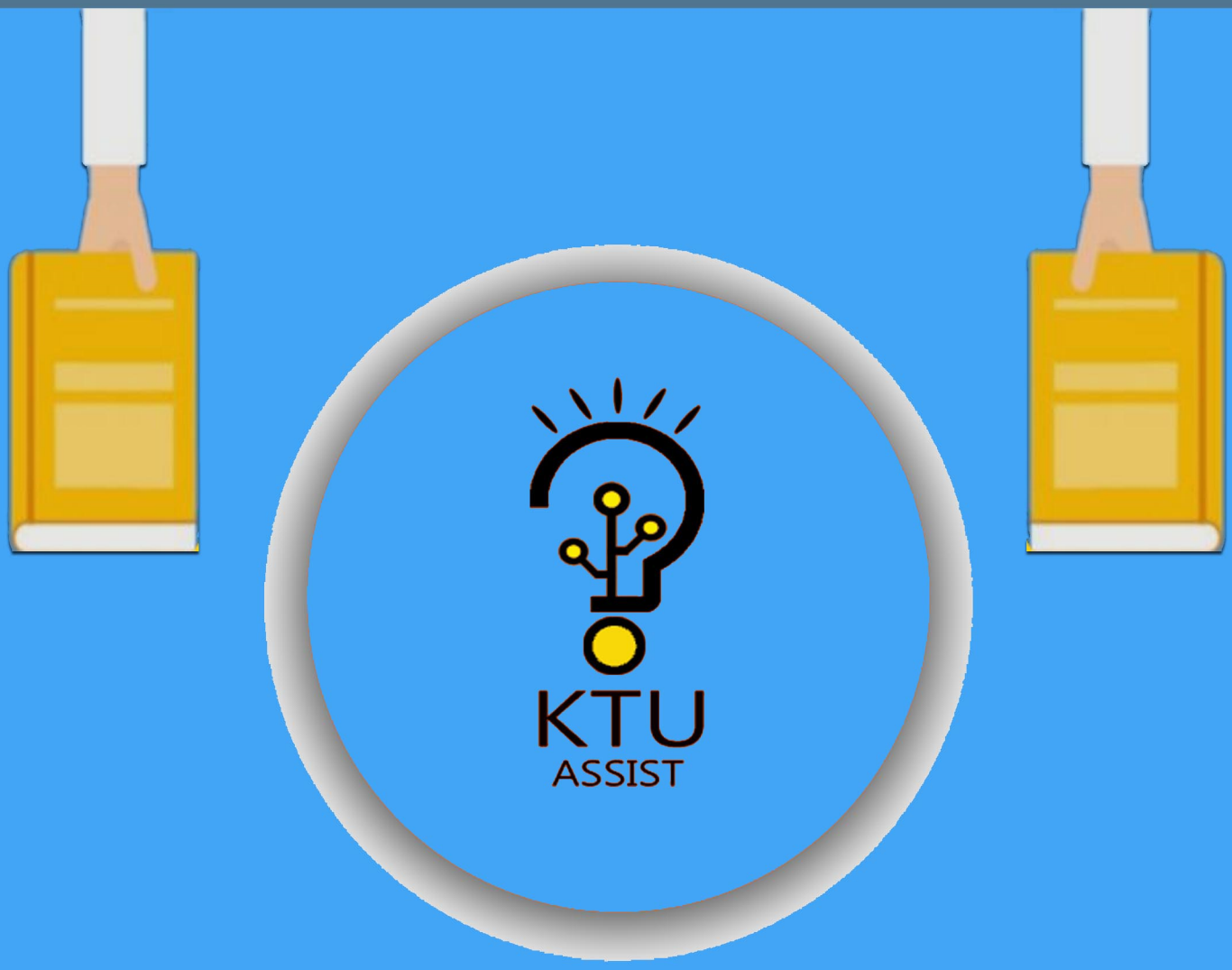
APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

STUDY MATERIALS



Module 2

Data Link Layer Design Issues

DATA LINK LAYER(DLL)

Ques 1) Define data link layer.

Ans: Data Link Layer
Data Link Layer is the second layer of the OSI model. Its position is given in the **figure 2.1**.

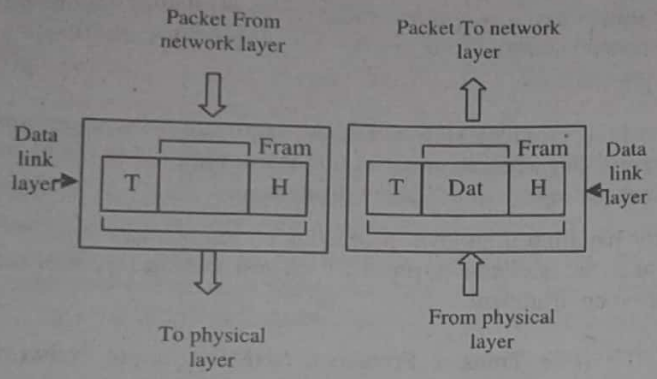


Figure 2.1: Data Link Layer

The data-link layer is responsible for error free transfer of data frames. This layer provides synchronisation for the physical level. The purpose of the data link layer is to transfer blocks of data without error between two adjacent devices. Adjacent devices are physically connected by a communication channel such as telephone lines, coaxial cables, optical fibers, or satellites.

Date link layer deals with two basic issues:

1) How data frames can be reliably transmitted, and
2) How a shared communication medium can be accessed

Ques 2) What are the data link layer design issues? Discuss them.

Or

What do you mean by flow control and error control?

Ans: Data Link Layer Design Issues
The data link layer has a number of functions to carry out. These functions include providing a well-defined service interface to the network layer, determining how the bits of the physical layer are grouped into frames.
The design issues of the data link layer are given below:

1) **Services Provided to Network Layer:** The function of the data link layer is to provide services to the network layer. The principle service is transferring data from the network layer on the source machine to the network layer on the destination machine. The job of the data link layer is to transmit the bits to the destination machine, so they can be handed over to the network layer. The actual transmission follows the path but it is easier to think in terms of two data link layer processes communicating using a data link protocol.

   The data link layer can be designed to offer various services. The actual services offered can vary from system to system. Three reasonable possibilities that commonly provided are:

   i) **Unacknowledged Connectionless Service:** Unacknowledged connectionless service consists of having the source machine send independent frames to the destination machine without having the destination machine acknowledge them.

   ii) **Acknowledged Connectionless Service:** The next step up in terms of reliability is acknowledged connectionless service. When this service is offered, there are still no connections used, but each frame sent is individually acknowledged. In this way, the sender knows whether or not a frame has arrived safely.

   iii) **Acknowledged Connection-Oriented Service:** The most sophisticated service the data link layer can provide to the network layer is connection-oriented service. With this service, the source and destination machines establish a connection before any data are transferred. Each frame sent over the connection is numbered and the data link layer guarantees that each frame sent is indeed received.

2) **Framing:** Data transmission in the physical layer means moving bits in the form of a signal from the source to the destination. The physical layer provides bit synchronisation to ensure that the sender and receiver use the same bit durations and timing.

   The data link layer, on the other hand, needs to pack bits into frames, so that each frame is distinguishable from another. Framing is the function of the data link layer that separates a message from one source to a destination or from other messages to other destinations, by adding a sender address and a destination address. The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

   i) **Fixed-Size Framing:** Frames can be of fixed or variable size. In fixed-size framing, there is no nee

for defining the boundaries of the frame; the size itself can be used as a delimiter. An **example** of this type of framing is the ATM wide-area network, which uses frames of fixed size called **cells**.

ii) **Variable-Size Framing:** In Variable-Size Framing, one needs a way to define the end of the frame and the beginning of the next. Historically, two approaches were used for this purpose:

a) **Character-Oriented Protocols:** In a Character-oriented Protocol, data to be carried are 8-bit characters from a coding system such as ASCII. The header, which normally carries the source and destination addresses and other control information and the trailer, which carries error detection or error correction redundant bits, are also multiples of 8 bits. **Figure 2.2** shows the format of a frame in a character-oriented protocol.

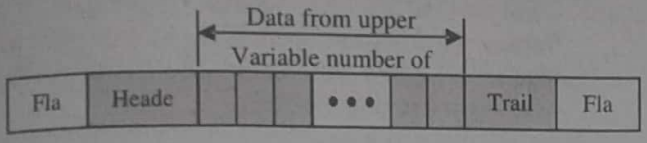


Figure 2.2: Frame in Character-oriented Protocol

Character-oriented framing was popular when only text was exchanged by the data link layers. The flag could be selected to be any character not used for text communication.

b) **Bit-Oriented Protocols:** In a bit-oriented Protocol, 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. However, in addition to headers (and possible trailers), still 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, as shown in **figure 2.3.**

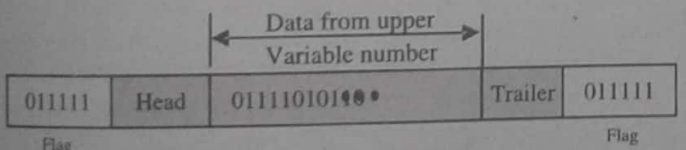


Figure 2.3: Frame in a Bit-oriented

3) **Flow Control:** Flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver. The flow of data must not be allowed to overwhelm the receiver. Any receiving device has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data.

The receiving device must be able to inform the sending device before those limits are reached and to request that the transmitting device send fewer frames or stop temporarily. Incoming data must be checked and processed before they can be used. The rate of such processing is often slower than the rate of transmission. For flow control there is two approaches are commonly used:

i) **Feedback-Based Flow Control:** In this approach receiver sends back information to the sender giving it permission to send more data or at least telling the sender how the receiver is doing.

ii) **Rate-Based Flow Control:** In this the protocol has a built-in mechanism that limits the rate at which senders may transmit data, without using feedback from the receiver.

The two categories of flow control are:
a) Stop-and-Wait
b) Sliding Window

4) **Error Control:** Error control provides error detection and correction. There are two basic strategies for dealing with errors. These are:

i) To include only enough redundancy to allow the receiver to confirm that an error occurred, but not aware of which error and therefore request it for re-transmission.

ii) Second method is to include enough unwanted data along with each block of data sent to enable to receiver to extract what the transmitted character must have been.

Mechanics for **error handling** at this layer are based on error detection and retransmission with the error handling usually performed using algorithms implemented in software such as checksum in error detection and correction.

Ques 3) Discuss the different categories of flow control protocols.

