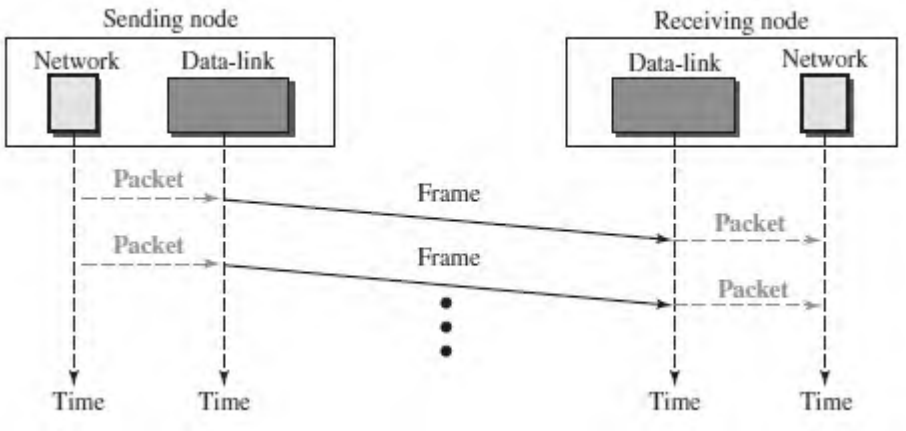
5.5 DATA-LINK LAYER PROTOCOLS

Four protocols have been defined for the data-link layer controls.
They are

1. Simple Protocol
2. Stop-and-Wait Protocol
3. Go-Back-N Protocol
4. Selective-Repeat Protocol

SIMPLE PROTOCOL

- The first protocol is a simple protocol with neither flow nor error control.
- We assume that the receiver can immediately handle any frame it receives.
- In other words, the receiver can never be overwhelmed with incoming frames.
- The data-link layers of the sender and receiver provide transmission services for their network layers.



- The data-link layer at the sender gets a packet from its network layer, makes a frame out of it, and sends the frame.
- The data-link layer at the receiver receives a frame from the link, extracts the packet from the frame, and delivers the packet to its network layer.

NOTE :

2. **STOP-AND-WAIT PROTOCOL**
   REFER STOP AND WAIT FROM FLOW CONTROL
3. **GO-BACK-N PROTOCOL**
   REFER GO-BACK-N ARQ FROM ERROR CONTROL
4. **SELECTIVE-REPEAT PROTOCOL**
   REFER SELECTIVE-REPEAT ARQ FROM ERROR CONTROL

5.6 HDLC (HIGH-LEVEL DATA LINK CONTROL)

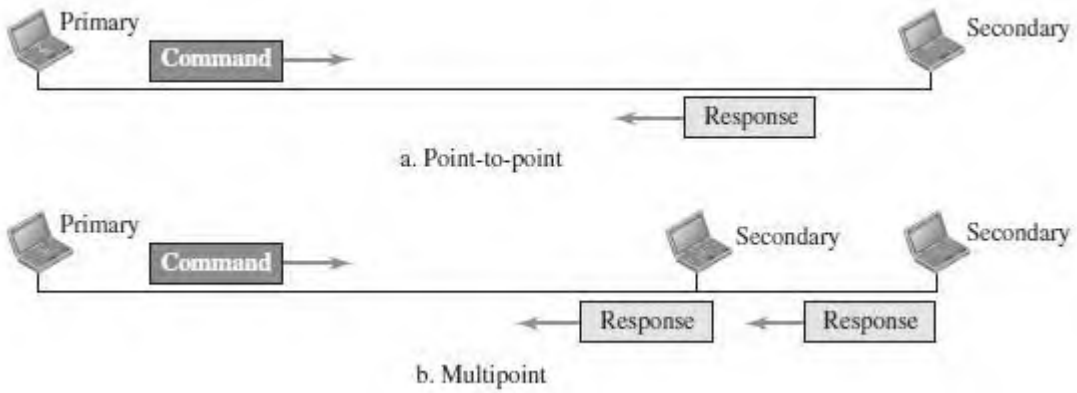
- High-level Data Link Control (HDLC) is a bit-oriented protocol
- HDLC is used for communication over point-to-point and multipoint links.
- HDLC implements the Stop-and-Wait protocol.

