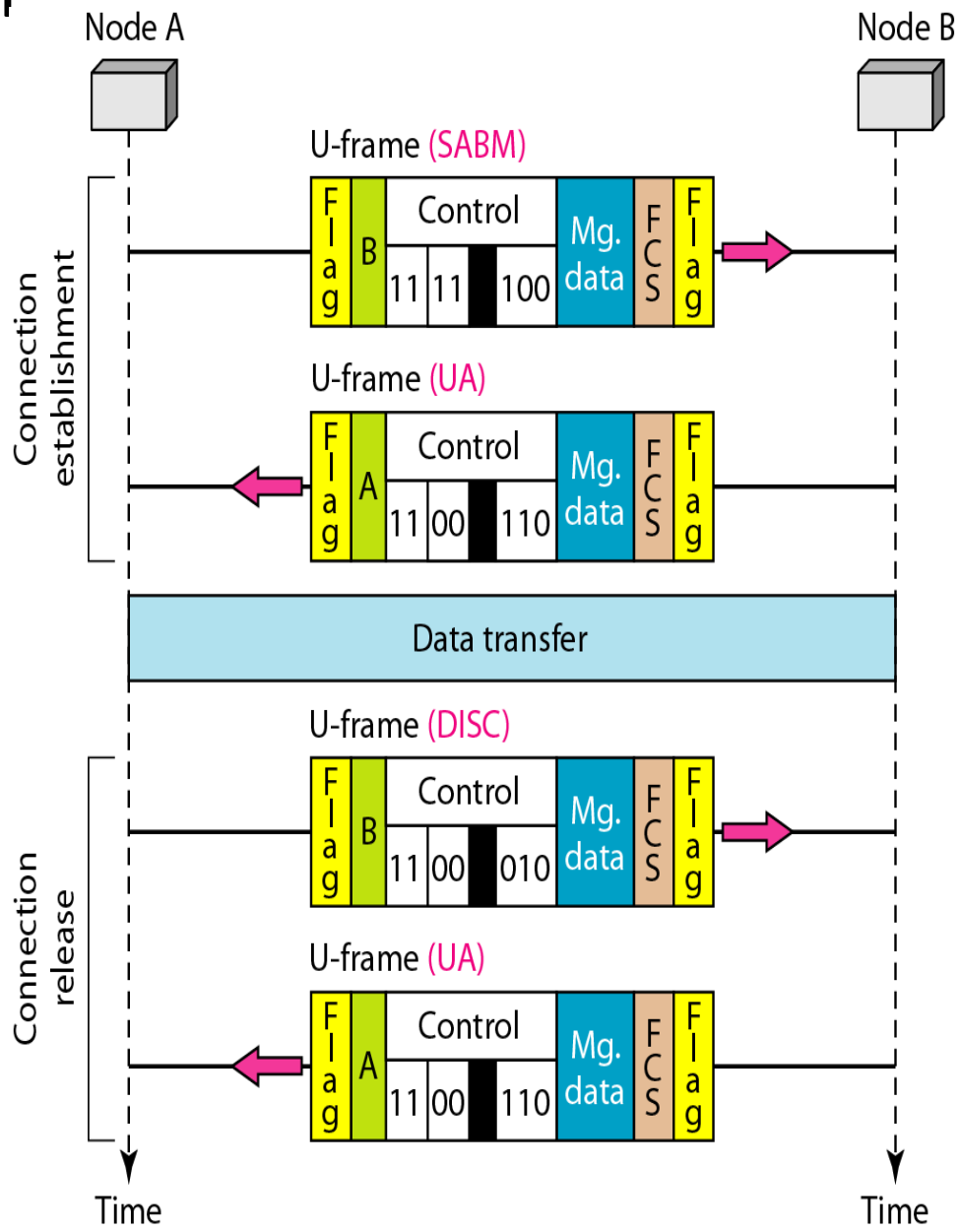
- **Supervisory frames (S-frames):** are used for flow and error control whenever piggybacking is either impossible or inappropriate.
- S-frames do not have information field.
- First two bits of the control field **10** indicate S-frame.
- N(R) corresponds to ACK/NAK numbers depending on the type of S-frame.
- Code defines the type of S-frame.
  - Receive Ready (RR): **(Code: 00)**, It ACKs the receipt of a frame or a group of frames. N(R) defines the ACK number.
  - Receive not ready (RNR): **(Code 10)**, It ACKs the receipt of a frame or a group of frames and it announces that the receiver is now busy and cannot accept more frames.
  - Reject (REJ): **(Code 01)**, This is a NAK frame that can be used in Go-Back-N ARQ.
  - Selective reject (SREJ): **(Code 11)**, This is a NAK frame used in Selective Repeat ARQ.

U-frame control command and response

Code	*Command*	*Response*	*Meaning*
00 001	SNRM		Set normal response mode
11 011	SNRME		Set normal response mode, extended
11 100	SABM	**DM**	Set asynchronous balanced mode or **disconnect mode**
11 110	SABME		Set asynchronous balanced mode, extended
00 000	UI	**UI**	Unnumbered information
00 110		**UA**	**Unnumbered acknowledgment**
00 010	DISC	**RD**	Disconnect or **request disconnect**
10 000	SIM	**RIM**	Set initialization mode or **request information mode**
00 100	UP		Unnumbered poll
11 001	RSET		Reset
11 101	XID	**XID**	Exchange ID
10 001	FRMR	**FRMR**	Frame reject

