DLC SERVICES

Unit- 2

DLC SERVICES

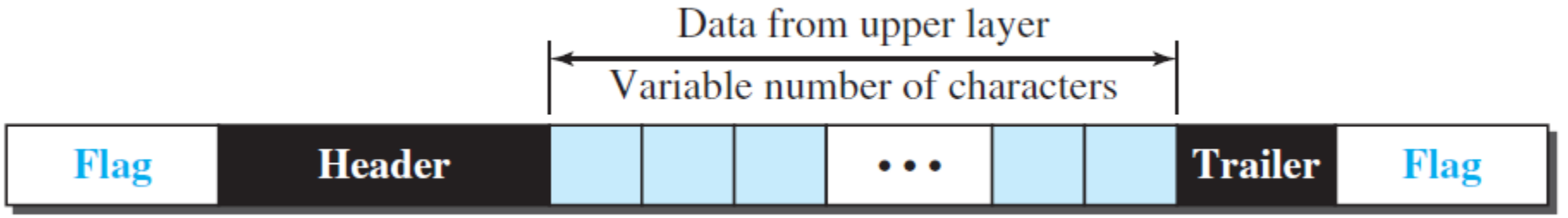
- Data link control functions include framing and flow and error control.

Framing

- Physical layer : bit synchronization to ensure that the sender and receiver use the same bit durations and timing
- Frames can be of fixed or variable size.
- Fixed-size framing: no need for defining the boundaries of the frames; the size itself can be used as a delimiter eg: atm wan
- Variable-size framing: need to define the end of one frame and the beginning of the next.
- Two approaches : a character-oriented approach and a bit-oriented approach.

Character-Oriented Framing (byte-oriented)

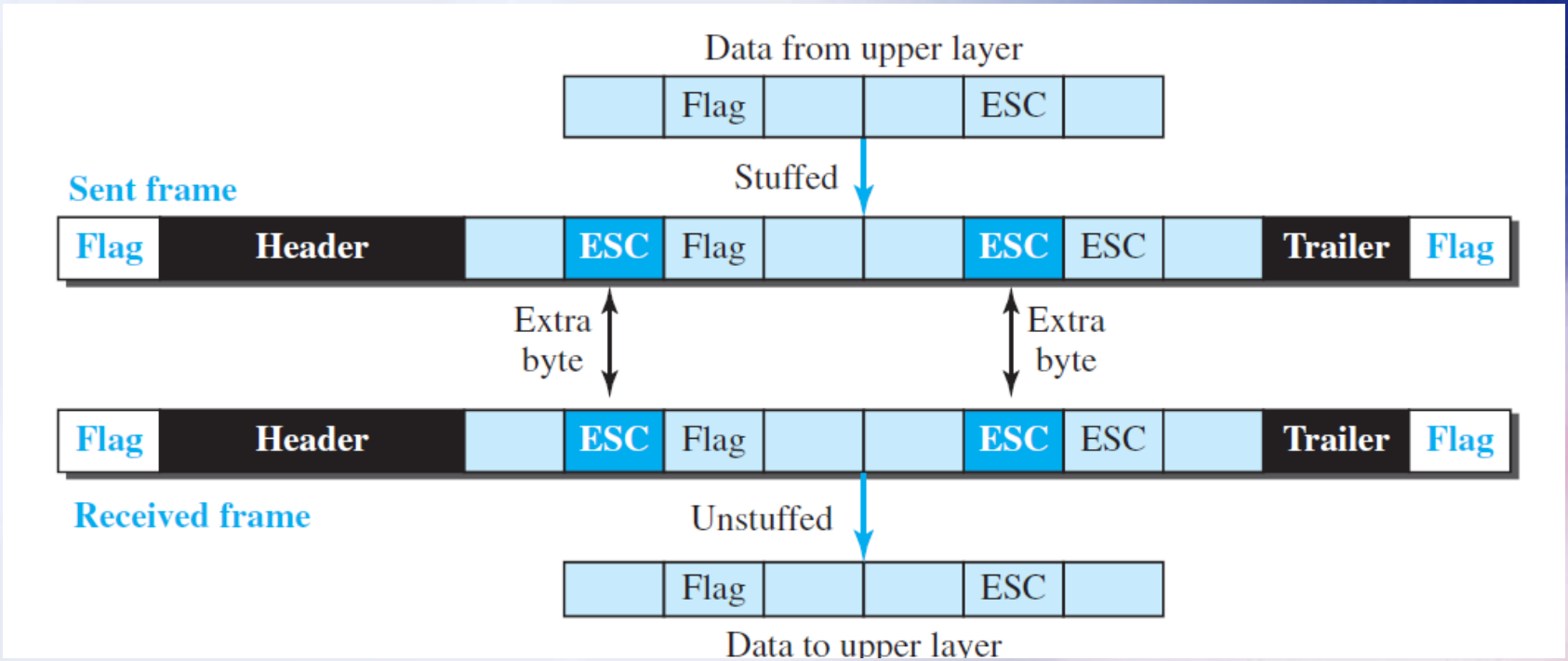
- Data to be carried are 8-bit characters from a coding system such as ASCII.
- The header has source and destination addresses and other control information, and trailer, has error detection redundant bits, are also multiples of 8 bits.
- To separate one frame from the next, an 8-bit (1-byte) flag is added at the beginning and the end of a frame.
- The flag, composed of protocol-dependent special characters, signals the start or end of a frame



Character-Oriented Framing

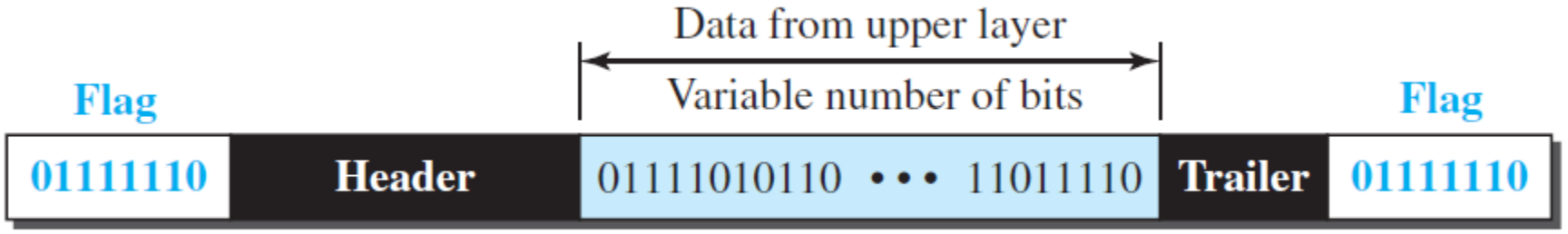
- When any character used for the flag could also be part of the information.
- To fix this, a byte-stuffing strategy is used
- Byte stuffing (or character stuffing): a special byte is added to the data section of the frame when there is a character with the same pattern as the flag.
- The data section is stuffed with an extra byte. This byte is usually called the escape character (ESC) and has a predefined bit pattern.
- Receiver removes the esc character, and treats the next character as data, not as a delimiting flag.

Byte stuffing (Character stuffing)