Or

Explain the following flow control protocols:

1) Stop-and-Wait

2) Sliding Window

Ans: Categories of Flow Control

1) **Stop-and-Wait Protocol:** In stop-and-wait protocol, the source sends a packet and only after receiving the acknowledgement from the destination, it sends next packet. This is a simple protocol, but it results in lots of delay, and the bandwidth is not used efficiently.

When the source (end system A) sends the first packet to the destination (end system B) and waits for the acknowledgment, then B sends an acknowledgement packet.

Then A sends the second packet, and B sends the acknowledgement. A repeat this process until sender

A transmit an end of transmission frame (EOT). The process is illustrated in **figure 2.4**.

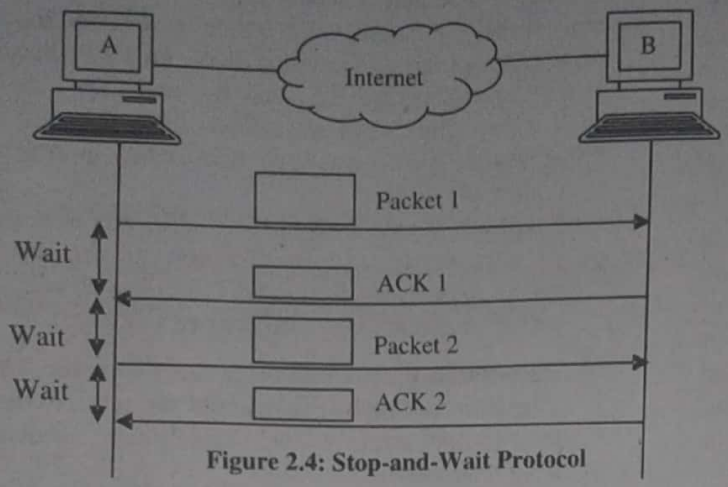


Figure 2.4: Stop-and-Wait Protocol

A **refinement** to this protocol is the sliding window protocol.

Advantages of Stop-and-Wait Protocol

i) It is a very simple protocol of flow control.
ii) Since size of frames is small hence error detection is easy

Disadvantage of Stop-and-Wait Protocol

i) Only single frame is transmitted which makes the protocol inefficient
ii) Throughput is very poor and the channel bandwidth is not used efficiently. **For example,** if this protocol is used in a satellite network, A will send a packet, and after one second it will receive the acknowledgement. During that one second, the satellite channel is free, and the channel is not used effectively.

2) **Sliding Window Protocol:** In the elementary data link protocols, data frames are transmitted in one direction only but there is a need to transmitting data in both directions. This is achieved by sliding window protocol.

In the sliding window method, the sender can transmit several frames before needing an acknowledgment. Frames can be sent one right after another, meaning that the link can carry several frames at once and its capacity can be used efficiently. The **sender maintains information** about:

i) Size of sender window,
ii) Last acknowledgement received,
iii) Last frame sent.

The receiver acknowledges only some of the frames, using a single ACK to confirm the receipt of multiple data frames.

Receiver holds information about:

i) Receiver window size,
ii) Large acceptable frame,
iii) Last frame received.

In the sliding window method protocol, several frames can be in transit at a time. The sliding window refers to imaginary boxes at both the sender and the receiver. This window can hold frames at either end and provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgment.

Frames may be acknowledged at any point without waiting for the window to fill up and may be transmitted as long as the window is not yet full. To keep track of which frames have been transmitted and which received, sliding window introduces an identification scheme based on the size of the window.

The frames are numbered modulo-n, which means they are numbered from 0 to n – 1.When the receiver sends an ACK, it includes the number of the next frame it expects to receive. The window can hold n – 1 frames at either end; therefore, a maximum of n – 1 frames may be sent before an acknowledgment is required. **Figure 2.5** shows the relationship of a window to the main buffer.

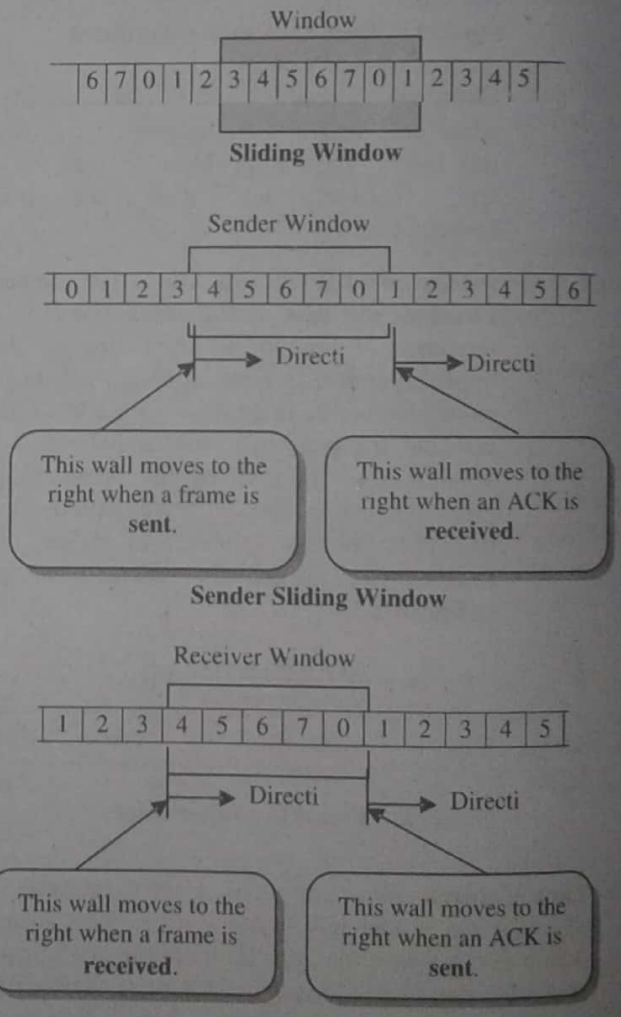


Figure 2.5: Receiver Sliding Window

For example, figure 2.5 shows a sample transmission that uses sliding window flow control with a window of seven frames. In this example, all frames arrive

undamaged. There are two steps as given below for implementation:

Step 1: When data 0 and data 1 are sent by the sender, sliding window of the sender shrank from the left. The receiver received the data 0 and data 1 and then sliding window of the receiver shrank from the left.

Step 2: When acknowledgement is sent by receiver for data 0 and data 1, the sliding window of receiver is expanded to the right. The sender received the acknowledgement for data 0 and data 1 and then the sliding window of sender expanded from the right.

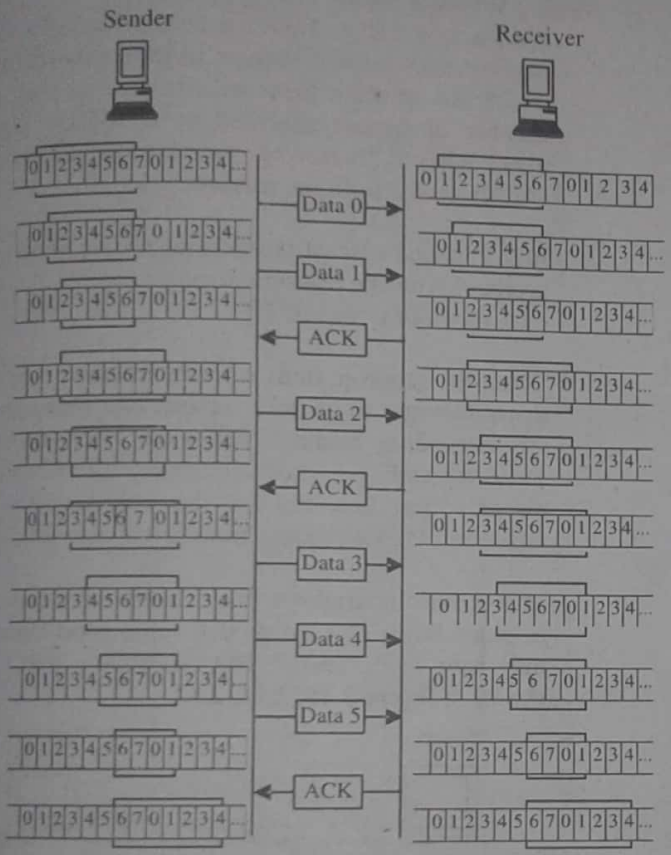


Figure 2.6: Example of Sliding Window

Similarly we repeat Step 1 and Step2 for transmitting data 2 from sender to the receiver and transmitting acknowledgement from the receiver to the sender. Again we will repeat the same process for data 3, data 4 and data 5 as well as for acknowledgement 6.

Advantages of Sliding Window Protocol

i) The primary advantage is network utilization.
ii) Data can be transmitted in both directions.
iii) Several frames can be in transit at a time.

Disadvantages of Sliding Window Protocol

i) The primary disadvantages are complexity and hardware capacity.
ii) The window can hold n-1 frames at either end, therefore, a maximum of n – 1 frame may be sent before an acknowledgment is required.

Ques 4) What is ARQ? What are the different types of ARQ techniques? Also discuss their advantages and disadvantages?

Or

Discuss about Stop-and-Wait ARQ and Sliding Window ARQ with suitable diagram.

Ans: Automatic Repeat Request (ARQ)

Automatic Repeat Request (ARQ), also known as **Automatic Repeat Query**, is an error-control method for data transmission that uses acknowledgements (messages sent by the receiver indicating that it has correctly received a data frame or packet) and timeouts (specified periods of time allowed to elapse before an acknowledgment is to be received) to achieve reliable data transmission over an unreliable service.

If the sender does not receive an acknowledgment before the timeout, it usually re-transmits the frame/packet until the sender receives an acknowledgment or exceeds a predefined number of re-transmissions. The receiver will send back an ARQ message to the transmitter to indicate that the last block should be retransmitted.

Types of ARQ Techniques

There are two commonly used ARQ techniques:

1) **Stop-and-Wait ARQ:** Stop-and-wait ARQ is a form of stop-and-wait flow control extended to include retransmission of data in case of lost or damaged frames It is also known as **ABP(Alternating Bit Protocol).**

   For retransmission to work, four features are added to the basic flow control mechanism:

   i) The sending device keeps a copy of the last frame transmitted until it receives an acknowledgment for that frame. Keeping a copy allows the sender to retransmit lost or damaged frames until they are received correctly.

   ii) For identification purposes, both data frames and ACK frames are numbered alternately 0 and 1. This numbering allows for identification of data frames in case of duplicate transmission.