HDLC CONFIGURATIONS AND TRANSFER MODES

- HDLC provides two common transfer modes that can be used in different configurations:
    1. **Normal response mode (NRM)**
    2. **Asynchronous balanced mode (ABM).**

Normal response mode (NRM)

- In normal response mode (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.



Asynchronous balanced mode (ABM)

- 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).
- This is the common mode today.

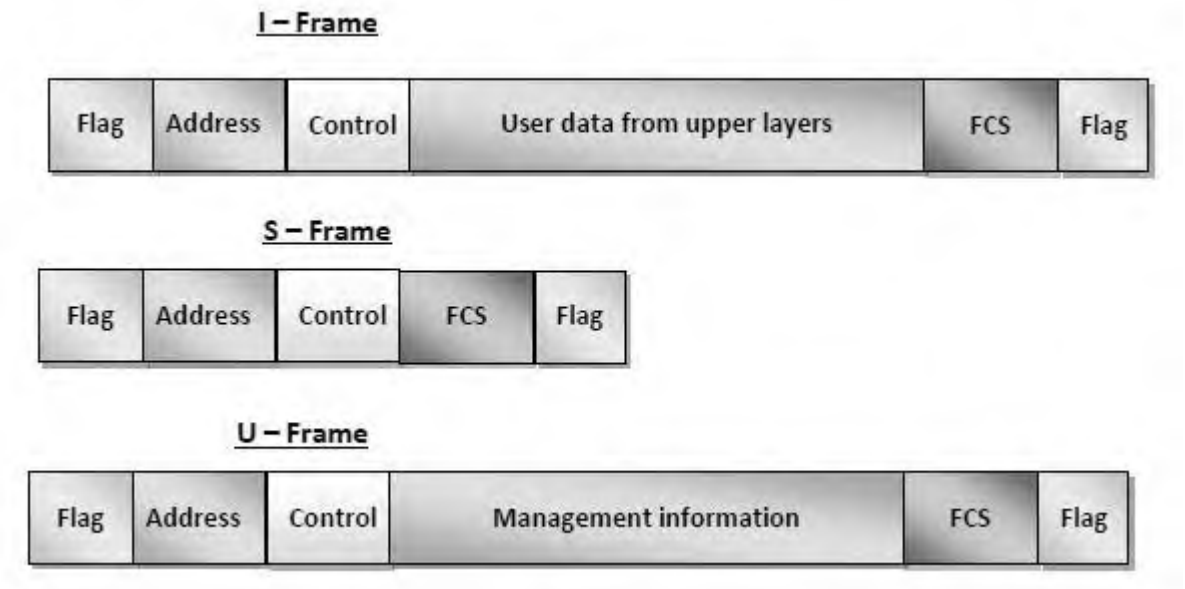
HDLC FRAMES

HDLC defines three types of frames:

1. Information frames (I-frames) - used to carry user data
2. Supervisory frames (S-frames) - used to carry control information
3. Unnumbered frames (U-frames) – reserved for system management

Each type of frame serves as an envelope for the transmission of a different type of message. Each frame in HDLC may contain up to six fields:

1. Beginning flag field
2. Address field
3. Control field
4. Information field (User Information/ Management Information)
5. Frame check sequence (FCS) field
6. Ending flag field In multiple-frame transmissions, the ending flag of one frame can serve as the beginning flag of the next frame.



- **Flag field -** This field contains synchronization pattern 01111110, which identifies both the beginning and the end of a frame.

- **Address field -** This field contains 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. The address field can be one byte or several bytes long, depending on the needs of the network.

- **Control field.** The control field is one or two bytes used for flow and error control.

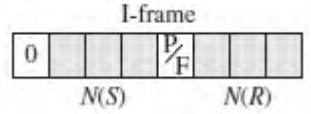
- **Information field.** The information field contains the user's data from the network layer or management information. Its length can vary from one network to another.