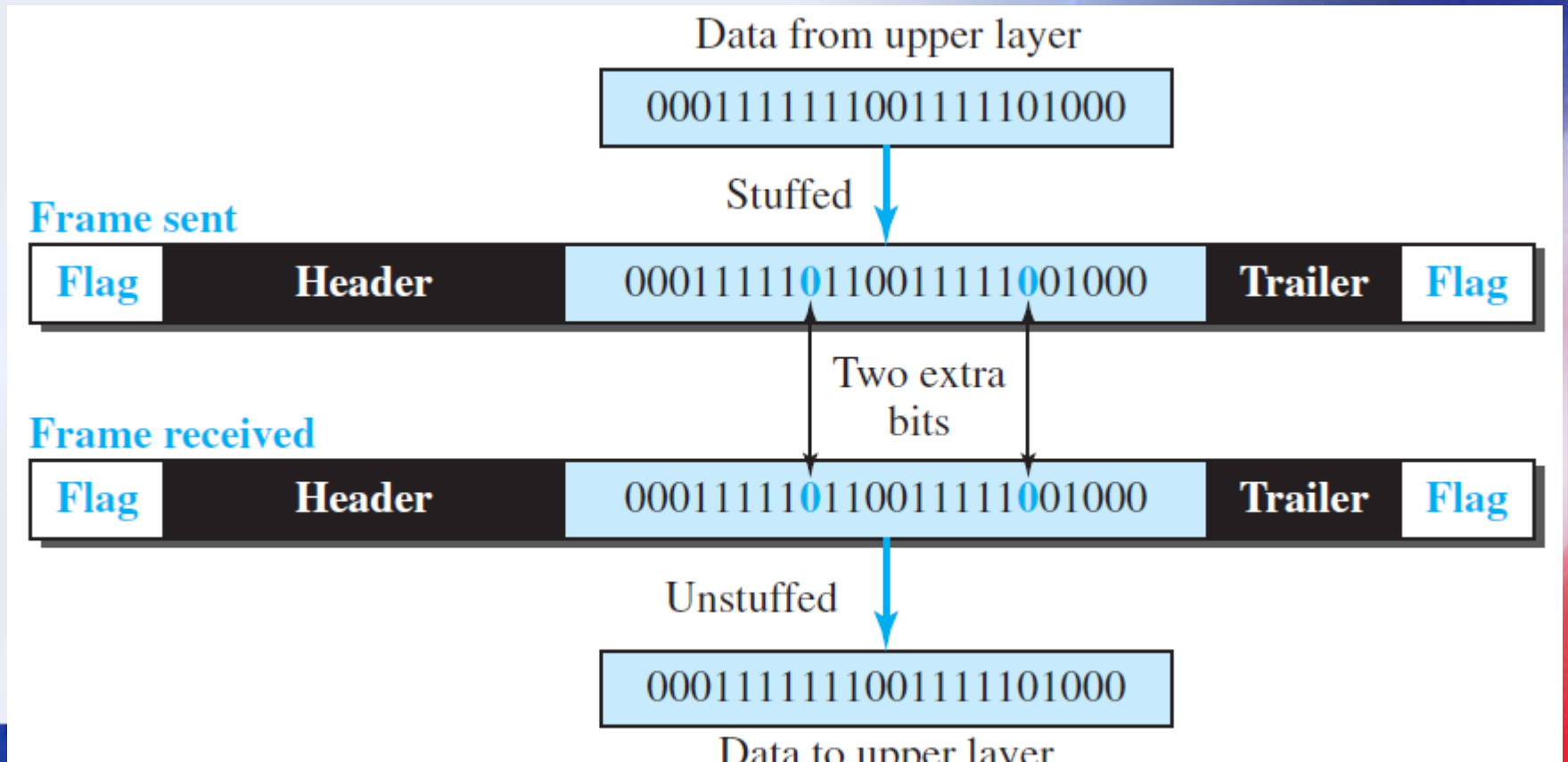
Bit-Oriented Framing

- The data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video, and so on.
- In addition to headers (and possible trailers), we need a delimiter to separate one frame from the other.
- Most protocols use a special 8-bit pattern flag, 01111110, as the delimiter to define the beginning and the end of the frame

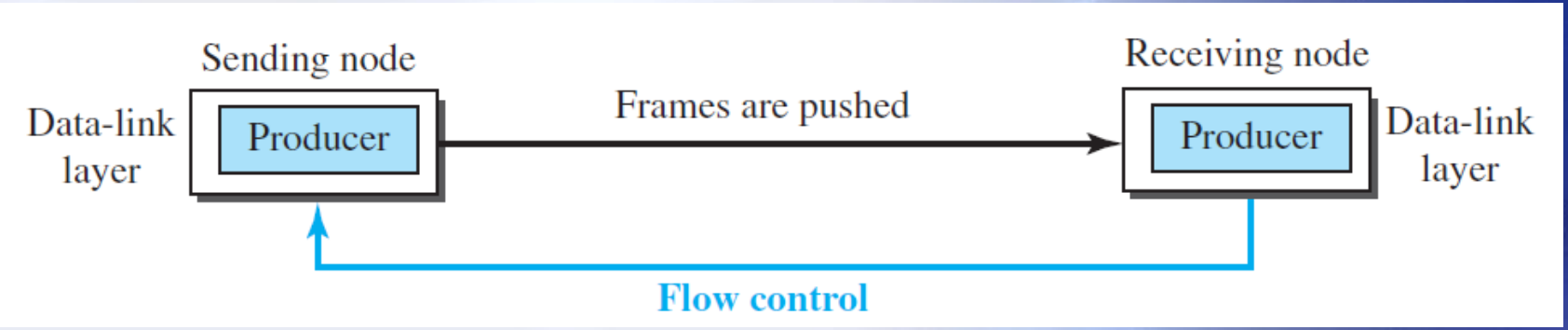


Bit stuffing

- If a 0 and 5 consecutive 1 bits are encountered, an extra 0 is added.
- The extra bit is added after one 0 followed by five 1s regardless of the value of the next bit.



Flow Control



- Solution: use two buffers; one at the sending data-link layer and the other at the receiving data-link layer.
- The flow control communication can occur by sending signals from the consumer to the producer.
- When the buffer of the receiving data-link layer is full, it informs the sending data-link layer to stop pushing frames.

Error Control

- The underlying technology at physical layer is not fully reliable, data-link layer implements error control. Two methods.
- CRC is added to the frame header by the sender and checked by the receiver.
  - if the frame is corrupted, it is silently discarded; if it is not corrupted, the packet is delivered to the network layer. This method is used mostly in wired LANs →Ethernet.
  - if the frame is corrupted, it is silently discarded; if it is not corrupted, an acknowledgment is sent (for the purpose of both flow and error control)to the sender.

Connectionless and Connection-Oriented

Connectionless protocol

- Frames are sent from one node to the next without any relationship between the frames;
- Each frame is independent. →It means that there is no connection between frames.
- The frames are not numbered and there is no sense of ordering.
- Most of the data-link protocols for LANs are connectionless protocols.

Connection-Oriented Protocol

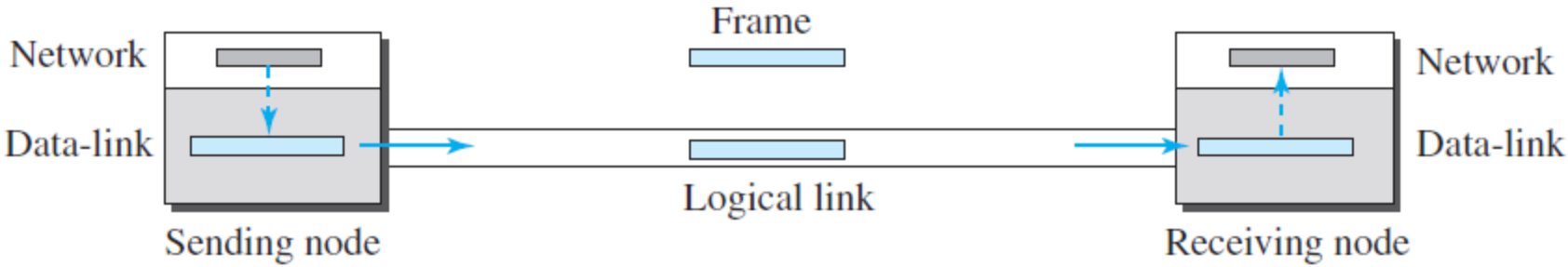
- A logical connection should first be established between the two nodes (setup phase).
- After all frames are transmitted ,the logical connection is terminated
- The frames are numbered and sent in order.
- If they are not received in order, the receiver needs to wait until all frames belonging to the
- Same set are received and then deliver them in order to the network layer.
- Rare in wired lans, in some point-to-point protocols, some wireless lans, and some wans.

DATA-LINK LAYER PROTOCOLS

- Simple, Stop-and-Wait, Go-Back-N, and Selective-Repeat

Simple Protocol

- neither has flow nor error control.