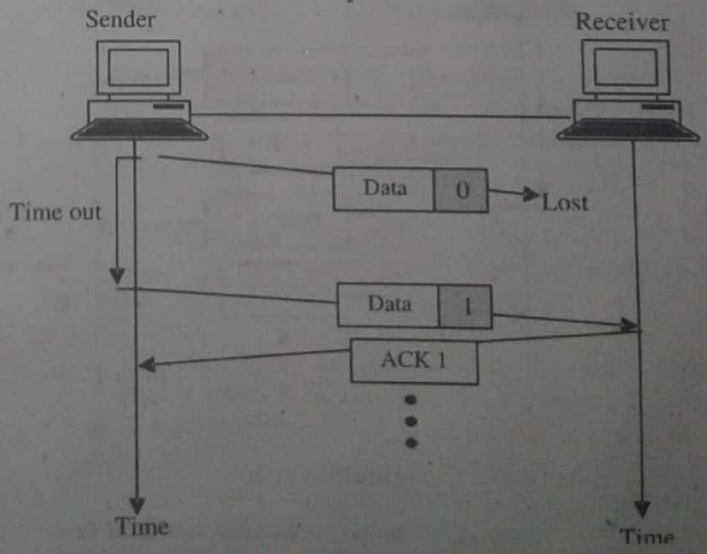


Figure 2.7: Stop-and-Wait ARQ, Lost Data Frame

iii) If an error is discovered in a data frame, indicating that it has been corrupted in transit, a NAK frame is returned. NAK frames, which are not numbered, tell the sender to retransmit the last frame sent (**Figure 2.7**).

iv) The sending device is equipped with a timer. If an expected acknowledgment is not received within an allotted time period, the sender assumes that the last data frame was lost in transit and sends it again (**Figure 2.8 and Figure 2.9**).

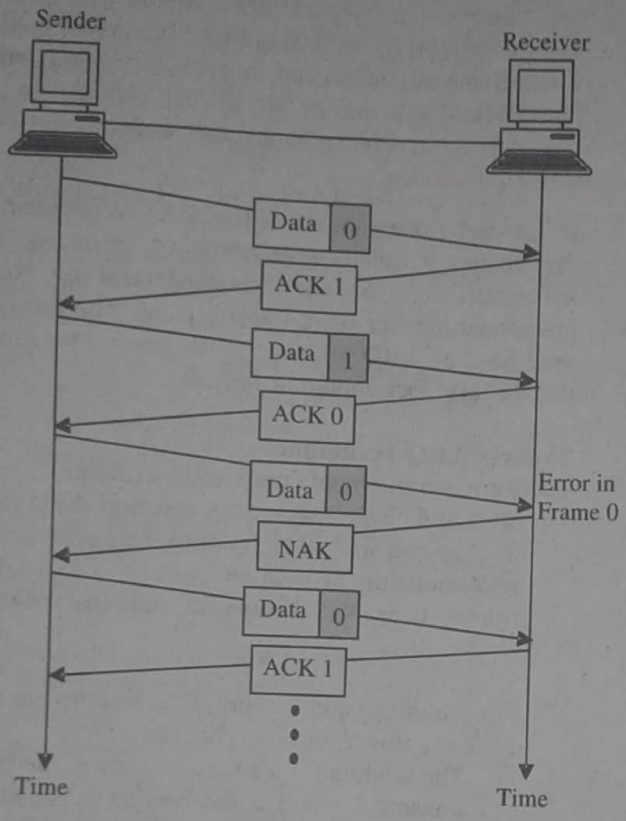


Figure 2.8: Stop-and-Wait ARQ, Damaged Frame

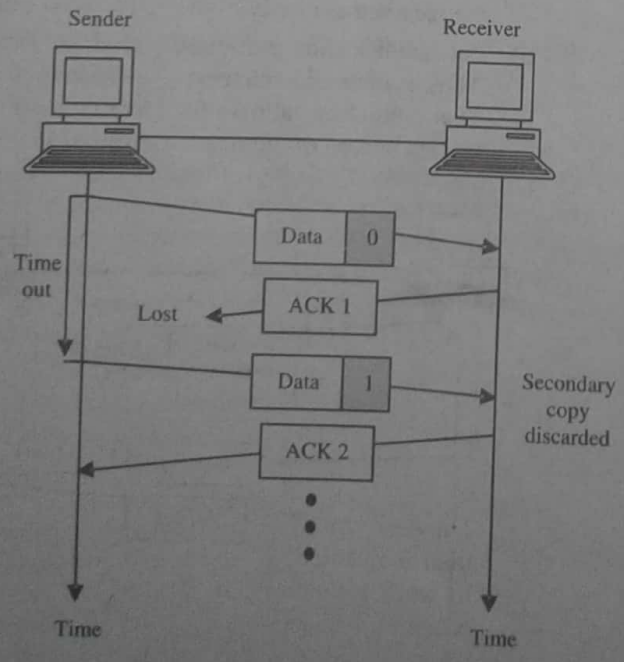


Figure 2.9: Stop-and-Wait ARQ, Lost ACK Frame

Advantages of Stop-and-Wait ARQ

i) It can be used for noisy channels.
ii) It has both error and flow control mechanism.
iii) It has timer implementation.
iv) Easy to implement.
v) Low processor burden.
vi) Low buffer requirement.

Disadvantages of Stop-and-Wait ARQ

i) Efficiency is very less.
ii) Timer should be set for each individual frame.
iii) No pipelining.
iv) Sender window size is 1.
v) Receiver window size 1.

2) **Sliding Window ARQ:** It is of two types:

i) **Go-Back-n ARQ:** This is a specific instance of the automatic repeat request (ARQ) protocol, in which the sending process continues to send a number of frames specified by a window size even without receiving an acknowledgement (ACK) packet from the receiver.

It is a special case of the general sliding window protocol with the transmit window size of N and receive window size of 1.

When the receiver finds a frame in error, it tells the transmitter to go back, resend that frame and all succeeding frames. After the erred frame, some succeeding frames will arrive. The receiver discards these knowing that the erred frame will arrive and the succeeding frames will also follow.

This feature guarantees that frames are received in order, but it also means that some good frames may have to be resent. The Go-Back-n ARQ is shown in **figure 2.10, 2.11, 2.12**.

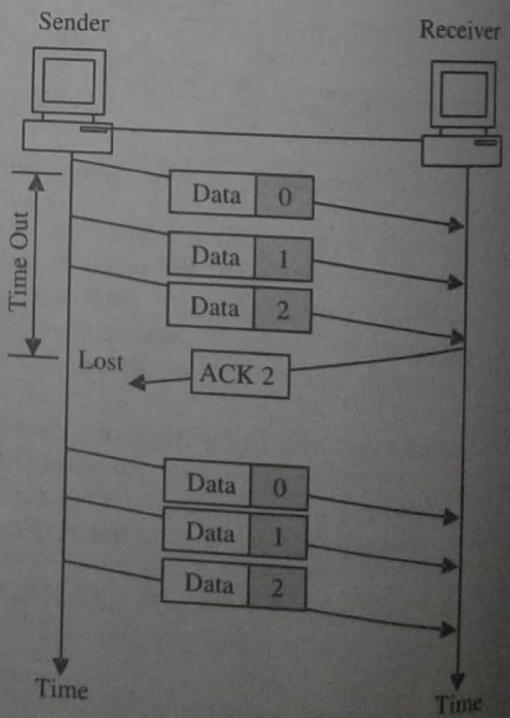


Figure 2.10: Go-back-n, lost ACK

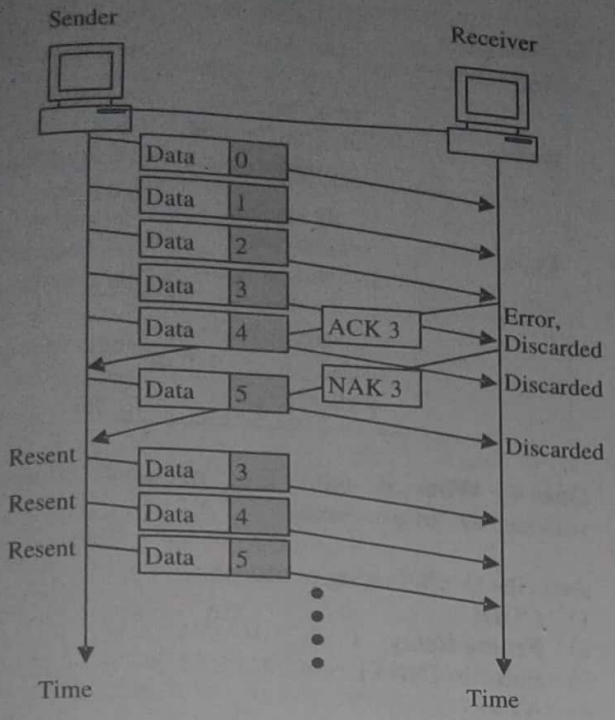


Figure 2.11: Go-back-n, damaged data frame

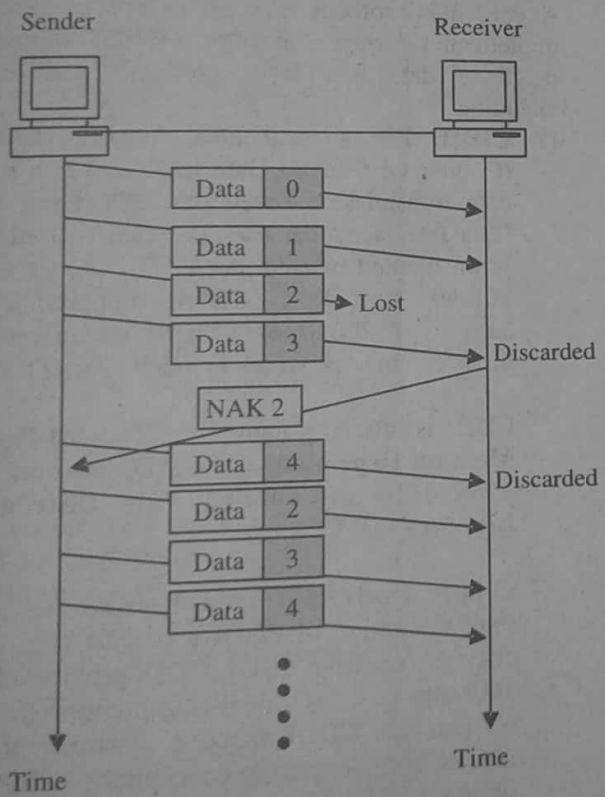


Figure 2.12: Go-back-n, lost Data Frame

Advantages of Go-Back-n ARQ

a) The sender can send many frames at a time.
b) Timer can be set for a group of frames.
c) Only one ACK can acknowledge one or more frames.
d) Efficiency is more.
e) Waiting time is pretty low.
f) We can alter the size of the sender window.