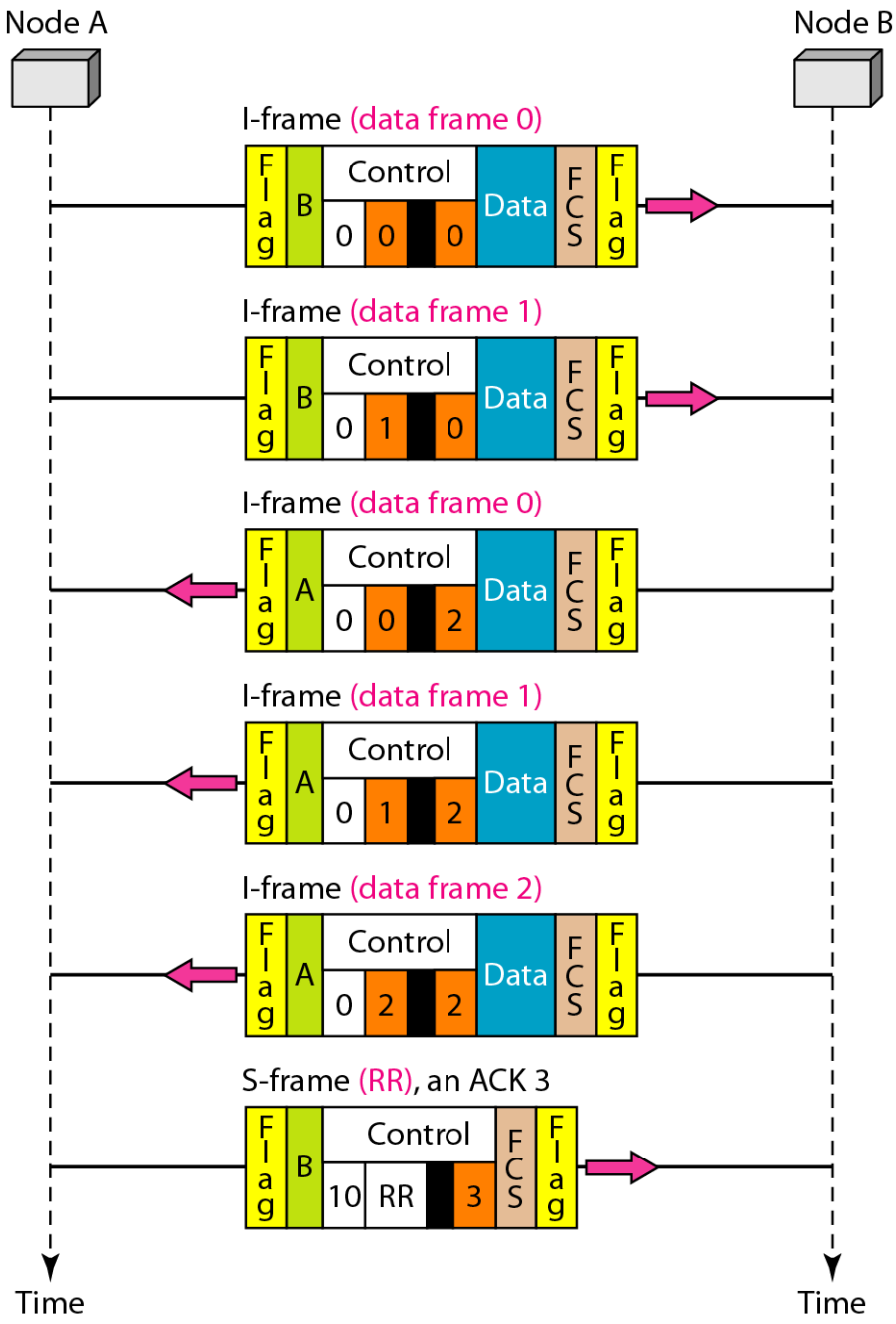
Example of connection and disconnection

- U-frames can be used for connection establishment and connection release. Node A asks for a connection with a set asynchronous balanced mode (SABM) frame; node B gives a positive response with an unnumbered acknowledgment (UA) frame.
- After these two exchanges, data can be transferred between the two nodes.
- After data transfer, node A sends a DISC (disconnect) frame to release the connection; it is confirmed by node B responding with a UA (unnumbered acknowledgment).