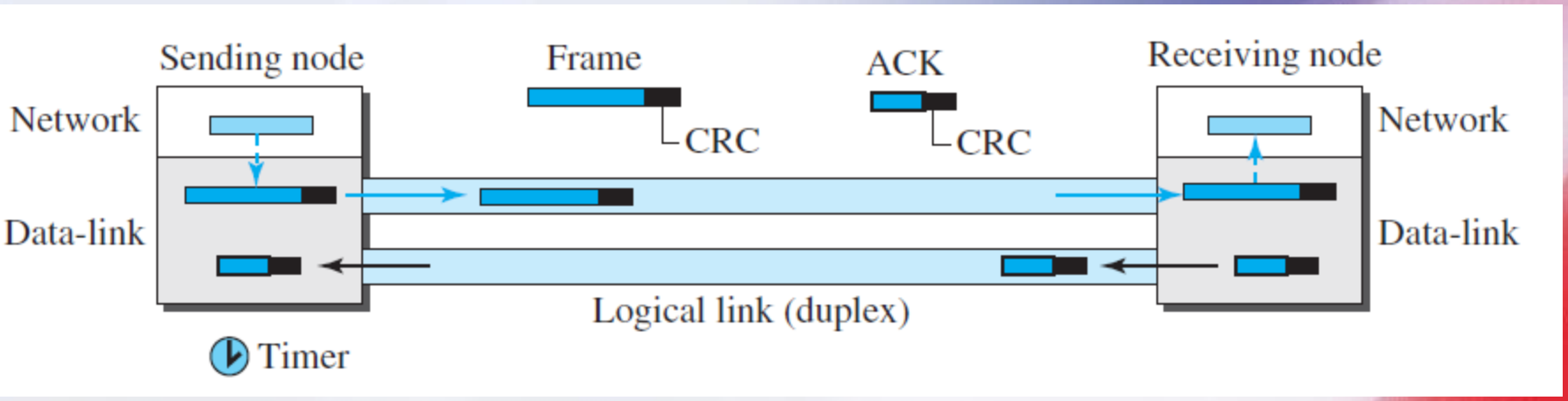


Stop-and-Wait Protocol

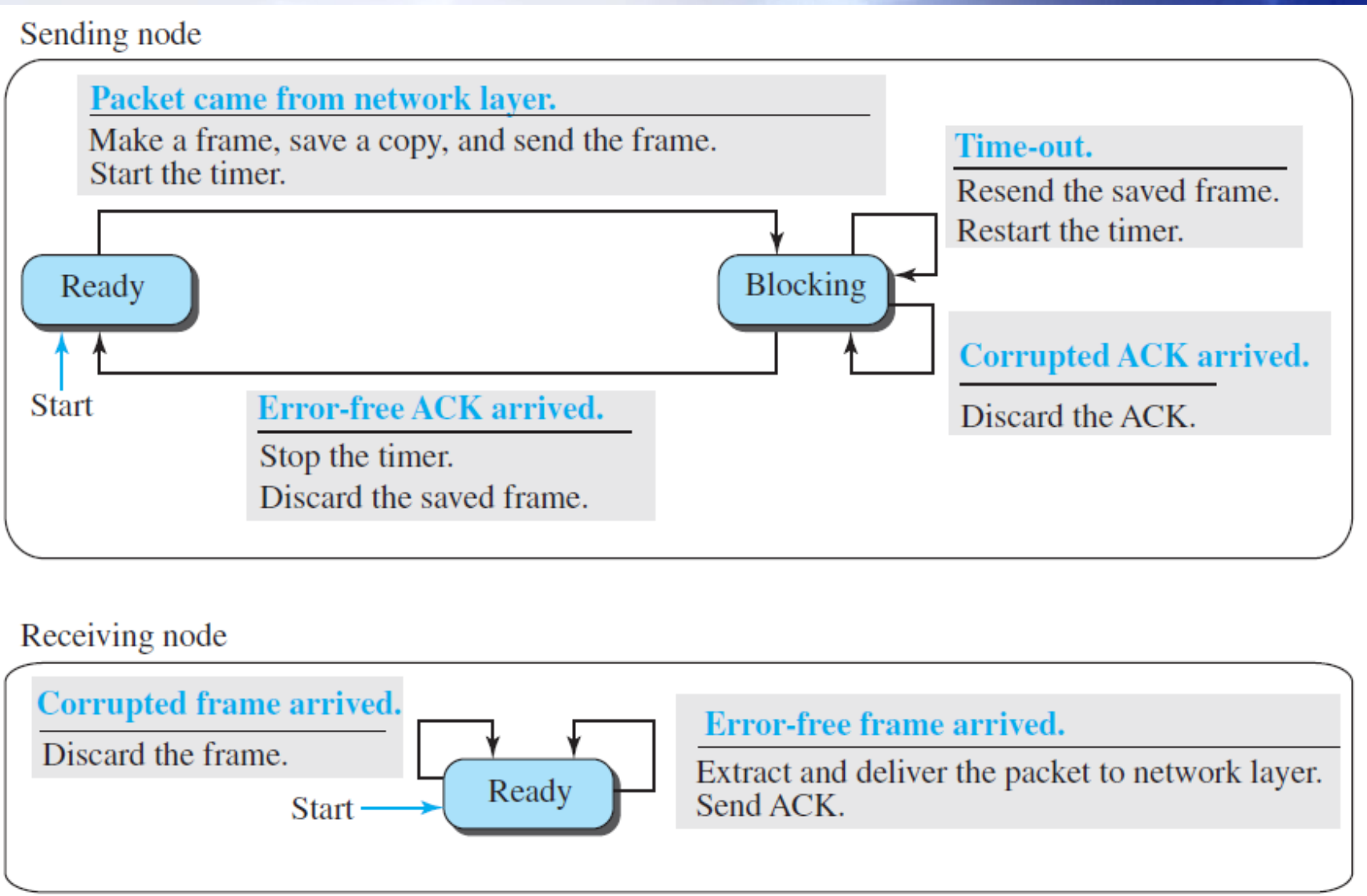
- Uses both flow and error control.
- The sender sends one frame at a time and waits for an acknowledgment before sending the next one.
- To detect corrupted frames, add a CRC to the frame.
- If its CRC is incorrect at the receiver , the frame is corrupted and silently discarded.
- The silence of the receiver is a signal for the sender that a frame was either corrupted or lost.
- Every time the sender sends a frame, it starts a timer. If an acknowledgment arrives before the timer expires, the timer is stopped and the sender sends the next frame (if it has one to send).

Stop-and-Wait Protocol

- If the timer expires, the sender resends the previous frame, assuming that the frame was either lost or corrupted.
- The sender needs to keep a copy of the frame until its acknowledgment arrives.
- When the corresponding acknowledgment arrives, the sender discards the copy and sends the next frame if it is ready.



FSM for the Stop-and-Wait protocol



Stop-and-Wait protocol

Sender States

- The sender is initially in the ready state, but it can move between the ready and blocking state.
- **Ready State:** sender only waiting for a packet from the network layer.
  - If a packet comes from the network layer, the sender creates a frame, saves a copy of the frame, starts the only timer and sends the frame.
- The sender then moves to the blocking state.

Stop-and-Wait protocol

- **Blocking State:** When the sender is in this state, three events can occur:

  a. If a **time-out occurs**, the sender resends the saved copy of the frame and restarts the timer.

  b. If a **corrupted ACK** arrives, it is discarded.

  c. If an **error-free ACK arrives**, the sender stops the timer and discards the saved copy of the frame →moves to the ready state.

Receiver

- Always in the ready state. Two events may occur:

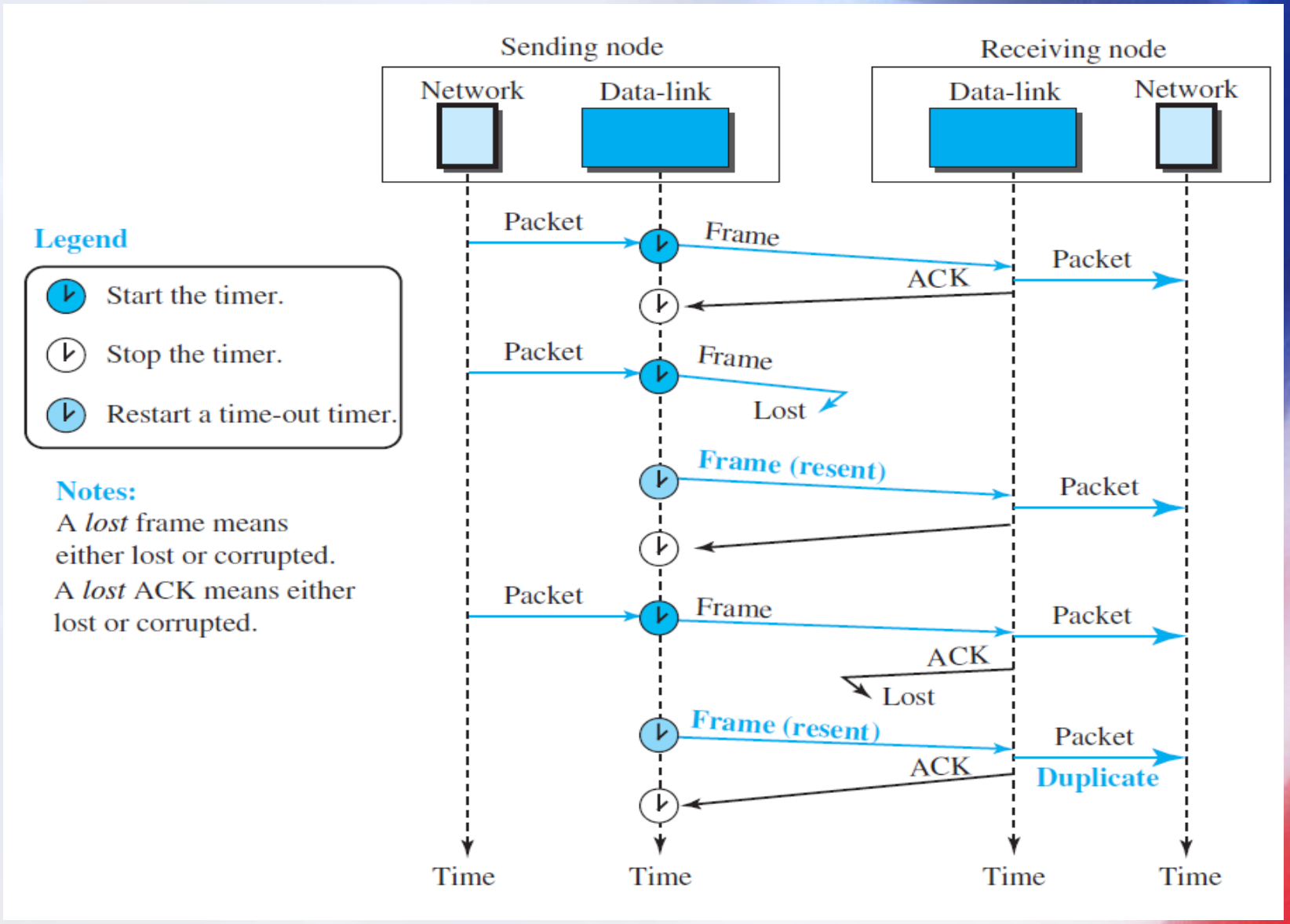
  a. If an **error-free frame arrives**, the message in the frame is delivered to the network layer and an **ACK is sent**.

  b. If a **corrupted frame** arrives, the frame is **discarded.**

Sequence and Acknowledgment Numbers

- **Duplicate packets, corrupted packets**, need to be **avoided**.
- Need to **add sequence numbers** to the data frames and acknowledgment numbers to the ack frames.
- Sequence numbers are 0, 1, 0, 1, 0, 1, . . . ; the acknowledgment numbers can also be 1, 0, 1, 0, 1, 0, …
- The **sequence numbers start with 0, the acknowledgment numbers start with 1**.
- An acknowledgment number always defines the sequence number of the next frame to receive

Flow diagram



Piggybacking

- The two protocols are designed for unidirectional communication,
- To make the communication more efficient, the data in one direction is piggybacked with the acknowledgment in the other direction.

High-level Data Link Control (HDLC)

- HDLC is a bit-oriented protocol for communication over point-to-point and multipoint links.
- It implements the Stop-and-Wait protocol

Configurations and Transfer Modes

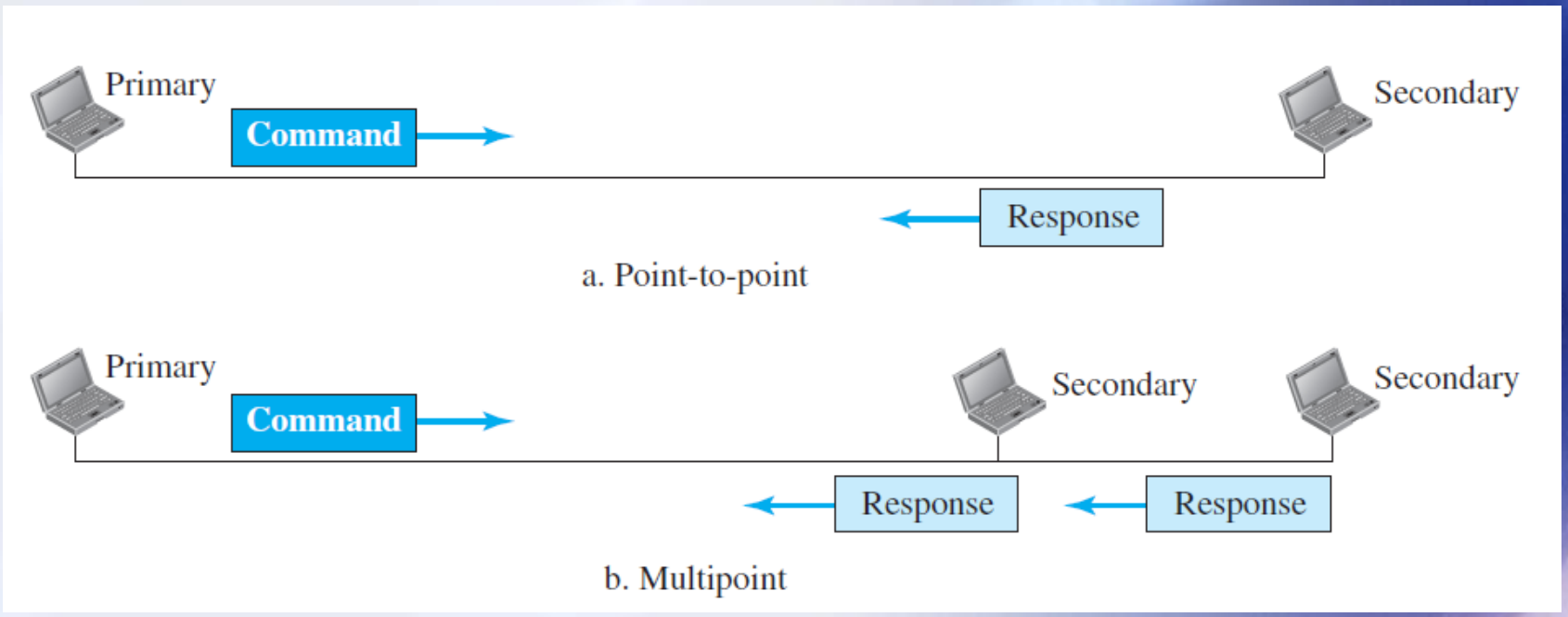
- Two common transfer modes that can be used in different configurations:
  - **Normal response mode (NRM) and asynchronous balanced mode (ABM).**
  - In NRM, the **station configuration is unbalanced**. We have one primary station and multiple secondary stations.
  - A primary station can send commands; a secondary station can only respond.

- The NRM is used for both point-to-point and multipoint links,
- In ABM, the **configuration is balanced**. The link is point-to-point, and each station can function as a primary and a secondary (acting as peers),

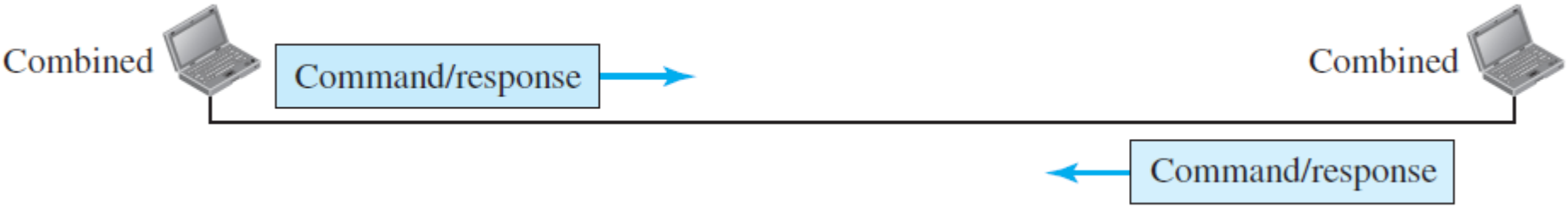
Framing

- HDLC defines three types of frames: **information frames (I-frames), supervisory frames (S-frames), and unnumbered frames (U-frames).**
- Each type of frame serves as an envelope for the transmission of a different type of message.
- **Iframes** are used to **data-link user data** and control information relating to user data (piggybacking).
- **S-frames** are used only to transport **control information**.
- **U-frames** are reserved for **system management**. Information carried by U-frames is intended for managing the link itself