Disadvantages of Go-Back-n ARQ

a) Buffer requirement.
b) Transmitter needs to store the last N packets.
c) Scheme is inefficient when round-trip delay large and data transmission rate is high.
d) Re-transmission of many error-free packets following an erroneous packet.
e) If NAK is lost, a long time is wasted until re-transmission of all packets (until another NAK is sent).

ii) **Selective Reject ARQ:** Selective Reject or Selective Repeat is one of the automatic repeat-request (ARQ) techniques. With selective repeat, the sender sends a number of frames specified by a window size even without the need to wait for individual ACK from the receiver as in stop-and-wait.

However, the receiver sends ACK for each frame individually, which is not like cumulative ACK as used with go-back-n.

The receiver accepts out-of-order frames and buffers them. The sender individually retransmits frames that have timed out.

In selective-repeat ARQ, only the specific damaged or lost frame is retransmitted. If a frame is corrupted in transit, a NAK is returned and the frame is resent out of sequence. The receiving device must be able to sort the frames it has and insert the retransmitted frame into its proper place in the sequence.

The receiving device must contain sorting logic to enable it to reorder frames received out of sequence. It must also be able to store frames received after a NAK has been sent until the damaged frame has been replaced.

The sending device must contain a searching mechanism that allows it to find and select only the requested frame for retransmission.

A buffer in the receiver must keep all previously received frames on hold until all retransmissions have been sorted and any duplicate frames have been identified and discarded.

To aid selectivity, ACK numbers, like NAK numbers, must refer to the frame received (or lost) instead of the next frame expected.

This complexity requires a smaller window size than is needed by the go-back-n method if it is to work efficiently. It is recommended that the window size be less than or equal to (n+1)/2, where n – 1 is the go-back-n window size. **Figure 2.13** of selective repeat, damaged data frame is **shown above.**

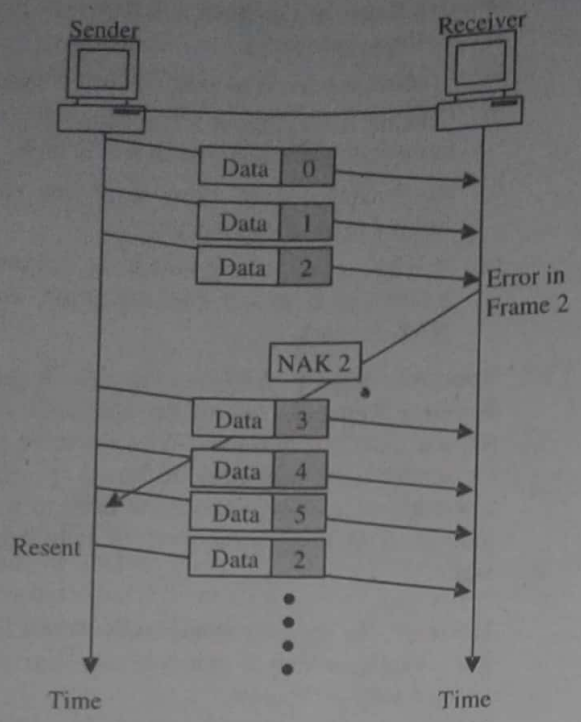


Figure 2.13: Selective Repeat, Damaged Data Frame

Advantages of Selective-Repeat ARQ

i) Similar to Go-Back-N ARQ. Hówever, the sender only retransmits frames for which a NAK is received.

ii) Fewer retransmissions.

Disadvantages of Selective-Repeat ARQ

i) More complexity at sender and receiver

ii) Each frame must be acknowledged individually (no cumulative acknowledgements)

iii) Receiver may receive frames out of sequence

Ques 5) What is difference between Selective-Reject and Go-Back-N

Ans: Difference between Selective-Reject and Go-Back-N
The difference between Selective-Reject and Go-Back-N is shown in **table 2.1**:

Table 2.1: Selective Reject *vs.* Go-Back-N

Basis	Selective Reject	Go-Back-N
Retransmission	Selective Retransmission	Unnecessary retransmissions in case of lost packets
Complexity	More complex than Go back N	Less complex
Simplicity	Not very simple to implement	simple to implement
Throughput	Lesser throughput	Gives more throughput in case of significant end-to end transmission delay
Amount of Retransmission	Minimizes the amount of retransmissions	No minimal retransmission
Buffer	Receiver needs large buffer and reinsertion logic	Receiver does not need to buffer received packets
Type	Only rejected packets are retransmitted	All packets following the lost packet that are to be retransmitted
Logic	Complex logic to send packets out of order	Lesser complex logic to send packets out of order

Ques 6) What is data link protocol? Discuss the various related protocols.

Or

Describe the following protocols:

1) CDDI
2) Frame Relay
3) Point-to-Point Protocol
4) ATM

Ans: Data Link Layer Protocols and Technologies
A data link protocol is a set of specifications used to implement the data link layer. OPNET supports a wide range of data link layer protocols and technologies including:

1) **CDDI:** For a local area network (LAN), CDDI (Copper Distributed Data Interface) is a standard for data transmission based on FDDI (Fiber Distributed Data Interface) that uses shielded twisted-pair (STP) or unshielded twisted pair (UTP) copper wire instead of fiber optic lines. CDDI supports a dual-ring capacity of 200 Mbps. CDDI's maximum distance is up to 200 meters, which is much shorter than FDDI.

CDDI is officially named the **Twisted-Pair Physical Medium Dependent** (TP-PMD) standard and is also referred to as **Twisted Pair Distributed Data Interface** (TP-DDI).

Copper Distributed Data Interface (CDDI) is the implementation of FDDI protocols over twisted-pair copper wire. Like FDDI, CDDI provides data rates of 100Mbps and uses dual-ring architecture to provide redundancy. CDDI supports distances of about 100 meters from desktop to concentrator. CDDI is defined by the ANSI X3T9.5 Committee. The CDDI standard is officially named the Twisted-Pair Physical Medium-Dependent (TP-PMD) standard. It is also referred to as the Twisted-Pair Distributed Data Interface (TP-DDI), consistent with the term Fiber Distributed Data Interface (FDDI). CDDI is consistent with the physical and media-access control layers defined by the ANSI standard.

The ANSI standard recognises only two types of cables for CDDI – Shielded Twisted Pair (STP) and

unshielded twisted pair (UTP). STP cabling has 150ohm impedance and adheres to EIA/TIA 568 (IBM Type 1) specifications. UTP is data-grade cabling (Category 5) consisting of four unshielded pairs using tight-pair twists and specially developed insulating polymers in plastic jackets adhering to EIA/TIA 568B specifications.

Figure 2.14 Illustrates the CDDI TP-PMD specification in relation to the remaining FDDI specifications:

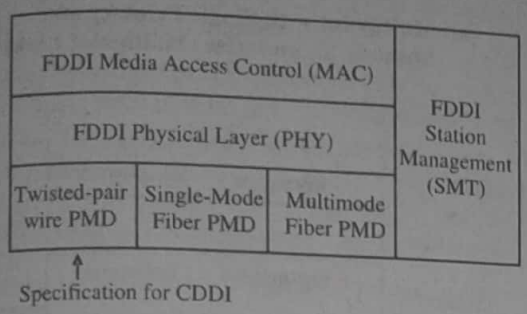


Figure 2.14: CDDI TP-PMD and FDDI Specifications Adhere to Different Standards

2) **Frame Relay:** In packet switching packet are moved between the various network segments until the destination is reached. Frame relay uses variable length packets for more efficient and flexible transfer than that offered by X.25 the older packet switching technology.

In sum, the service that the network provides can be speeded up by increasing data rate, eliminating error-recovery procedures and reducing processing time. Another advantage of frame relay over a conventional static TDM connection is that it uses virtual connections. Data traffic is often bursty and normally would require much larger bandwidths to support the short data messages and much of the time that bandwidth would remain idle.

Virtual connections of frame relay only use the required bandwidth for the period of the burst or usage. This is one reason why frame relay is used so widely to interconnect LANs over a Wide Area Network (WAN). **Figure 2.15** shows a typical frame relay network.

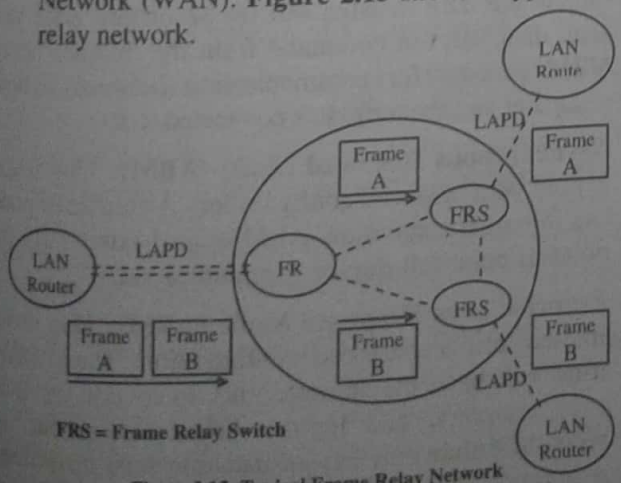


Figure 2.15: Typical Frame Relay Network

3) **ATM (Asynchronous Transfer Mode):** ATM is a networking technology that was designed specifically to handle a combination of the low-delay steady-stream characteristics of voice and video and the bursty, intermittent characteristics of data communications.

Asynchronous Transfer Mode (ATM) is an electronic digital data transmission technology. ATM is implemented as a network protocol and was first developed in the mid-1980s. The goal was to design a single networking strategy that could transport real-time video and audio as well as image files, text and e-mail.

Two groups, the International Telecommunications Union and the ATM Forum were involved in the creation of the standards. ATM is a packet switching protocol that encodes data into small fixed-sized cells (cell relay) and provides data link layer services that run over OSI Layer 1 physical links.

It differs from other networks as ATM exposes properties from both circuit switched and small packet switched networking, making it suitable for wide area data networking as well as real-time media transport. ATM uses a connection-oriented model and establishes a virtual circuit between two endpoints before the actual data exchange begins. ATM is a core protocol used in the SONET/SDH backbone of the public switched telephone network (**figure 2.16**).