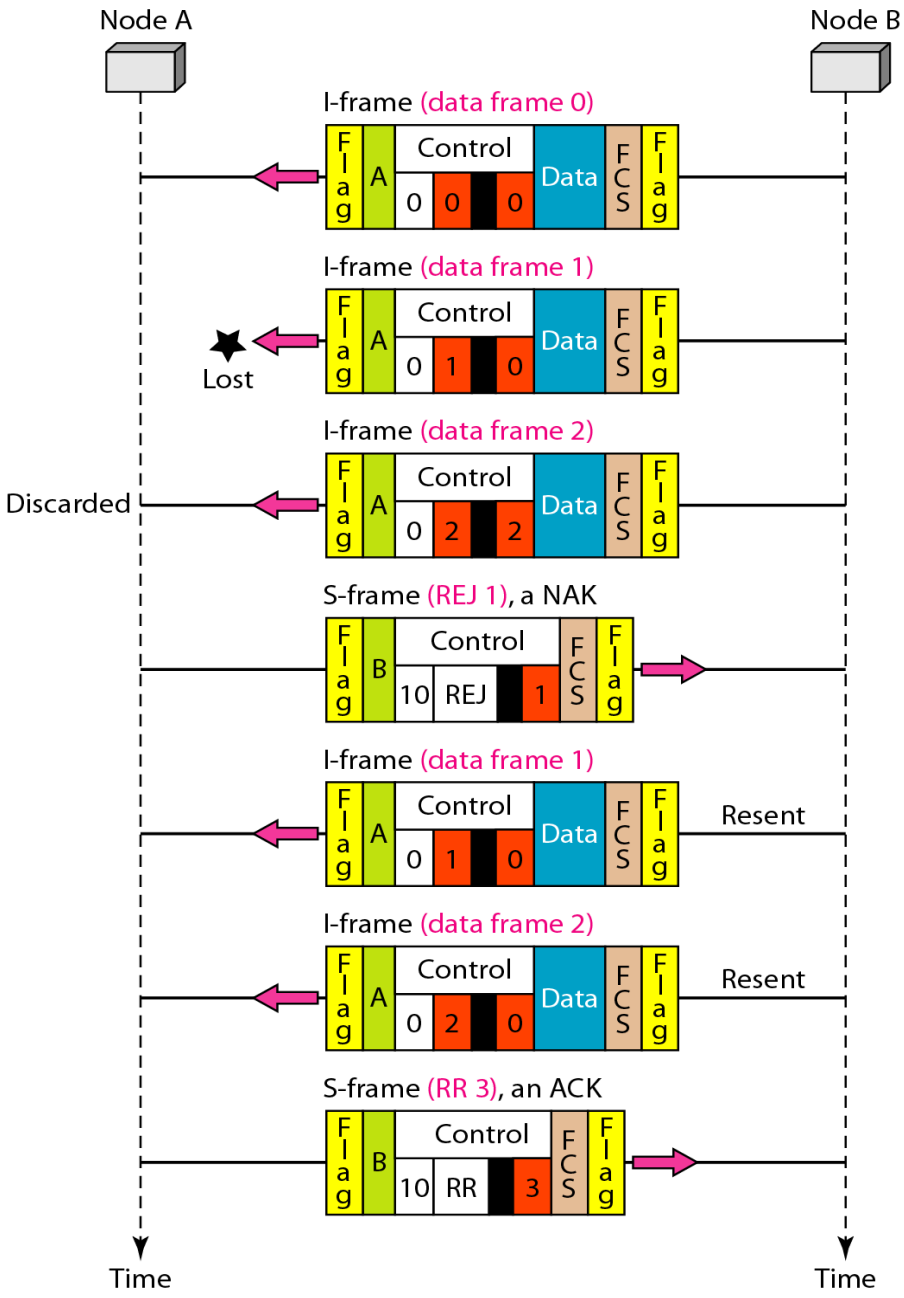
Example of piggybacking without error

- Node A begins with an I-frame numbered 0 followed by another I-frame numbered 1.
- Node B piggybacks its acknowledgment of both frames onto an I-frame numbered 0 [N(S) field] and 2 in its N(R) field, acknowledging the receipt of A's frames 1 and 0 and indicating that it expects frame 2 to arrive next. It also transmits two I-frames (numbered 1 and 2) before accepting further frames from node A.
- Node A has sent all its data. Therefore, it sends an S-frame instead. The RR code indicates that A is still ready to receive. The number 3 in the N(R) field tells B that frames 0, 1, and 2 have all been accepted and that A is now expecting frame number 3.



Example of piggybacking with error

- Node B sends three data frames (0, 1, and 2), but frame 1 is lost.
- When node A receives frame 2, it discards it and sends a REJ frame for frame 1. Note that the protocol being used is Go-Back-N with the special use of an REJ frame as a NAK frame. The NAK frame does two things here: It confirms the receipt of frame 0 and declares that frame 1 and any following frames must be resent.
- Node B, after receiving the REJ frame, resends frames 1 and 2. Node A acknowledges the receipt by sending an RR frame (ACK) with acknowledgment number 3.



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

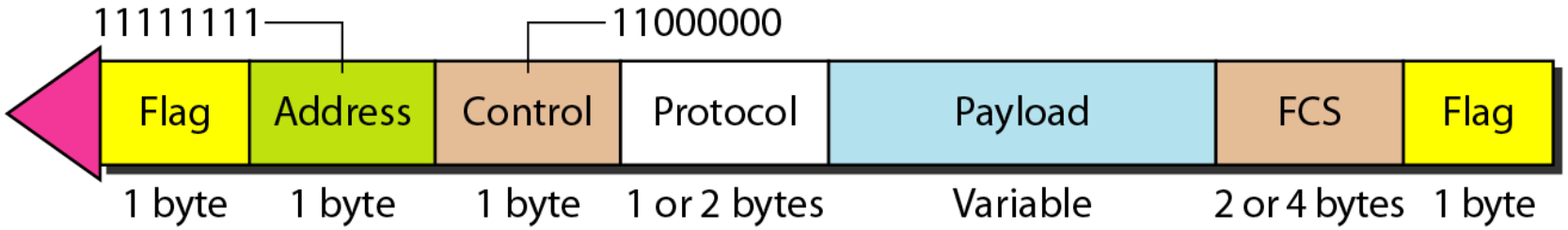
POINT-TO-POINT PROTOCOL

POINT-TO-POINT PROTOCOL

- PPP provides several services:
  - Defines frame format to be exchanged between devices
  - Defines how two devices can negotiate the establishment of link and the exchange of data.
  - Defines how network layer data are encapsulated in the data link layer.
  - Defines how two devices can authenticate each other.
  - Provides multiple network layer services
  - Provides network address configuration, which is useful when a home user needs a temporary address to connect to the internet.

- However, several functions are missing in PPP
  - PPP does not provide flow control
  - PPP has very simple mechanism for error control. A CRC field is used to detect errors. If a frame is corrupted, it is silently discarded; the upper layer needs to take care of the problem. Lack of error control and sequence number can cause packets to be received out of order.