Normal response mode

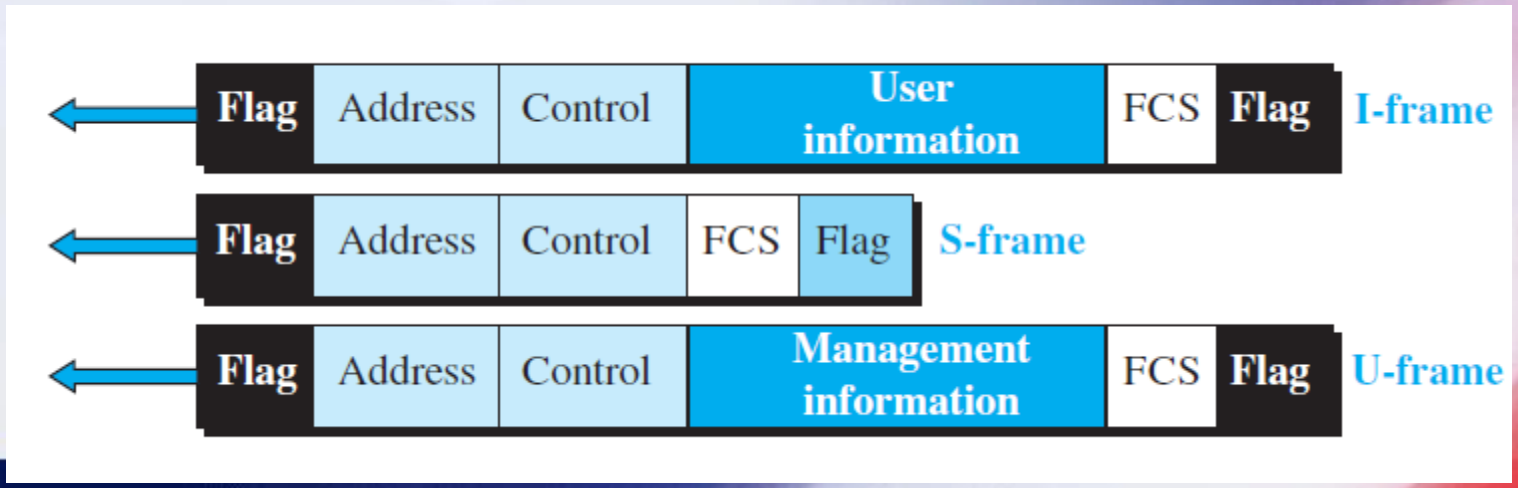


Asynchronous balanced mode



HDLC frames

- Each frame in HDLC may contain up to **six fields**
- Beginning flag field, an address field, a control field, an information field, a frame check sequence (FCS) field, and an ending flag field.
- In multiple-frame transmissions, the ending flag of one frame can serve as the beginning flag of the next frame.



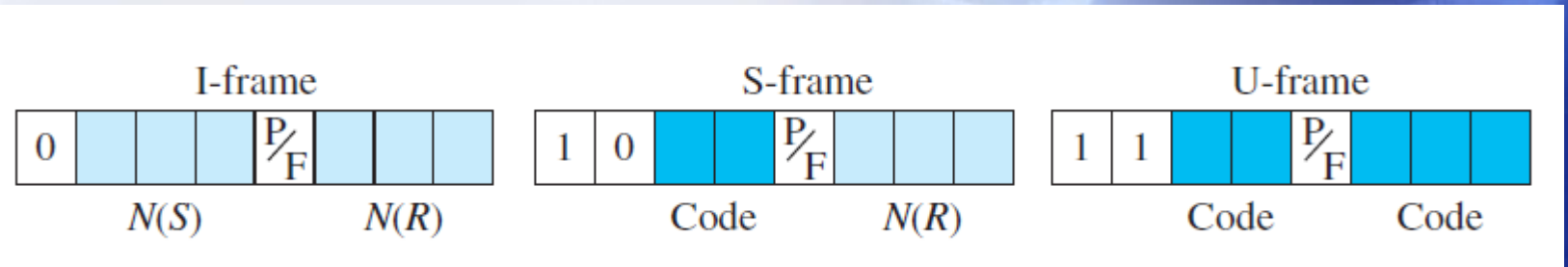
HDLC frames

- **Flag field**: has synchronization pattern 01111110, identifies both the beginning and the end of a frame.
- **Address field:** Has the address of the secondary station.
- If a primary station created the frame, it contains a **to** address.
- If a secondary station creates the frame, it contains a **from** address. Length: varying.

- **Control field:** one or two bytes used for flow and error control.
- The control field determines the **type of frame and defines its functionality**

- **Information field**: the user's **data or management** information. Its length can vary
- FCS field: frame check sequence -HDLC error detection field. contain either a 2- or 4-byte CRC.

Control Field for I-Frames



- designed to carry **user data / flow- and error-control information** (piggybacking).
- first bit defines the type. **0, →is an I-frame**, next 3 bits → **N(S), sequence number**
- last 3 bits, called N(R)→**acknowledgment** number when piggybacking is used.
- single bit between N(S) and N(R) is called **the P/F bit.**
- when it is set (bit = 1) and mean poll or final.
- means **poll** when the **frame is sent by a primary station** to a secondary
- **means final** when the frame is sent by a **secondary to a primary**

Control Field for S-Frames

- Supervisory frames are used for **flow and error control whenever piggybacking is either impossible or inappropriate.**
- do not have information fields.
- If the first 2 bits of the control field are 10, this means the frame is an S-frame.
- The last 3 bits, called N(R) → the acknowledgment number (ACK) or negative acknowledgment number (NAK),
- The 2 bits called code are used to define the **type of S-frame itself.**

S-frames

With 2 bits, we can have four types of S-frames

- **Receive ready (RR): 00**, it is an RR S-frame.
  - frame **acknowledges the receipt** of a safe and sound frame or group of frames- the value of the N(R) field defines the acknowledgment number.
- **Receive not ready (RNR):** 10, RNR S-frame.
  - is an **RR frame with additional function** – acknowledges the receipt of a frame or group of frames,
  - announces that the **receiver is busy** and **cannot receive more frames.**
  - It acts as a kind of **congestion-control** mechanism by asking the sender to slow down. The value of N(R) is the acknowledgment number.