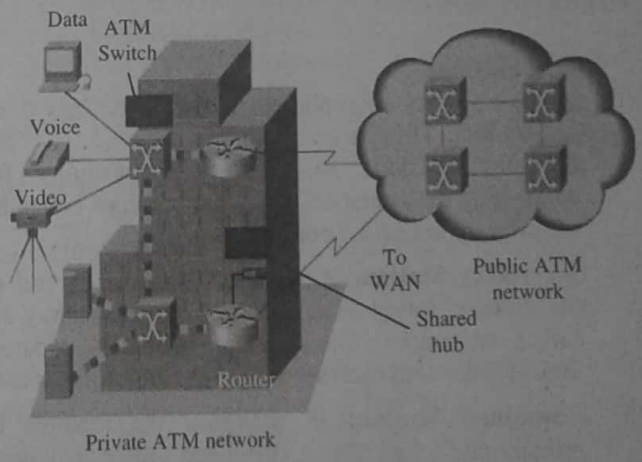


Figure 2.16: Private ATM Network and a Public ATM Network both can carry Voice, Video and Data Traffic

4) **Point-to-Point Protocol:** PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP is widely used, especially in the analog modem access to the ISP, where one end is the PC and the

other end is the ISP router. The functions performed are:

i) The Point-to-Point Protocol (PPP) was designed to transport multi-protocol packets between two peers connected by simple links.

ii) These links provide full-duplex simultaneous bi-directional operation.

5) **HDLC:** High-level Data Link Control is an International Standards Organisation data link protocol. All these **bit-oriented protocols** grew out from the original IBM SDLC (**Synchronous Data Link Control**).

HDLC is a discipline for the management of information transfer over a data communication channel. HDLC has a basic structure that governs the function and the use of control procedures.

Ques 7) Discuss HDLC? Also explain the Transfer Modes and frames types of HDLC.

Ans: HDLC

High-level Data Link Control is an International Standards Organisation data link protocol. All these **bit-oriented protocols** grew out from the original IBM SDLC (**Synchronous Data Link Control**).

HDLC is a discipline for the management of information transfer over a data communication channel. HDLC has a basic structure that governs the function and the use of control procedures.

Types of Stations

To satisfy a variety of applications, HDLC defines three types of stations. These are:

1) **Primary Station:** It has the responsibility for controlling the operation of the link. Frames issued by the primary are called **command**.

2) **Secondary Station:** It operates under the control of the primary station. Frames issued by a secondary are called **responses**. The primary maintains separate logical links with each secondary station of the line.

3) **Combined Station:** It combines the features of primary and secondary. A combined station may issue both commands and responses.

Since, HDLC has been defined as a general purpose data link control protocol. The stations can be configured in different network configurations as (all configurations are illustrated in **figure 2.17, 2.18 (a)** and **(b)**):

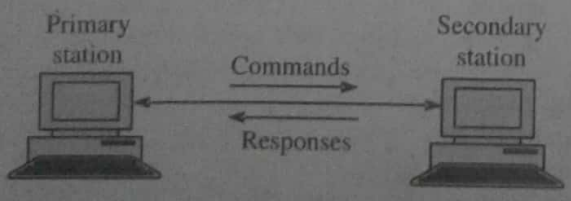
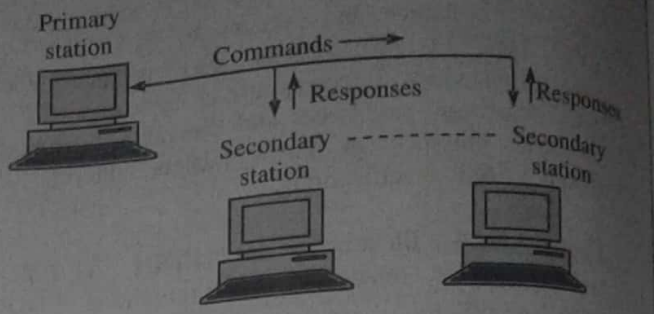
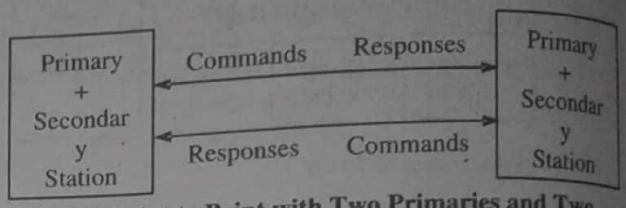


Figure 2.17: Point to Point with Single Primary and Secondary (Point-to-Point Link)



(a): Multipoint with Single Primary and Multiple Secondaries (Multipoint Link)



(b): Point to Point with Two Primaries and Two Secondaries (Point-to-Point Link between Combined Stations)

Figure 2.18

The frames sent by primary station to the secondary station are known as commands and those from the secondary to the primary as responses.

Two configurations shown in part (1) and (2) have a single primary station are known as **unbalanced configurations**. Unbalanced configuration supports both full duplex and half duplex transmission.

The configuration in part (3) has two primary stations and is known as **balanced configuration**. Balanced configuration supports both full duplex and half duplex transmission. Since each station has both a primary and a secondary, they are also known as combined stations.

Transfer Modes of HDLC

The data transfer can be in one of the following three modes:

1) **Normal Response Mode (NRM):** This mode is used in unbalanced configuration. The primary node will initiate the data transfer, but the secondary node can send data only on command from the primary node. NRM is used for communication between a host computer and the terminals connected to it.

2) **Asynchronous Balanced Mode (ABM):** This mode is used with balanced configuration. A combined node can initiate transmission. ABM is used extensively for point-to-point full-duplex communication.

3) **Asynchronous Response Mode (ARM):** This mode is used with unbalanced configuration. The primary node will have the responsibility to initiate the link, error recovery, and logical disconnection, but the secondary node may initiate data transmission without permission from the primary. ARM is rarely used.

Ques 8) Explain frames types of HDLC?
Or
What is the frame format of HDLC?

Ans: Frames Types
In HDLC both data and control messages are carried in a standard format frame. Three classes of frame are used in HDLC:

1) **Unnumbered Frames (U-Frames):** These are used for functions such as link setup and disconnection. The name derives from the fact that they do not contain any acknowledgement information, which is contained in sequence numbers.

2) **Information Frames (I-Frames):** These carry the actual information or data and are normally referred to simply as I-frames. They can be used to piggy back acknowledgement information relating to the flow of I-frames in the reverse direction when the link is being operated in ABM or ARM.

3) **Supervisory Frames (S-Frames):** These are used for error and flow control and hence contain send and receive sequence numbers.

Frame Format in HDLC
The frame format of HDLC is shown in **figure 2.19**:

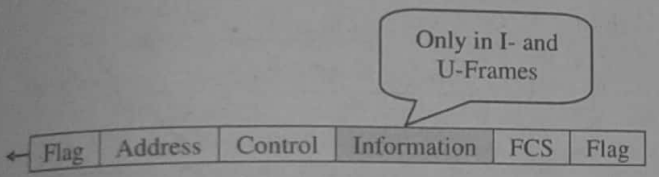


Figure 2.19: HDLC – Frame Format

The functions of each field are as follows:

1) **Flag Field:** This field of an HDLC frame is an 8-bit sequence with a bit pattern of 01111110. It identifies both the beginning and end of a frame and serves as a synchronisation pattern for the receiver.

2) **Address Field:** This field contains the address of the secondary station. If a primary station creates a frame, it contains to address. If a secondary creates the frame, it contains from address. An address field can be 1 byte or several bytes long, depending on the network. One byte of address can identify upto 128 stations.

3) **Control Field:** This field is a 1 or 2 byte segment of the frame used for flow and error control.

4) **Information Field:** This field contains the user's data from the network layer or network management information. Its length can vary from one network to another but is always fixed within each network.

5) **Frame Check Sequence (FCS):** FCS in an error detection field. It contains either a 2- or 4-byte.

Ques 9) What is the role of DLL in Internet?

Ans: Data Link Layer (DLL) in Internet
Internet consists of various "networks", i.e., they may support different network layer protocols, and even links within may be very different. A data link layer protocol for internet needs to be able to deal with these issues.

Internet connection, in practice, is built up on point-to-point links:

1) **Organisations' Routers:** They are connected to outside world's routers via point-to-point leased lines (router-router).
2) **Home Users:** They are connected to outside internet routers via cable modems and dial-up telephone lines (host-router).

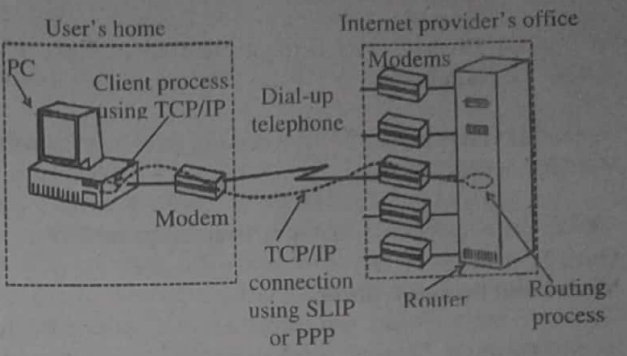


Figure 2.20

For either case of connections, some data link layer protocol is required. Internet uses the Point-to-Point Protocol (PPP) which handles error detection, supports multiple protocols, and allows IP addresses to be negotiated at connection time, permit authentication.

Two protocols used for data link layer in Internet are:
1) SLIP (Serial Line IP), and
2) PPP (Point-to-Point Protocol).

Ques 10) What is SLIP?

Ans: SLIP(Serial Line IP)
SLIP can be defined as an encapsulation method for transmitting IP packets over a serial connection. From its creation until the present time, the recommended method for implementing SLIP has remained a *de facto* standard.

The TCP/IP protocol family runs over a variety of network media – IEEE 802.3 (Ethernet) and 802.5 (token ring) LAN's, X.25 lines, satellite links, and serial lines. There are standard encapsulations for IP packets defined for many of these networks, but there is no standard for serial lines. SLIP, Serial Line IP, is currently a *de facto* standard, commonly used for point-to-point serial connections running TCP/IP. It is not an internet standard. Distribution of this memo is unlimited.

SLIP has its origins in the 3COM UNET TCP/IP implementation from the early 1980s. It is merely a packet framing protocol – SLIP defines a sequence of characters that frame IP packets on a serial line, and nothing more. It provides no addressing, packet type identification, error detection/correction or compression mechanisms. Because the protocol does so little, though, it is usually very easy to implement.

SLIP is commonly used on dedicated serial links and sometimes for dialup purposes, and is usually used with line speeds between 1200bps and 19.2Kbps. It is useful for allowing mixes of hosts and routers to communicate with one another (host-host, host-router and router-router are all common SLIP network configurations).

Data Format of SLIP

The data format of SLIP is:

Data	End Flag

A special END character (equivalent to decimal 192) marks the end of data.

Ques 11) What is PPP? What are the different layers of PPP?

Or

Discuss the operations of Point-to-point protocol?