PPP frame format



- Flag: 1 byte flag with bit pattern 01111110.
- Address: Since PPP is used for point to point connection, it uses the broadcast address, 11111111.
- Control: uses the format of U-frame in HDLC. The value 11000000 shows that the frame does not contain any sequence numbers and there is no flow or error control.
- Protocol: defines what is being carried in the payload, i.e., user data or other information.
- Payload: user data or other information. The data field is a sequence of bytes with a default of a max of 1500 bytes, but it can change during negotiation. Padding is needed of the size is less than the max default value or the maximum negotiated value.
- Frame Check Sequence (FRC): 2~4 byte CRC.

Byte stuffing

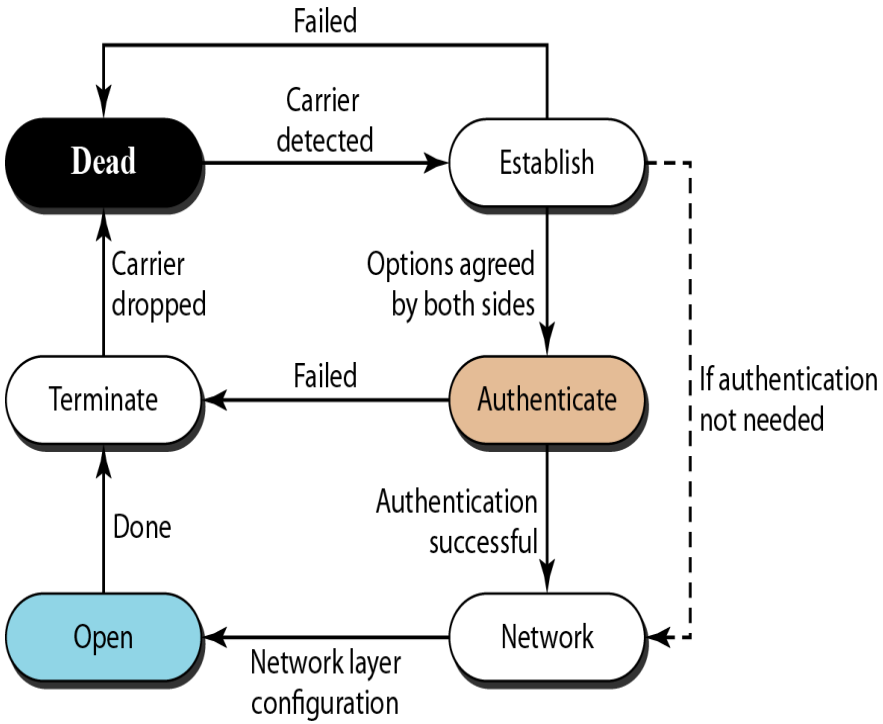
- The flag in PPP is a byte and needs to be escaped whenever it appears in the data section of the frame.