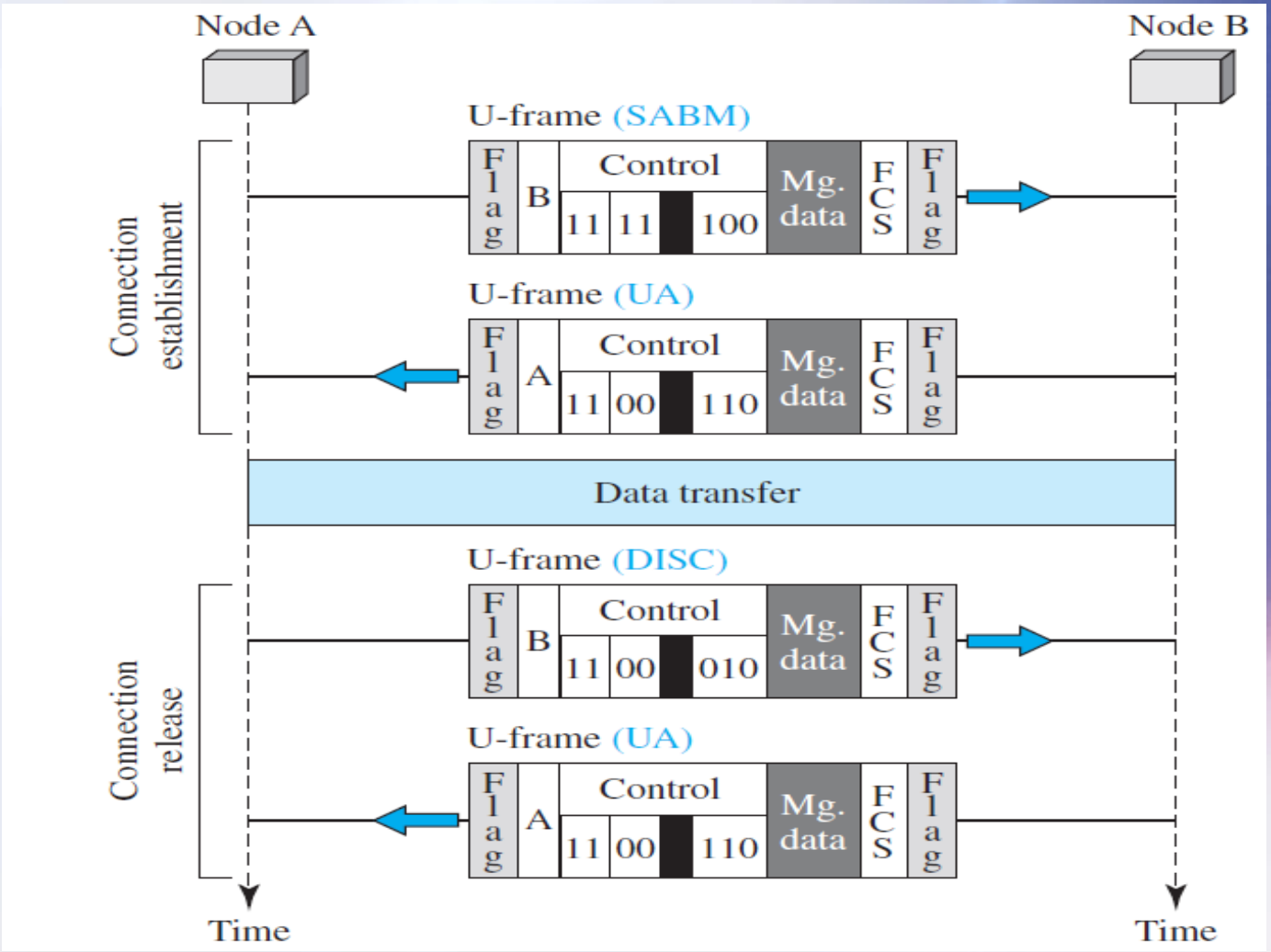
S-frames

- **Reject (REJ):** 01, a NAK frame
  - That can be used in go-back-n ARQ to improve the efficiency of the process by
  - Informing the sender, before the sender timer expires, that the **last frame is lost or damaged**. The value of N(R) is the negative acknowledgment number.
- **Selective reject (SREJ):** 11
- This is a NAK frame **used in Selective Repeat ARQ.**
- The value of N(R) is the negative acknowledgment number.

Control Field for U-Frames

- **Unnumbered frames** are used to exchange session **management and control** information
- U-frames contain an information field, but one used for system management information, not user data.
- U-frame codes are **divided into two sections**: a 2-bit prefix before the P/ F bit and a 3-bit suffix after the P/F bit.
- These two segments (5 bits) can be used to create up to **32 different types of U-frames**.

Connection and disconnection



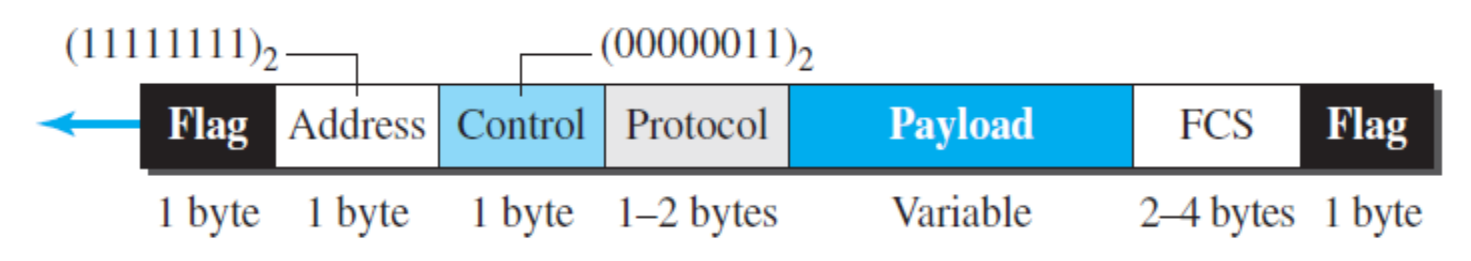
POINT-TO-POINT PROTOCOL (PPP)

Services

- PPP **defines the format of the frame**, also defines how two can negotiate
- Designed to **accept payloads** from several network layers (not only IP).
- **Authentication** is also provided in the protocol
- Provides **network address configuration**.
- **Does not provide flow control**; a crc field is used to detect errors.

Framing

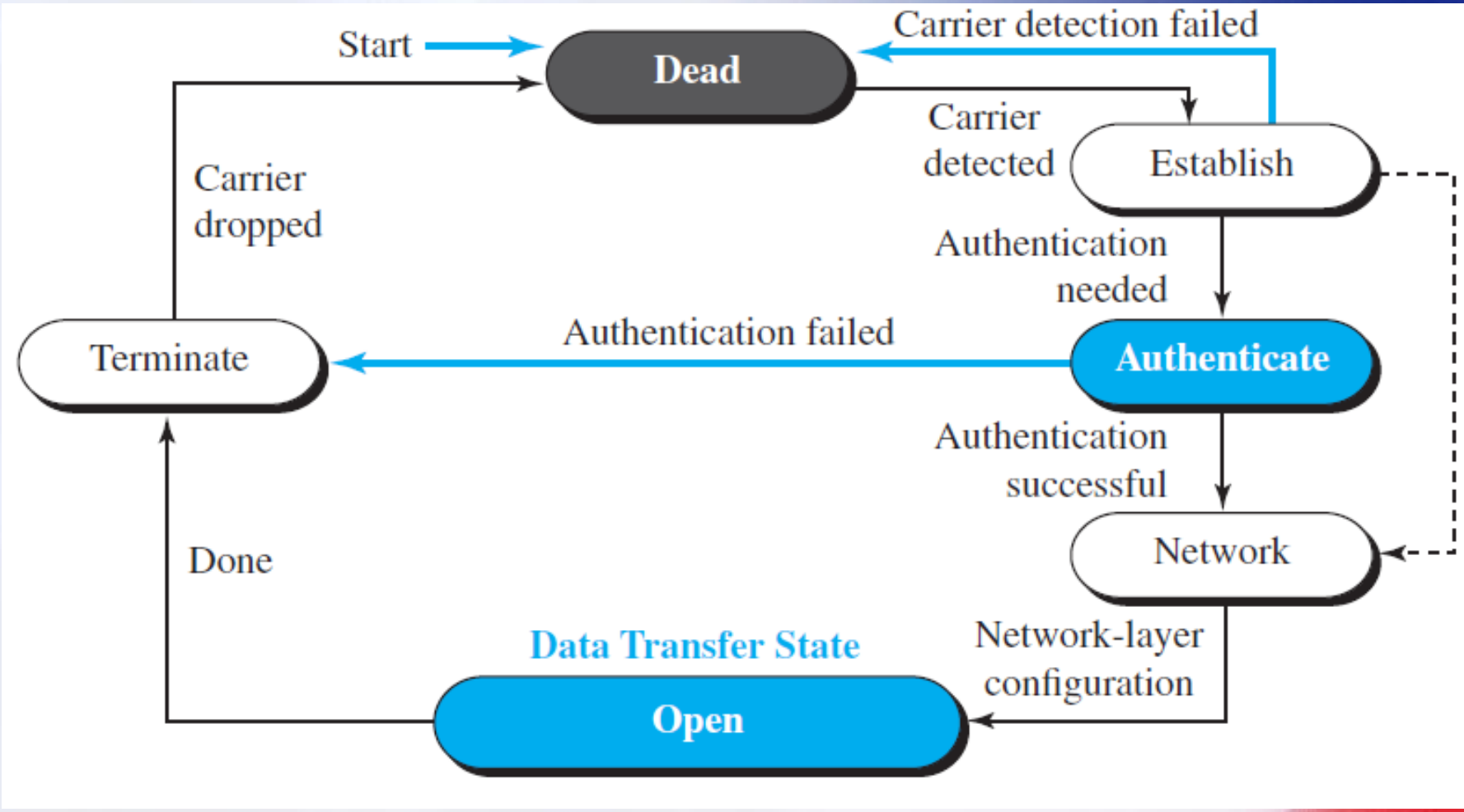
- **Flag:** frame starts & ends with a 1-byte flag with **01111110**
- **Address:** set to 11111111 (broadcast address).
- **Control:** 00000011 ;Error control is limited to **error detection**.
- **Protocol:** type of data in data field:
- **Payload field:** user data / other information ; **byte-stuffed** ; escape byte is 01111101
- **The data field :maximum of 1500 bytes** ; padding is needed if the size is less than the maximum
- **FCS:** Frame Check Sequence (FCS) is a 2-byte or 4-byte standard CRC.



Transition Phases

- A PPP connection **goes through phases** shown as a FSM,
- Starts with the **dead state**: when there is **no active carrier** (at the physical layer) and the line is quiet.
- When one of the **two nodes starts the communication**, the **connection** goes **into the establish state**; options are negotiated between the two parties.
- If the two parties agree that they **need authentication**, then the system needs to do authentication.
- The **link-control protocol packets**, are used for this purpose.