Ans: Point-to-Point Protocol

PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP is widely used, especially in the analog modem access to the ISP, where one end is the PC and the other end is the ISP router. The functions performed are:

1) The Point-to-Point Protocol (PPP) was designed to transport multi-protocol packets between two peers connected by simple links.
2) These links provide full-duplex simultaneous bi-directional operation.

PPP Operation

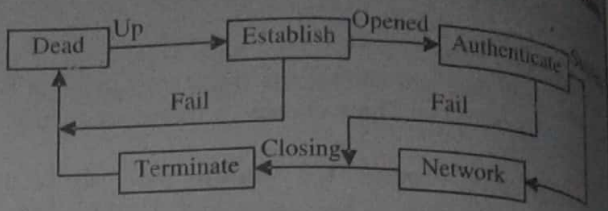
The operation of PPP is as follows:

Step 1: Before the two ends can start sending data packets, each end of the PPP link must first send LCP packets to configure and test the data link.

Step 2: Once the link has been established, the peer may be authenticated. Then, PPP must send NCP packets to choose and configure one or more network-layer protocols.

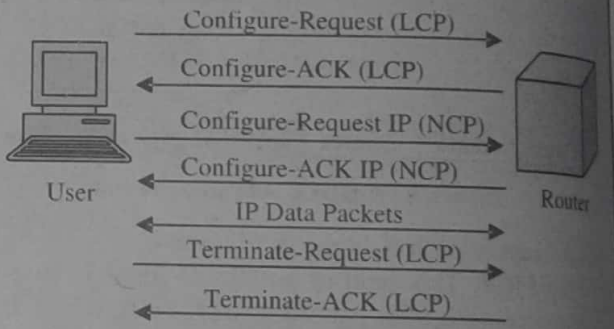
Step 3: Once each of the chosen network-layer protocols has been configured, datagrams from each network-layer protocol can be sent over the link. The link will remain configured for communications until explicit LCP or NCP packets close the link down, or until some external event occurs (e.g., an inactivity timer expires or network administrator intervention).

Step 4: In the process of configuring, maintaining and terminating the point-to-point link, the PPP link goes through several distinct phases which are specified in the following simplified **state diagram**.



The link begins with Link-**Dead state**. When the physical layer is ready for communication (e.g., two analog modems are connected to each other), PPP will proceed to the Link **Establishment state**. The LCP is used to establish the connection through an exchange of Configure packets. When this is completed, it enters the LCP Opened state. Once the Opened state is reached, the two peers may authenticate the other. If authentication is successful, each network-layer protocol must be configured separately by the appropriate NCP.

Step 5: When these are done, the two ends can begin sending packets. PPP can terminate the link at any time. Either LCP or NCP can be used to close the link. The sequence of the PPP operation is illustrated in the following:



Ques 12) What is the frame format of PPP?

Ans: PPP Frame Format

Figure 2.21 shows the format of a PPP frame:

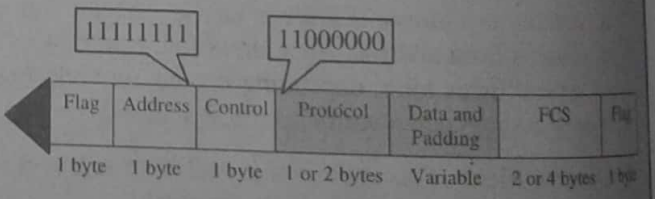


Figure 2.21: PPP Frame

The descriptions of the fields are as follows:

1) **Flag Field:** This field, like the one in HDLC, identifies the boundaries of a PPP frame. Its value is 01111110.

2) **Address Field:** Because PPP is used for a point-to-point connection; it uses the broadcast address of HDLC, 11111111, to avoid a data link address in the protocol.

3) **Control Field:** This field uses the format of the U-frame in HDLC. The value is 11000000 to show that the frame does not contain any sequence numbers and that there is no flow and error control.

4) **Protocol Field:** This field defines what is being carried in the data field – user data or other information.

5) **Data Field:** This field carries either the user data or other information.

6) **FCS:** The frame check sequence field, as in HDLC, is simply a two-byte or four-byte CRC.

MEDIUM ACCESS CONTROL (MAC) SUBLAYER

Ques 13) What is MAC (Medium Access Control) sub layer? Explain its features.

Ans: MAC (Medium Access Control) Sub Layer

This layer is basically dedicated to the broadcast networks. Broadcast networks are also referred to as multi-access channel or random access channel.

Protocols used to determine who goes next on a multi access channel belong to sub-layer of the data link layer called the MAC.

Medium Access Control (MAC) protocol is used to provide the basic functionality of data link layer of the Ethernet LAN system. MAC sub-layer is mainly concerned with media access strategies and is different for different LANs. It supports different types of transmission media at different data rates.

The MAC sub-layer accepts data from the Logical Link Control Layer (LLC), calculates a cyclic redundancy checks (CRC), and then transmits the encapsulated frames. The transmitting media access management procedure sends the serial bit stream to the physical layer, which listens to the media.

It halts the transmission if it senses a collision and tries to re-transmit it, and at the same time it sends a jam signal over the media.

Its location in OSI model is shown in **figure 2.22**.

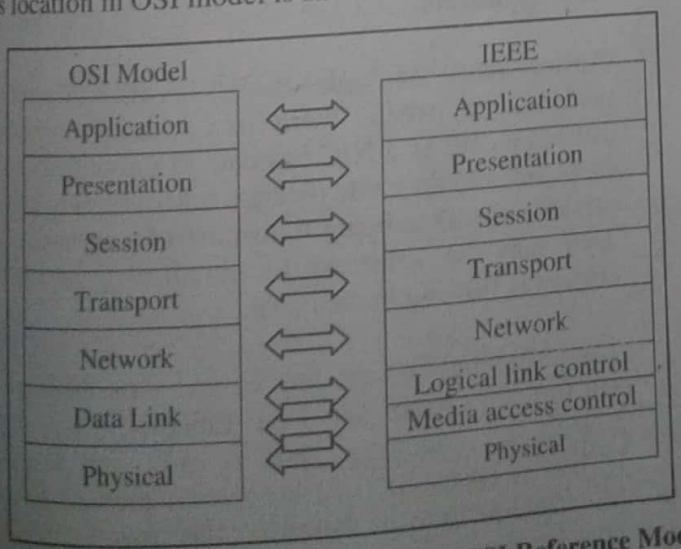


Figure 2.22: IEEE Model differs from the OSI Reference Model

Features of MAC/LLC

1) Controls the access to the shared channel in autonomous DTEs.
2) Provides a scheme that reduces a LANS susceptibility to errors.
3) Provides a more compatible interface with WANS, since the LLC is a subset of the equivalent portion of the WAN standard.
4) The LLC is independent of access method, whereas MAC is protocol specific. This gives the 802 network a flexible interface into and out of the LAN.

Ques 14) What is the structure of MAC?

Ans: Structure of MAC

The structure of MAC is divided into **preamble, header** and **CRC (cyclic redundancy check).**

1) **Preamble:** The purpose of the idle time before transmission starts is to allow a small time interval for the receiver electronics in each of the nodes to settle after completion of the previous frame.

   A node starts transmission by sending an 8 byte (64 bit) preamble sequence. This consists of 62 alternating 1's and 0's followed by the pattern 11.

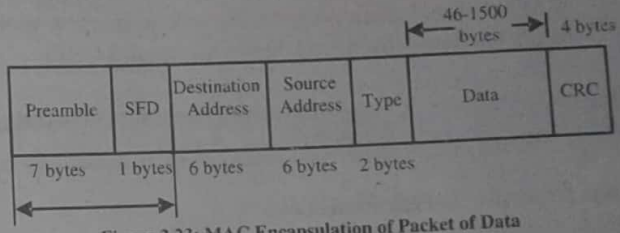


Figure 2.23: MAC Encapsulation of Packet of Data

   The last byte, which finished with the '11', is known as the **"Start of Frame Delimiter" (SFD).** It warns the station or stations that this is the last chance for synchronisation. When encoded using Manchester encoding, at 10 Mbps, the 62 alternating bits produce a 5 MHz square wave.

   The purpose of the preamble is to allow time for the receiver in each node to achieve lock of the receiver Digital Phase Lock Loop which is used to synchronise the receive data clock to the transmit data clock. At the point when the first bit of the preamble is received, each receiver may be in an arbitrary state (i.e. have an arbitrary phase for its local clock).

   During the course of the preamble it learns the correct phase, but in so doing it may miss (or gain) a number of bits. A special pattern (11) is therefore used to mark the last two bits of the preamble. When this is received, the Ethernet receive interface starts collecting the bits into bytes for processing by the MAC layer.

2) **Header:** The header consists of three parts:
   i) **Destination Address:** A 6-byte destination address, which specifies a single recipient node

(unicast mode), a group of recipient nodes (multicast mode), or the set of all recipient nodes (broadcast mode).

ii) **Source Address:** A 6-byte source address, which is set to the sender's globally unique node address. This may be used by the network layer protocol to identify the sender, but usually other mechanisms are used. Its main function is to allow address learning, which may be used to configure the filter tables in a bridge.

iii) **Type:** A 2-byte type field, which provides a Service Access Point (SAP) to identify the type of protocol being carried (e.g. the values 0x0800 is used to identify the IP network protocol, other values are used to indicate other network layer protocols). In the case of IEEE 802.3 LLC, this may also be used to indicate the length of the data part.

3) **Cyclic Redundancy Check (CRC):** The 32-bit CRC added at the end of the frame provides error detection in the case where line errors (or transmission collisions in Ethernet) result in corruption of the MAC frame. Any frame with an invalid CRC is discarded by the MAC receiver without further processing. The MAC protocol does not provide any indication that a frame has been discarded due to an invalid CRC.

Ques 15) Define the various multiple access control protocols.

Ans: Multiple Access Protocols

Many algorithms for allocating a multiple access channel are known. Protocols which are used in allocating a multiple access channel are given below:

1) **ALOHA:** "ALOHA refers to a simple communications scheme in which each source (transmitter) in a network sends data whenever there is a frame to send." If the frame successfully reaches the destination (receiver), the next frame is sent. If the frame fails to be received at the destination, it is sent again.

ALOHA protocol is a main **contention protocol** (Access to the medium from many entry points is called **contention**. It is controlled with a contention protocol).

In a wireless broadcast system or a half-duplex two-way link, ALOHA works perfectly. But as networks become more complex **for example**, in an Ethernet system involving multiple sources and destinations in which data travels many paths at once, trouble occurs because data frames collide (conflict).