- The escape byte is 01111101

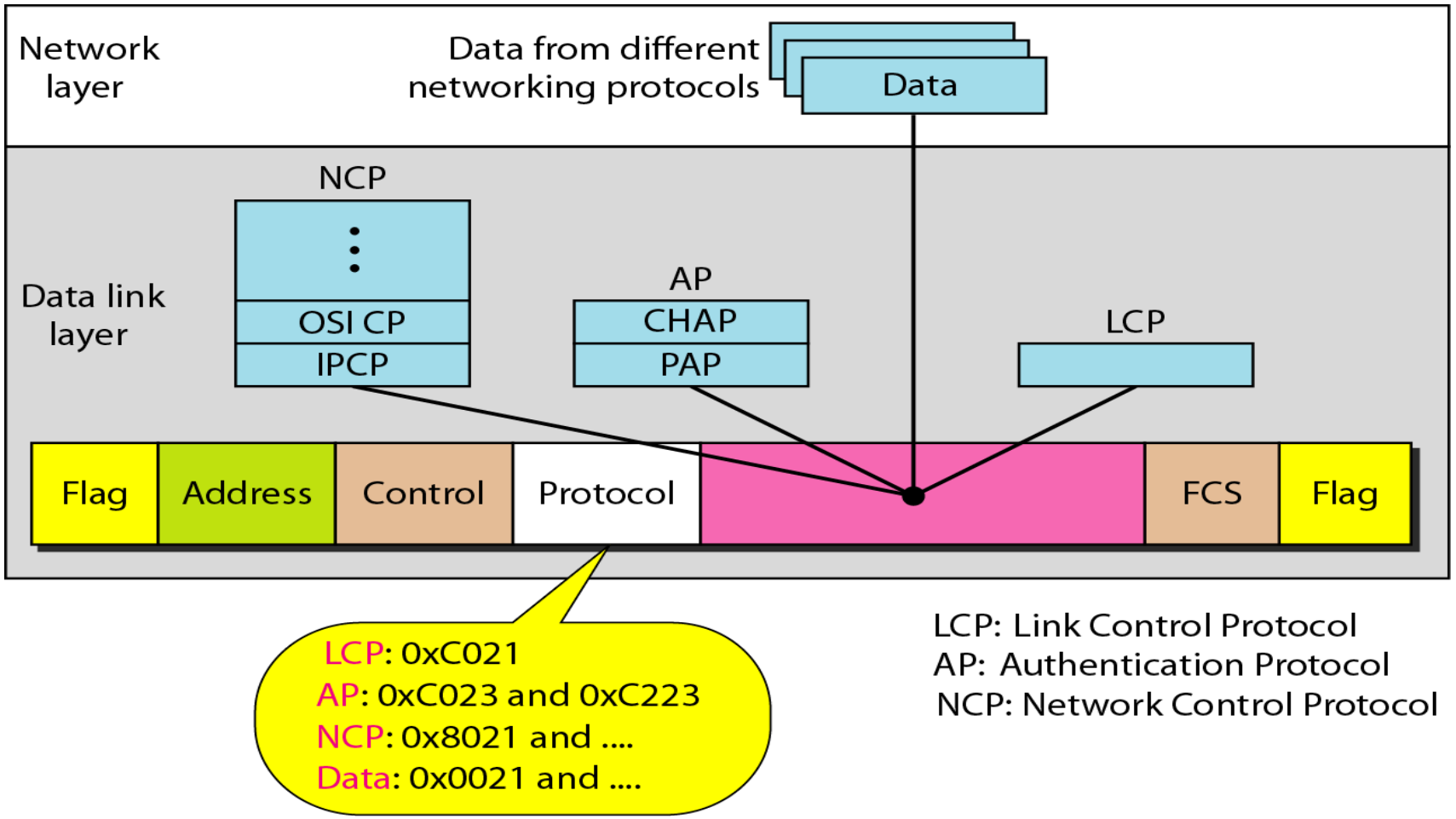
Transition phases

PPP connection goes through phases.

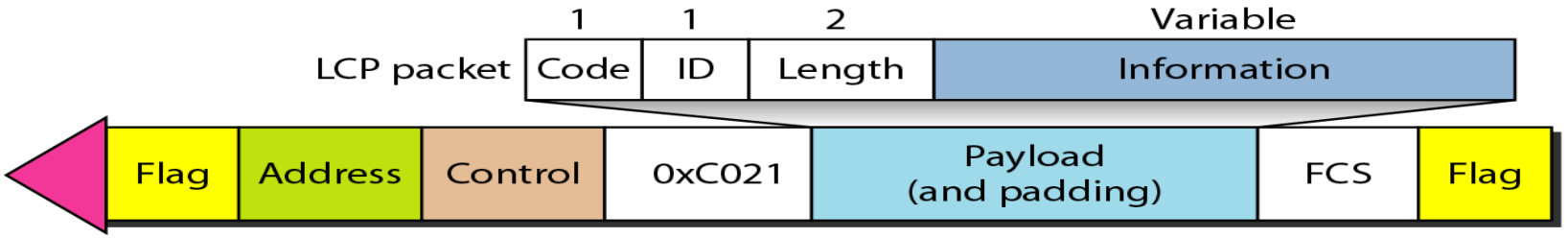
- Dead: the link is not used. No active carrier at the physical layer.
- Establish: When one of the nodes starts communication. Options are negotiated between two parties. If successful, the system goes through authentication phase (if required) or directly to networking phase. LCP packets are used in this phase.
- Authentication: This is optional. During establishment phase, nodes can decide, if they need authentication.
- Network: PPP supports multiple network layer protocols at the network layer. In this phase, negotiation for the network layer protocols take place.
- Open: data transfer takes place.
- Terminate: connection is terminated.



PPP


Network layer
Data from different networking protocols
Data
NCP
Data link layer
OSI CP
IPCP
AP
CHAP
PAP
LCP
Flag
Address
Control
Protocol
FCS
Flag
LCP: 0xC021
AP: 0xC023 and 0xC223
NCP: 0x8021 and ....
Data: 0x0021 and ....
LCP: Link Control Protocol
AP: Authentication Protocol
NCP: Network Control Protocol

Link Control Protocol (LCP) packet encapsulated in a frame



- The LCP is responsible for establishing, maintaining, configuring and terminating links.
- LCP packets are carried in the payload of a PPP frame with protocol field set as **0xC021**
- It provide negotiations to set options between two endpoints, before the link is established.
- FCP Packet
  - Code: defines the type of the packet.
  - ID: holds a value that matches a request with a reply. One endpoint inserts a value in this field with is copied in the reply packets.
  - Length: length of entire LCP packet.
  - Information: contains information such as options.

LCP packets

Used for link configuration during establish phase

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

Used for link termination during termination phase

Used for link monitoring and debugging

Common options

- Options are inserted in the information field of the configuration packets.
- The information field is divided into three fields: option type, option length, and option data.

Option	*Default*
Maximum receive unit (payload field size)	1500
Authentication protocol	None
Protocol field compression	Off
Address and control field compression	Off