Transition Phases



Transition Phases

- **Data transfer** takes place in the **open state**;
- The connection remains in this state **until one of the endpoints** wants to **terminate** the connection.
- In this case, the system goes to the terminate state.
- The system remains in this state until the carrier (physical-layer signal) is dropped, which moves the system to the **dead state** again.

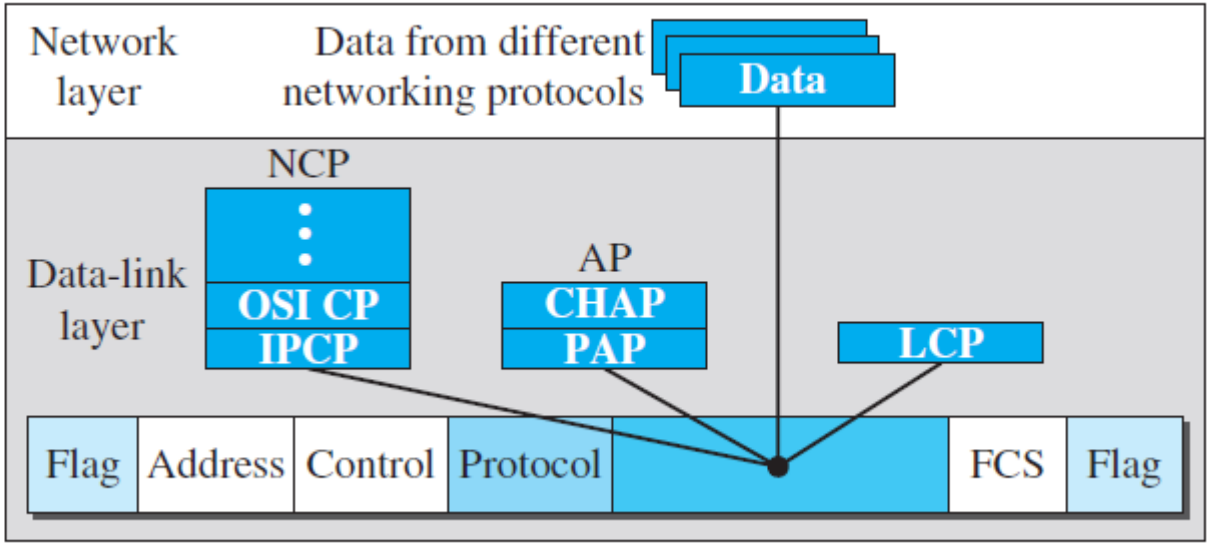
Multiplexing

- PPP uses another set of protocols **to establish link, authenticate and carry the network-layer data**.
- **Link Control Protocol (LCP), two Authentication Protocols (APs), and Network Control Protocols (NCPs).**
- a PPP packet can carry data from one of these protocols in its data field,
- Data may also come from several different network layers

Legend

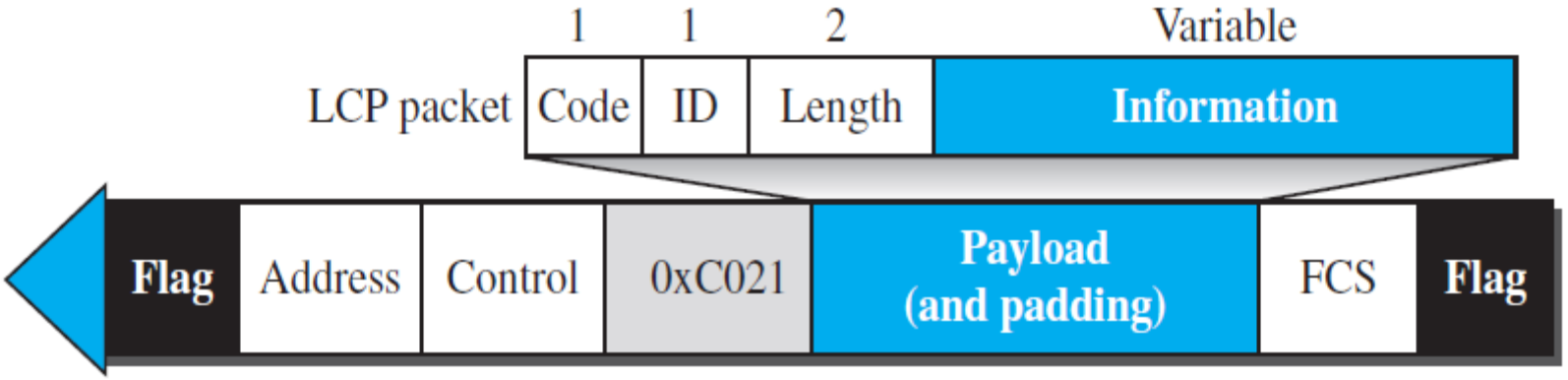
LCP : Link control protocol
AP: Authentication protocol
NCP: Network control protocol

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



Link Control Protocol

- LCP is responsible for **establishing, maintaining, configuring, and terminating links**.
- **Provides negotiation mechanisms** to set options between the two endpoints - reach an agreement before the link can be established.
- All **LCP packets are carried in the payload** field of the PPP frame with the **protocol field set to C021** in hexadecimal



Link Control Protocol

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

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

Link Control Protocol

- **3 categories** of packets.
- 1st category, has first 4 packet types: used for link configuration during the **establish phase**.
- 2nd category, comprising packet types 5 and 6, is used for **link termination** ; last 5 packets are used for link **monitoring and debugging**.
- The **ID field holds a value that matches a request** with a reply. One endpoint inserts a value in this field, which will be copied into the reply packet.
- The length field defines the **length of LCP packet**.
- The information field contains information, such as options, needed for some LCP packets.

Link Control Protocol

- **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 Protocols

- *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.**

Password Authentication Protocol (PAP)

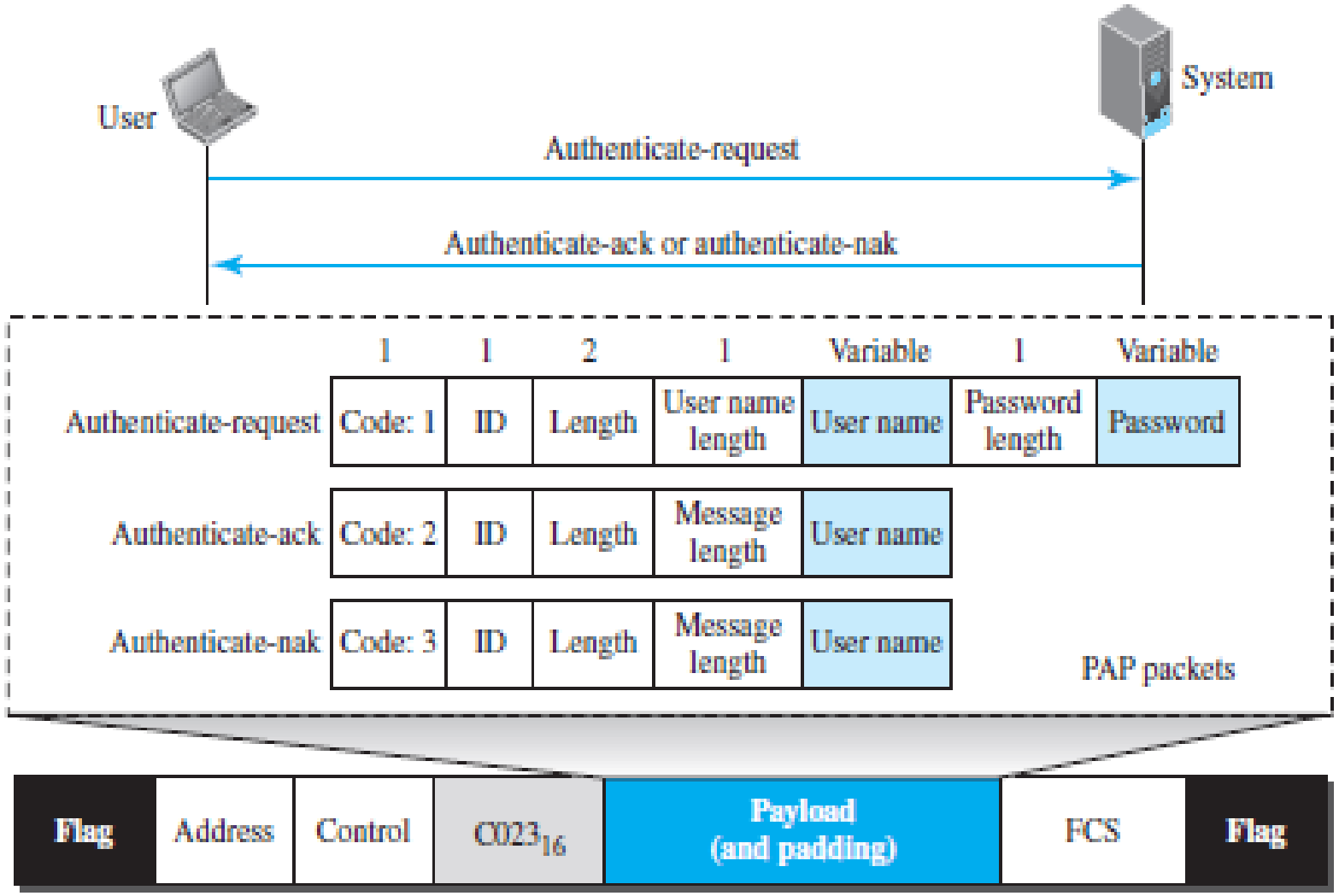
- PAP performs a **two-step process**:

  a. The user who wants to access a system sends an authentication identification 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, authenticate-ack, and authenticate-nak**.