- **FCS field.** The frame check sequence (FCS) is the HDLC error detection field. It can contain either a 16- bit or 32-bit CRC

CONTROL FIELD FORMAT FOR THE DIFFERENT FRAME TYPES

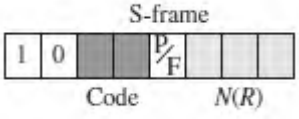
Control Field for I-Frames

- I-frames are designed to carry user data from the network layer. In addition, they can include flow-control and error-control information
- The first bit defines the type. If the first bit of the control field is 0, this means the frame is an I-frame.
- The next 3 bits, called N(S), define the sequence number of the frame.
- The last 3 bits, called N(R), correspond to the acknowledgment number when piggybacking is used.
- The single bit between N(S) and N(R) is called the P/F bit. If this bit is 1 it means poll (the frame is sent by a primary station to a secondary).



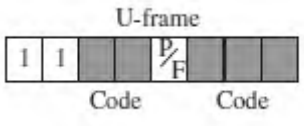
Control Field for S-Frames

- Supervisory frames are used for flow and error control whenever piggybacking is either impossible or inappropriate.
- S-frames 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),correspond to the acknowledgment number (ACK) or negative acknowledgment number (NAK), depending on the type of S-frame.
- The 2 bits called code are used to define the type of S-frame itself.
- With 2 bits, we can have four types of S-frames – Receive ready (RR), Receive not ready (RNR), Reject (REJ) and Selective reject (SREJ).



Control Field for U-Frames

- Unnumbered frames are used to exchange session management and control information between connected devices.
- U-frames contain an information field, but used only for system management information and not user data.
- If the first 2 bits of the control field are 11, this means the frame is an U-frame.
- 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.
- Together, these two segments (5 bits) can be used to create up to 32 different types of U-frames.



5.7 POINT-TO-POINT PROTOCOL (PPP)

- Point-to-Point Protocol (PPP) was devised by IETF (Internet Engineering Task Force) in 1990 as a Serial Line Internet Protocol (SLIP).
- PPP is a data link layer communications protocol used to establish a direct connection between two nodes.
- It connects two routers directly without any host or any other networking device in between.
- It is used to connect the Home PC to the server of ISP via a modem.
- It is a byte - oriented protocol that is widely used in broadband communications having heavy loads and high speeds.

Services Provided by PPP

The main services provided by Point - to - Point Protocol are –

1. Defining the frame format of the data to be transmitted.
2. Defining the procedure of establishing link between two points and exchange of data.
3. Stating the method of encapsulation of network layer data in the frame.
4. Stating authentication rules of the communicating devices.
5. Providing address for network communication.
6. Providing connections over multiple links.

7. Supporting a variety of network layer protocols by providing a range os services.

PPP Frame

PPP is a byte - oriented protocol where each field of the frame is composed of one or more bytes.

1. Flag − 1 byte that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
2. Address − 1 byte which is set to 11111111 in case of broadcast.
3. Control − 1 byte set to a constant value of 11000000.
4. Protocol − 1 or 2 bytes that define the type of data contained in the payload field.
5. Payload − This carries the data from the network layer. The maximum length of the payload field is 1500 bytes.
6. FCS − It is a 2 byte(16-bit) or 4 bytes(32-bit) frame check sequence for error detection. The standard code used is CRC.

Components/Protocols of PPP

Three sets of components/protocols are defined to make PPP powerful:
❖ Link Control Protocol (LCP)
❖ Authentication Protocols (AP)
❖ Network Control Protocols (NCP)

Link Control Protocol (LCP) –

It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission. It also provides negotiation mechanisms to set options between the two endpoints. Both endpoints of the link must reach an agreement about the options before the link can be established.

Authentication Protocols (AP) –

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.

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.

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.
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.
CHAP is more secure than PAP, especially if the system continuously changes the challenge value. Even if the intruder learns the challenge value and the result, the password is still secret.

Network Control Protocols (NCP) –

PPP is a multiple-network-layer protocol. It can carry a network-layer data packet from protocols defined by the Internet. PPP has defined a specific Network Control Protocol for each network protocol. These protocols are used for negotiating the parameters and facilities for the network layer. For every higher-layer protocol supported by PPP, one NCP is there.