Authentication Protocol

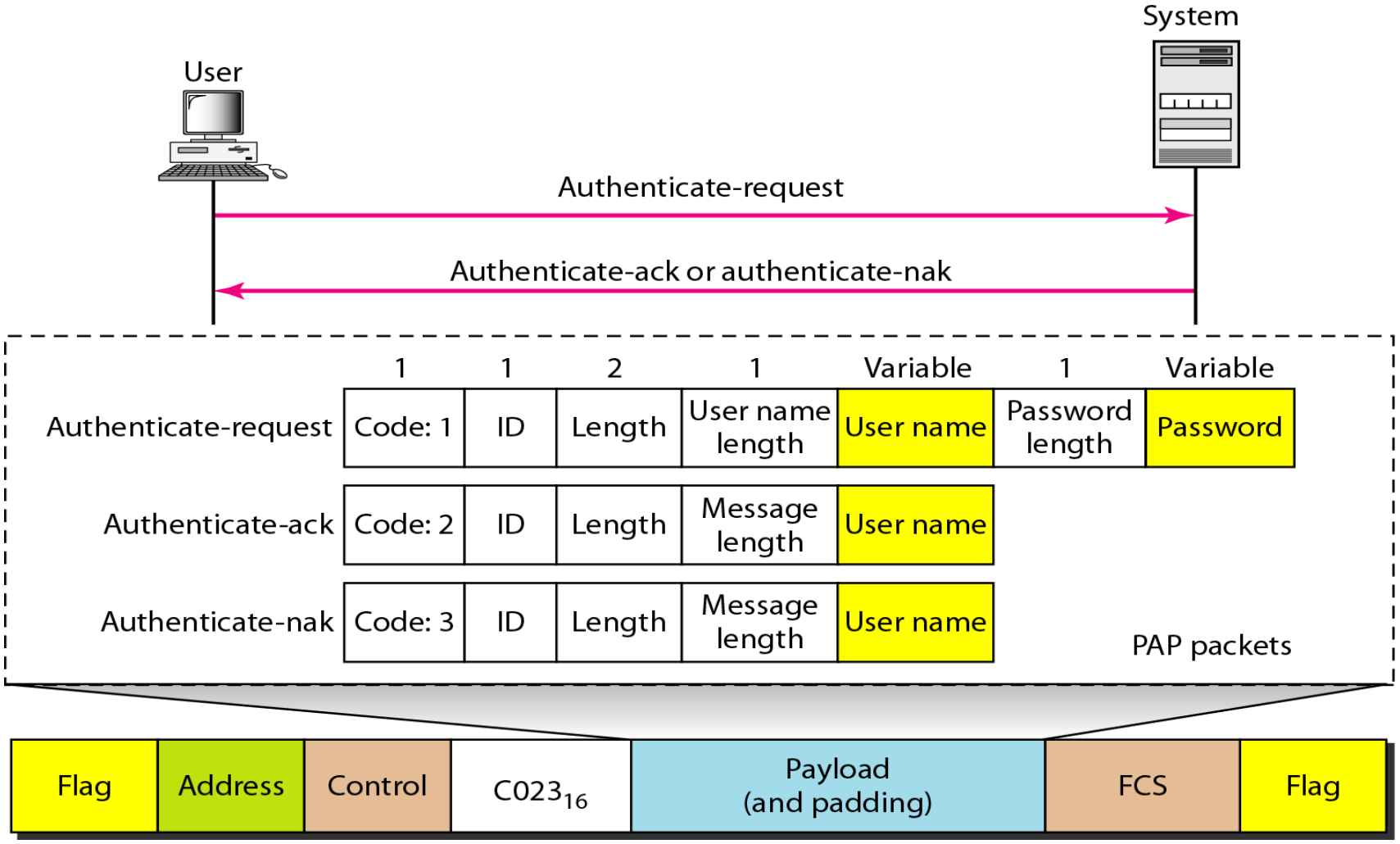
- Authentication means validating the identity of the user.
- PPP created two protocols for authentication:
  - Password Authentication Protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)

Password Authentication Protocol (PAP)

- Two steps:
  - The user willing to access the system sends an authentication identification and password.
  - The system checks the validity and can either accept or reject.

- When a PPP frame is carrying PAP packets, the value of the protocol field is 0xC023.
- Three PAP packets are:
  - Authentication-request
  - Authentication-ack
  - Authentication-nak