The heavier the communications volume, the worse the collision problems become. The result is degradation of system efficiency, because when two frames collide, the data contained in both frames is lost.

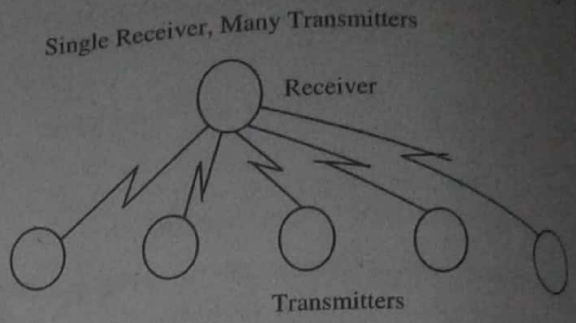


Figure 2.24: Satellite System, Wireless (ALOHA Protocol)

To minimise the number of collisions, thereby optimising network efficiency and increasing the number of subscribers that can use a given network, a scheme called slotted ALOHA was developed.

This system employs signals called **beacons** that are sent at precise intervals and tell each source when the channel is clear to send a frame. Further improvement can be realised by a more sophisticated protocol called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

2) **Carrier Sense Multiple Access (CSMA):** "**Carrier Sense**" describes the fact that a transmitter listens for a carrier wave before trying to send. That is, it tries to detect the presence of an encoded signal from another station before attempting to transmit.

If a carrier is sensed, the station waits for the transmission in progress to finish before initiating its own transmission.

"**Multiple Access**" describes the fact that multiple stations send and receive on the medium. Transmissions by one node are generally received by all other stations using the medium.

Working of Carrier Sense Multiple Access (CSMA)

Protocols in which stations listen for a carrier (i.e., a transmission) and act accordingly are called **carrier sense protocols**.

Carrier Sense Multiple Access (CSMA) improves performance when there is a higher medium utilisation. When a NIC has data to transmit, the NIC first listens to the cable (using a transceiver) to see if a carrier (signal) is being transmitted by another node. This may be achieved by monitoring whether a current is flowing in the cable.

The individual bits are sent by encoding them with a 10 (or 100 MHz for Fast Ethernet) clock using Manchester encoding. Data is only sent when no carrier is observed (i.e., no current present) and the physical medium is therefore idle. Any NIC, which does not need to transmit, listens to see if other NICs have started to transmit information to it.

However, this alone is unable to prevent two NICs transmitting at the same time. If two NICs simultaneously try transmitting, then both could see an idle physical medium (i.e. neither will see the other's carrier signal), and both will conclude that no other NIC is currently using the medium. In this case, both will then decide to transmit and a collision will occur. The collision will result in the corruption of the frame being sent, which will subsequently be discarded by the receiver since a corrupted Ethernet frame will (with a very high probability) not have a valid 32-bit MAC CRC at the end.

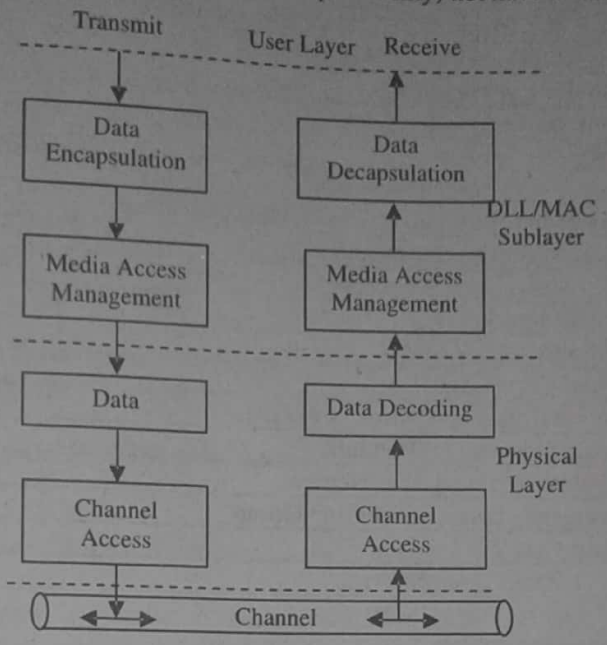


Figure 2.25: CSMA/CD Layers (IEEE 802.3)

IEEE 802 FOR LANS & MANS

Ques 16) Write a note on LAN/MAN standards.

Ans: LAN/MAN Standards

The IEEE 802 LAN/MAN Standards Committee develops LAN standards and MAN standards. The most widely used standards are for the Ethernet family, token ring, WLAN, Bridging, and Virtual Bridged LANs. All standards created by this committee are designated 802.

The "80" in 802 refers to the year the committee was formed and the "2" refers to the month in which the committee was formed. Working groups and technical advisory groups within the committee are designated by a dot-number (.#), to define the sub-technology for which they are responsible. **For example,** standards listed 802.11 designate the WLAN working Group within the LAN/MAN Standards Committee. Letters after the designations represent revisions or changes to the original standards for the working group. These groups meet several times a year to discuss new trends within their industry or to continue the process of refining a current standard.

Table 2.2 shows a fairly complete list of the IEEE 802 LAN and MAN standards relevant to supporting the TCP/IP protocols, as of mid-2011.

Table 2.2: IEEE 802 LAN and MAN standards

IEEE 802.1	Higher Layer LAN Protocols (Bridging)
IEEE 802.2	LLC
IEEE 802.3	Ethernet
IEEE 802.4	Token bus
IEEE 802.5	Token ring MAC layer
IEEE 802.6	MANs (DQDB)
IEEE 802.7	Broadband LAN using Coaxial Cable
IEEE 802.8	Fiber Optic TAG
IEEE 802.9	Integrated Services LAN
IEEE 802.10	Interoperable LAN Security

IEEE 802.11	Wireless LAN (WLAN) & Mesh (Wi-Fi certification)
IEEE 802.12	100BaseVG
IEEE 802.13	Unused
IEEE 802.14	Cable modems
IEEE 802.15	Wireless PAN
IEEE 802.15.1	Bluetooth certification
IEEE 802.15.2	IEEE 802.15 and IEEE 802.11 coexistence
IEEE 802.15.3	High-Rate wireless PAN (e.g., UWB, etc.)
IEEE 802.15.4	Low-Rate wireless PAN
IEEE 802.15.5	Mesh networking for WPAN
IEEE 802.15.6	Body area network
IEEE 802.15.7	Visible light communications
IEEE 802.16	Broadband Wireless Access (WiMAX certification)
IEEE 802.16.1	Local Multipoint Distribution Service
IEEE 802.16.2	Coexistence wireless access
IEEE 802.17	Resilient packet ring
IEEE 802.18	Radio Regulatory TAG
IEEE 802.19	Coexistence TAG
IEEE 802.20	Mobile Broadband Wireless Access
IEEE 802.21	Media Independent Handoff
IEEE 802.22	Wireless Regional Area Network
IEEE 802.23	Emergency Services Working Group
IEEE 802.24	Smart Grid TAG
IEEE 802.25	Omni-Range Area Network

Ques 17) Discuss IEEE 802.3 standard in detail.

Or

What is ethernet? What is the frame format of ethernet?

Or

What are the advantages and disadvantages of ethernet?

Ans: IEEE 802.3 Standard: Ethernet

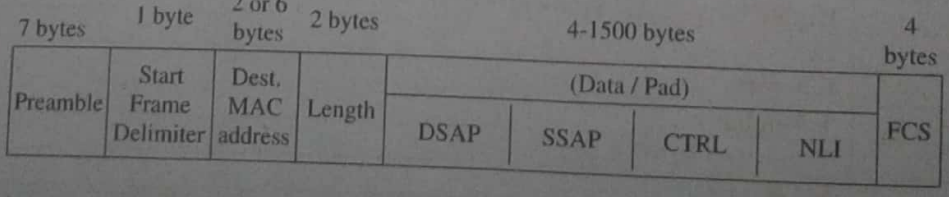
Ethernet is the most popular physical layer LAN technology in use today. Ethernet was invented by engineer **Robert Metcalfe**. It defines the number of conductors that are required for a connection, the performance thresholds that can be expected, and provides the framework for data transmission. A standard Ethernet network can transmit data at a rate up to 10 Megabits per second (10 Mbps).

Ethernet is popular because it strikes a good balance between speed, cost and ease of installation. These benefits, combined with wide acceptance in the computer marketplace and the ability to support virtually all popular network protocols, make Ethernet an ideal networking technology for most computer users today.

The Institute for Electrical and Electronic Engineers developed an Ethernet standard known as **IEEE Standard 802.3**. This standard defines rules for configuring an Ethernet network and also specifies how the elements in an Ethernet network interact with one another. By adhering to the IEEE standard, network equipment and network protocols can communicate efficiently.

Frame Format of Ethernet

The frame format of Ethernet is given below:



1) **Preamble:** This is a stream of bits used to allow the transmitter and receiver to synchronize their communication. The preamble is an alternating pattern of binary 56 ones and zeroes.

2) **Start Frame Delimiter:** This is always 10101011 and is used to indicate the beginning of the frame information.

3) **Destination MAC: This** is the MAC address of the machine receiving data. When a network interface card (NIC) is listening to the wire is checking this field for it's own MAC address.

4) **Source MAC: This** is the MAC address of the machine transmitting data.

5) **Length: This** is the length of the entire Ethernet frame in bytes. Although this field can hold any value between 0 and 65,534, it is rarely larger than 1500 as that is usually the maximum transmission frame size for most serial connections. Ethernet networks tend to use serial devices to access the Internet.

6) **Data/Padding (Payload):** The data is inserted here. This is where the IP header and data is placed if you are running IP over Ethernet. This field contains IPX information if you are running IPX/SPX (Novell). Contained within the data/padding section of an IEEE 803.2 frame are four specific fields:
   i) **DSAP** - Destination Service Access Point
   ii) **SSAP** - Source Service Access Point
   iii) **CTRL** - Control bits for Ethernet communication
   iv) **NLI** - Network Layer Interface

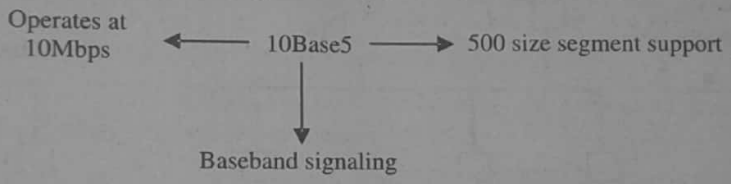
7) **FCS:** This field contains the Frame Check Sequence (FCS) which is calculated using a Cyclic Redundancy Check (CRC). The FCS allows Ethernet to detect errors in the Ethernet frame and reject the frame if it appears damaged.