PAP packets encapsulated in a PPP frame



Challenge Handshake Authentication Protocol (CHAP)

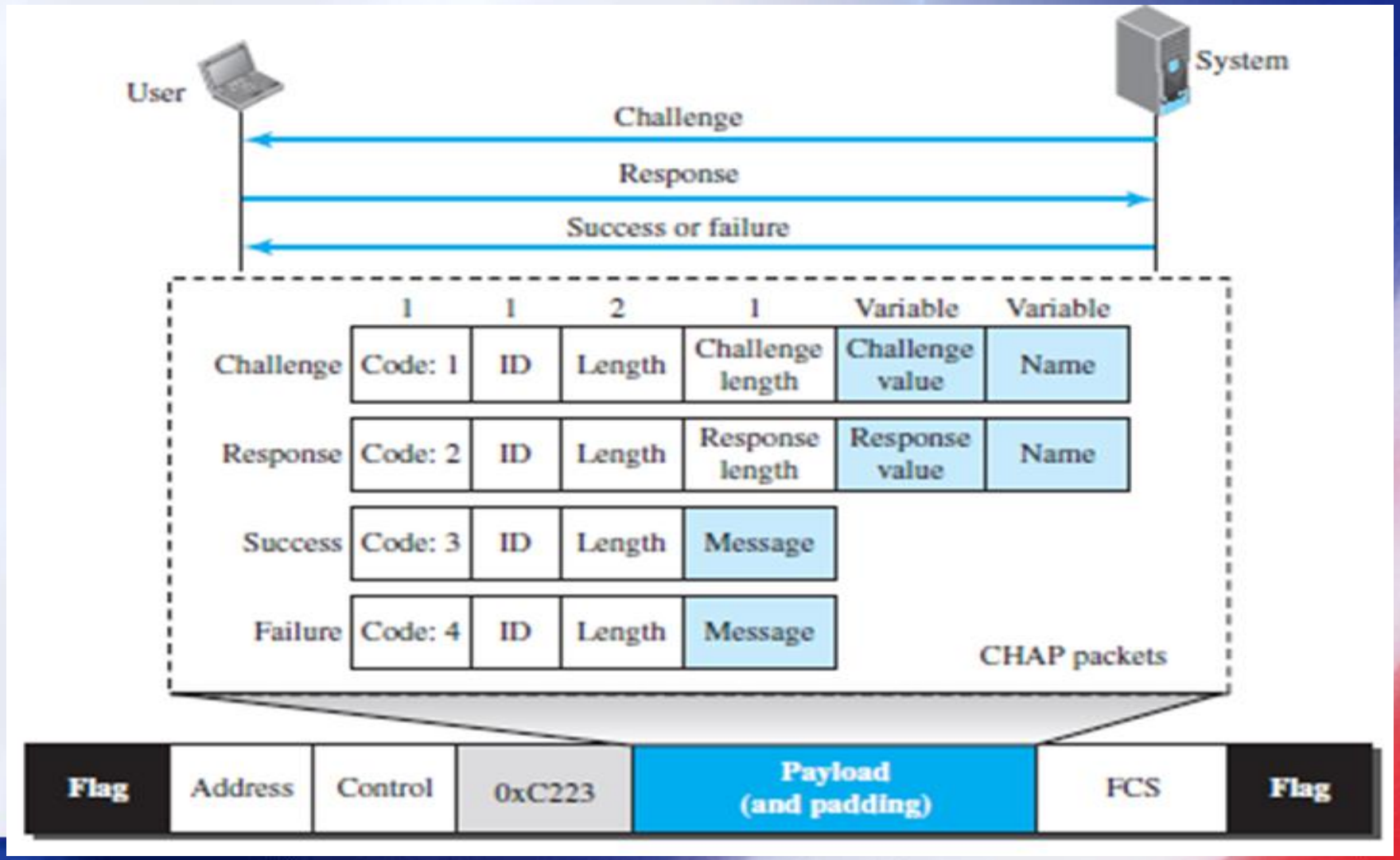
- CHAP is a **three-way handshaking authentication** protocol that provides greater security than PAP.
- the password is kept secret; it is never sent online.

  a. The **system sends the user a challenge packet** containing a challenge value

  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.

CHAP packets encapsulated in a PPP frame



Challenge Handshake Authentication Protocol

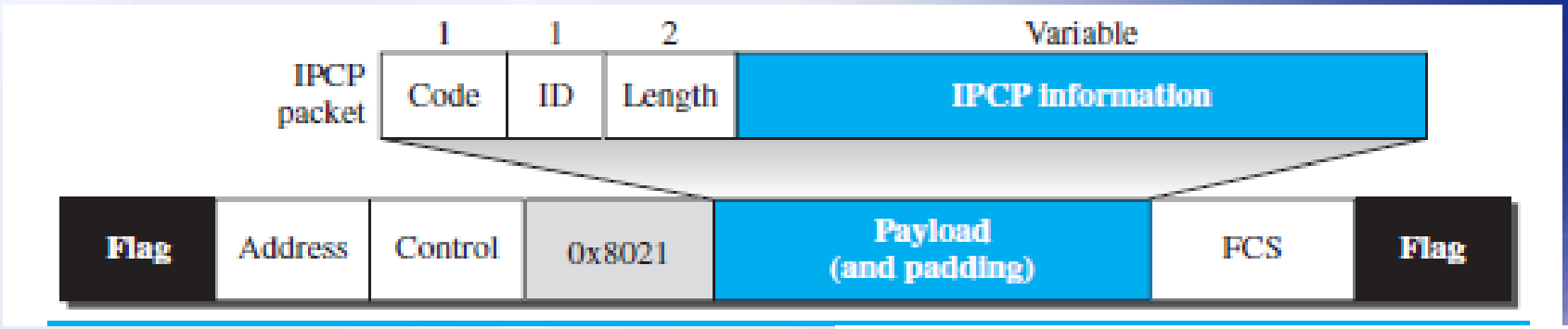
- CHAP packets are encapsulated in the PPP frame with the **protocol value C223**
- There are **four CHAP packets: challenge, response, success, and failure.**
- The first packet is used by the system to send the challenge value.
- The second is used by the user to return the result of the calculation.
- The third is used by the system to allow access to the system.
- The fourth is used by the system to deny access to the system.

Network Control Protocols

- PPP is a **multiple-network-layer protocol-** can carry a network-layer data packet from protocols defined by the Internet, OSI, Xerox, DECnet, AppleTalk, Novel, and so on.
- To do this, PPP has defined a **specific Network Control Protocol for each network protocol.**
- IPCP (Internet Protocol Control Protocol) configures the link for carrying IP data packets. Xerox CP does the same for the Xerox protocol data packets,

Internet Protocol Control Protocol - IPCP

- Configures the link used **to carry IP packets** in the internet.
- The value of the protocol field in hexadecimal is **8021.**



- IPCP defines 7 packets, distinguished by their code values

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

Summary

- Data link control deals with the design and procedures for node-to-node communication
- Byte-oriented and bit-oriented.
- Flow control means creating a balance
- Error control :corrupted frames - discarded; uncorrupted frames are accepted with or without sending acknowledgments.
- DLC protocol can be either connectionless or connection-oriented
- High-level data link control (HDLC)
- Point-to-point protocol (PPP)

Test your Understanding

- Why flags are needed when we use variable-size frames?
- What is *piggybacking* and list its benefit?
- Compare and contrast HDLC with PPP