PAP packets encapsulated in a PPP frame

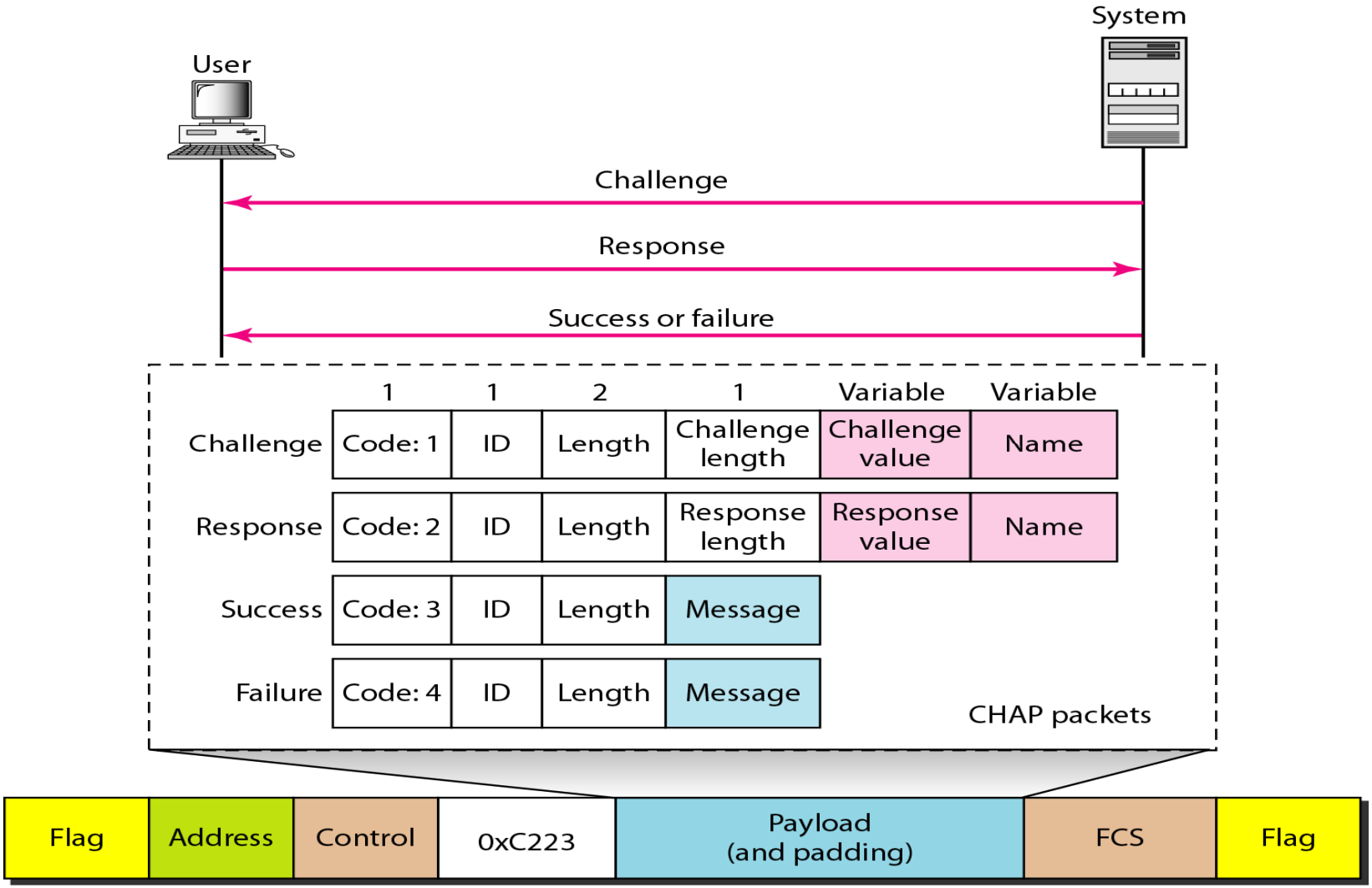


Challenge Handshake Authentication Protocol (CHAP)

- Three way hand-shake authentication protocol providing greater security than PAP.
  - The system sends the user a challenge packet containing a challenge value, usually a few bytes.
  - The user applies a predefined function that takes the challenge value and the user's own password and creates a result. User sends the result in the response packet to the system.
  - The system does the same. It applies the same function to the password and the challenge value to create a result. If the two results match, access is granted; otherwise, its denied.

- The password is kept secret, it is never sent online.

CHAP packets encapsulated in a PPP frame



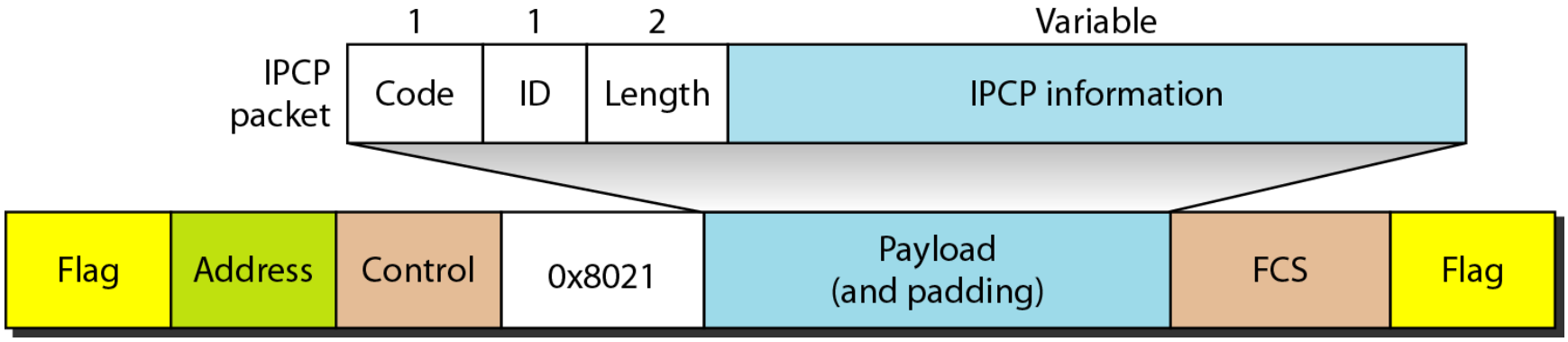
Network Control Protocols

- PPP is a multiple network layer protocol. It can carry network layer data packets from protocols defined by the Internet, Xerox, AppleTalk, Novel, and so on.

- PPP has defined specific NCP for each network protocol.
  - IPCP (Internet Protocol Control Protocol) configures the link for carrying IP packets.
  - Xerox CP does the same for Xerox protocol.

- Note: NCP packets do not carry network layer data; they just configure the link at the network layer for incoming data.

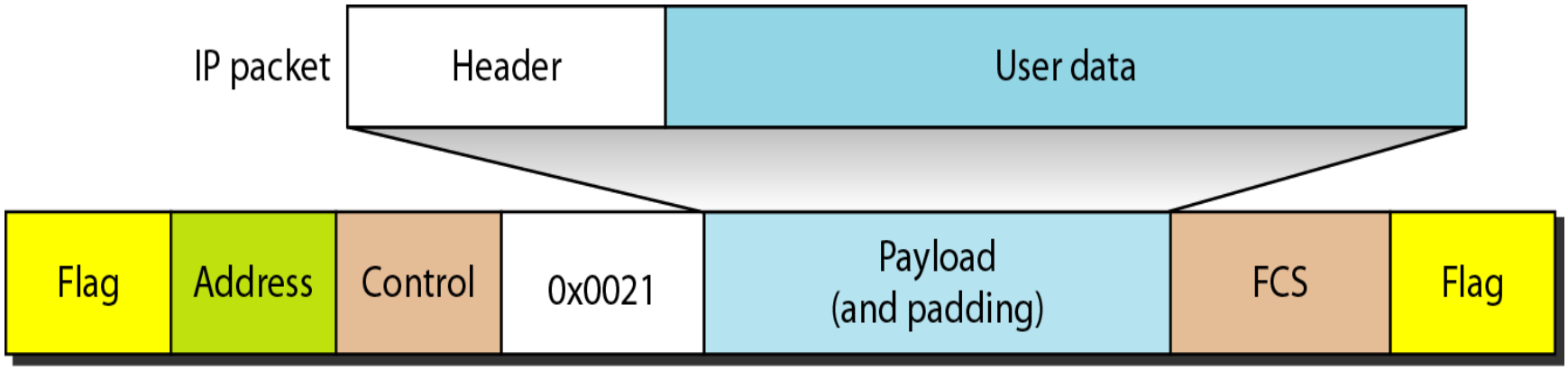
IPCP packet encapsulated in PPP frame



- IPCP (Internet Protocol Control Protocol) configures the link for carrying IP packets.
- The protocol field is 0x8021

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

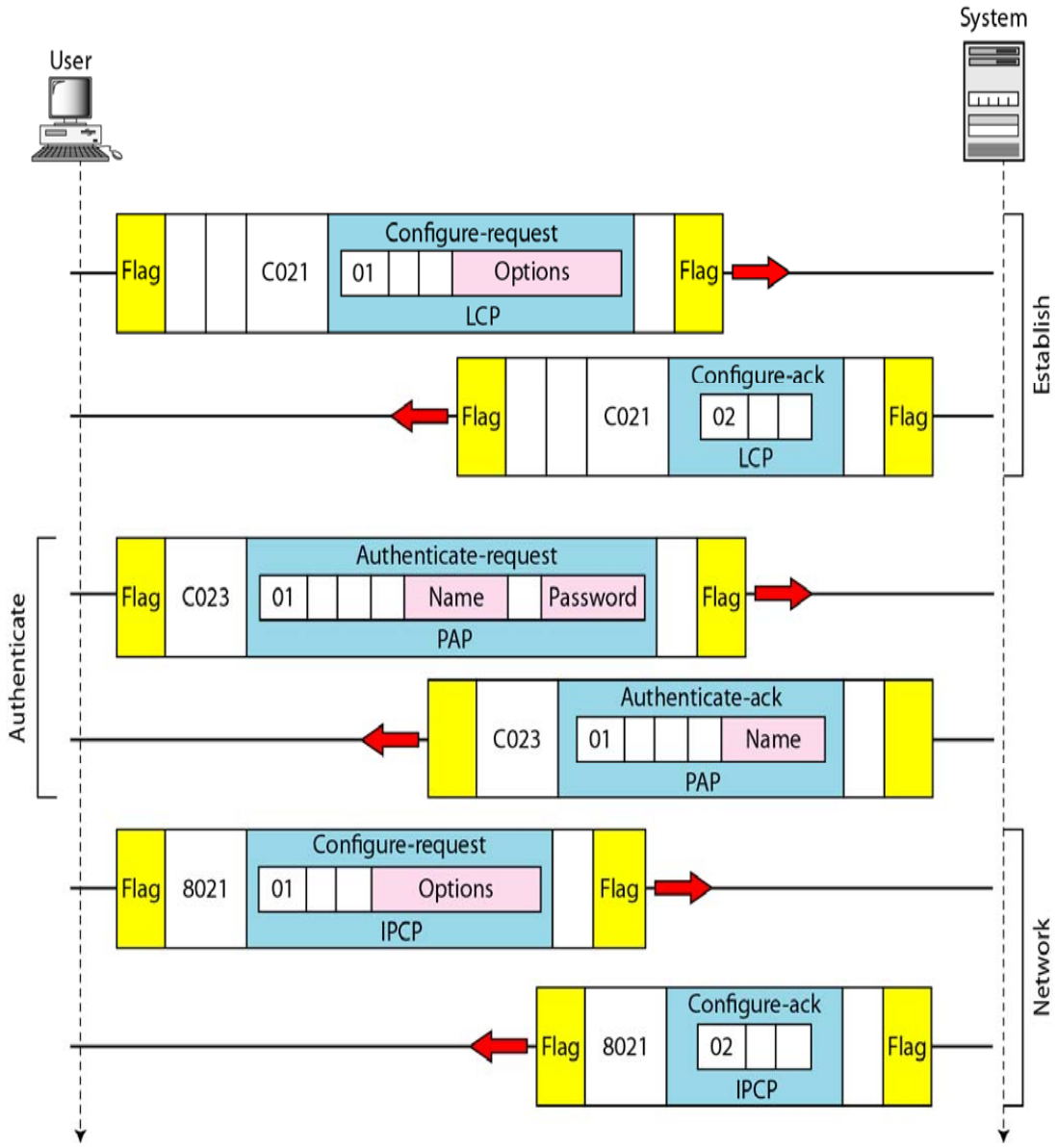
IP datagram encapsulated in a PPP frame



- After the network layer configuration is complete by one of the NCP protocols, the users can exchange data packets from the network layer.
- Different protocol fields are used for different network layers.
  - 0021 if PPP is carrying data from IP network layer.

PPP Example

- For simplicity, assume an unidirectional movement of data from the user site to the system site
- The first two frames show link establishment. We have chosen two options (not shown in the figure): using PAP for authentication and suppressing the address control fields.
- Frames 3 and 4 are for authentication.
- Frames 5 and 6 establish the network layer connection using IPCP.



PPP Example

- The next several frames show that some IP packets are encapsulated in the PPP frame. The system (receiver) may have been running several network layer protocols, but it knows that the incoming data must be delivered to the IP protocol because the NCP protocol used before the data transfer was IPCP.

- After data transfer, the user then terminates the data link connection, which is acknowledged by the system.