Ques 18) What are the standard ethernet? Discuss them.

Ans: Standard Ethernet

Standard Ethernet comes in four incarnations, depending on the type of cable used to string the network together as shown below:

1) **10Base5:** 10Base5 cabling is popularly called thick Ethernet. The notation 10Base5 means that it operates at 10Mbps, uses baseband signaling, and can support segments of upto 500 meters. The first number is the speed in Mbps.



Then comes the word "Base" (or sometimes "BASE") to indicate baseband transmission. There used to be a broadband variant.

2) **10Base2:** 10Base2, or thin Ethernet, bends easily. Thin Ethernet is much cheaper and easier to install, but it can run for only 185 meters per segment, each of which can handle only 30 machines.

3) **10Base-T:** 10Base3 problems associated with finding cable breaks drove systems toward a different kind of wiring pattern, in which all stations have a cable running to a central hub in which they are all connected electrically (as if they were soldered together). Usually, these wires are telephone company twisted pairs, since most office buildings are already wired this way, and normally plenty of spare pairs are available. This scheme is called 10Base-T. Hubs do not buffer incoming traffic (**figure 2.26**).

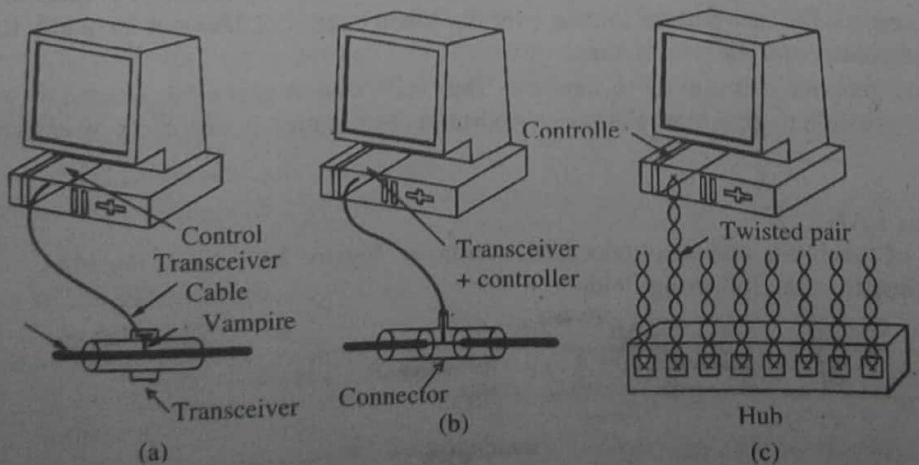


Figure 2.26: Three Kinds of Ethernet Cabling (a) 10Base5 (b) 10Base2 (c) 10Base-T

4) **10Base-F:** A fourth cabling option for Ethernet is 10Base-F, which uses fiber optics. This alternative is expensive due to the cost of the connectors and terminators, but it has excellent noise immunity and is the method of choice when running between buildings or widely-separated hubs. Runs of upto km are allowed. It also offers good security since wiretapping fiber is much more difficult than wiretapping copper wire.

Ques 19) Discuss IEEE 802.4 standard in detail.

Or

Ques 20) What is token bus LAN? What is the frame format of token bus LAN?

Ans: IEEE 802.4 Standard: Token Bus

A type of local-area network (LAN) that has a bus topology, in which all devices are connected to a central cable, called the **bus** or **backbone** and uses a token -passing mechanism to regulate traffic on the bus. Ethernet systems use a bus topology.

A token bus network is very similar to a token ring network, the main difference being that the endpoints of the bus do not meet to form a physical ring. The IEEE 802.4 standard defines **token bus networks**.

Token bus local area network was designed for production lines with the objective of realizing guaranteed response time. It is very similar to token ring local area network in operation. The physical topology of the network is bus but the stations are connected in a **logical ring topology (figure 2.27)**.

The logical topology follows the address hierarchy with the station with lowest address connected to the station with the highest address. Each station knows the identity of the preceding station and the succeeding station. There is no relation between the physical location of a station on the bus to its address.

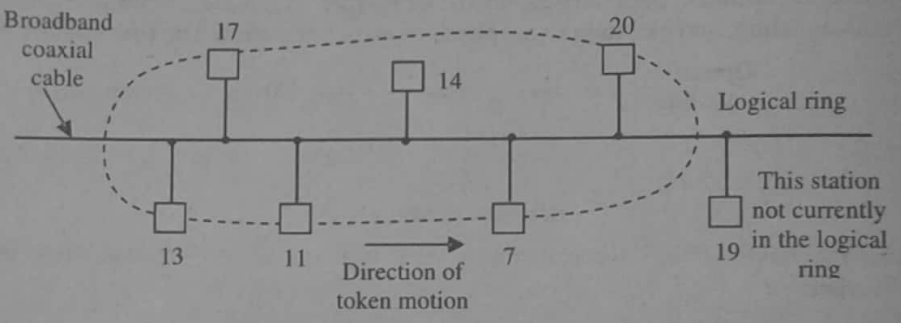


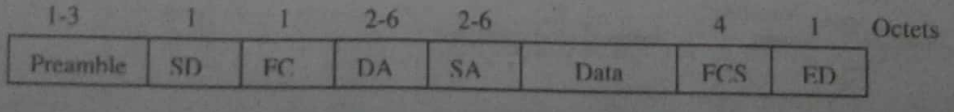
Figure 2.27: Token Bus

The basic operation of a token bus LAN in as follows:

1) The access to the interconnecting bus is regulated by a token. At any time, only the station that hold the token has the right to transmit its data frames on the bus. Each frame carries source and destination addresses. A station may send one or more frames while it is holding the token.
2) All stations are ready to receive frames at any time except when holding a token.
3) The token must be released before timeout with the address of the next station in the sequence.
4) The released token is taken over by the station whose address is on the token. To maintain continuity of communication, it is necessary for each station to take over the token even if it does not have any frames to send. It can release the token immediately for the next station.
5) In one cycle, each station gets one opportunity to transmit. Thus each station gets a fair chance to send its frames in round robin fashion. It is possible to give more than one opportunity to a station in one cycle by assigning it more than one address to it.

Frame Format of Token Bus LAN

IEEE 802.4 MAC sub layer of token bus operates under LLC sub layer. **Figure 2.28** shows the MAC frame structure as specified in IEEE 802.4. It consists of the following fields:



SD: Frame Start Delimiter
FC: Frame Control (type)
DA: Destination Address
SA: Source address
FCS: Frame Check Sequence
ED: End Delimiter

Figure 2.28: Format of IEEE 802.4 Frame

1) **Preamble:** The preamble is 1 to 3 octets long pattern. It enables bit synchronization.
2) **Start Delimiter (SD):** It is one octet long unique bit pattern which marks the start of the frame. As in token ring, SD contains non-data codes for identification.
3) **Frame Control (FC):** The frame control field indicates type of the frame—data frame or control frame. The token frame is one of the control frames. **Figure 2.29** lists the FC field of various types of frames. The functions of various frames are described later. This field is one octet long.

	1	2	3	4	5	6	7	8
(a) Claim - Token	0	0	0	0	0	0	0	0
(b) Solicit – Successor-1	0	0	0	0	0	0	0	1
(c) Solicit – Successor-2	0	0	0	0	0	0	1	0
(d) Who - Follows	0	0	0	0	0	0	1	1
(e) Resolve - Contention	0	0	0	0	0	1	0	0
(f) Token	0	0	0	0	1	0	0	0
(g) Set - Successor	0	0	0	0	1	1	0	0
(h) Data Frame	0	1	M	M	M	P	P	P
(i) Station Management	1	0	M	M	M	P	P	P

Figure 2.29: FC Field of IEEE 802.4

4) **Destination Address (DA):** The destination address field is 6 octets long.
5) **Source Address (SA):** The source address field is 6 octets long. As before the destination and source address fields can be 2 octets long but 2-octet long addresses are seldom used.
6) **Data:** Data field contains the LLC frame. Maximum size of the MAC frame excluding SD/ED fields should not exceed is 8191 octets.
7) **Frame Check Sequence (FCS):** Frame check sequence is 4 octets long and contains CRC. It checks on DA, SA, FC, and data fields.
8) **End Delimiter:** It is unique bit pattern which marks the end of the frame. It is one octet long. As in token ring, ED contains non-data codes for identification.

Ques 21) What are the advantages and disadvantages of token bus?

Ans: Advantage of Token Bus
1) The cabling cost is less as the bus topology requires the least amount of cable to connect the computers.
2) The bus topology is easy to understand, install and use for small networks.
3) Bus topology is easy to expand by joining two cables with a BNC barrel connector.
4) In the expansion of a bus topology repeaters can be used to boost the signal and increase the distance.

Disadvantages of Token Bus
1) The BNC connectors used for expansion of the bus attenuates the signal considerably.
2) Heavy network traffic slows down the bus speed.
3) A cable break of loose BNC connector will cause reflections and bring down the whole network causing all network activity to stop.

Ques 22) Discuss IEEE 802.5 standard in detail.

Or

What is token ring? What is the frame format of token ring?

Ans: IEEE 802.5 Standard: Token Ring

Token ring is the IEEE 802.5 standard for a token-passing ring in communication networks with a star-configured physical topology. Internally, signals travel around the Communication network from one station to the next in a ring. Physically, each station connects to a central hub called a MAU (multistation access unit).

A Token Ring network is a local area network (LAN) in which all computers are connected in a ring or star topology and a bit- or token-passing scheme is used in order to prevent the collision of data between two computers that want to send messages at the same time. The Token Ring protocol is the second most widely-used protocol on local area networks after Ethernet.

IEEE 802.5 Token Ring technology provides for data transfer rates of either 4 or 16 megabits per second. Token-passing networks move a small frame, called a token, around the network. Possession of the token grants the right to transmit. If a node receiving the token has no information to send, it seizes the token, alters 1 bit of the token (which turns the token into a start-of-frame sequence), appends the information that it wants to transmit, and sends this information to the next station on the ring.

While the information frame is circling the ring, no token is on the network, which means that other stations wanting to transmit must wait. Therefore, collisions cannot occur in Token Ring networks.

Frame Format of Token Ring

Token ring and IEEE 802.5 support two basic frame types: tokens and data/command frames. Tokens are 3 bytes in length and consist of a start delimiter, an access control byte, and an end delimiter. Data/command frames vary in size, depending on the size of the Information field. Data frames carry information for upper-layer protocols, while command frames contain control information and have no data for upper-layer protocols. Both formats are shown in **figure 2.30**.

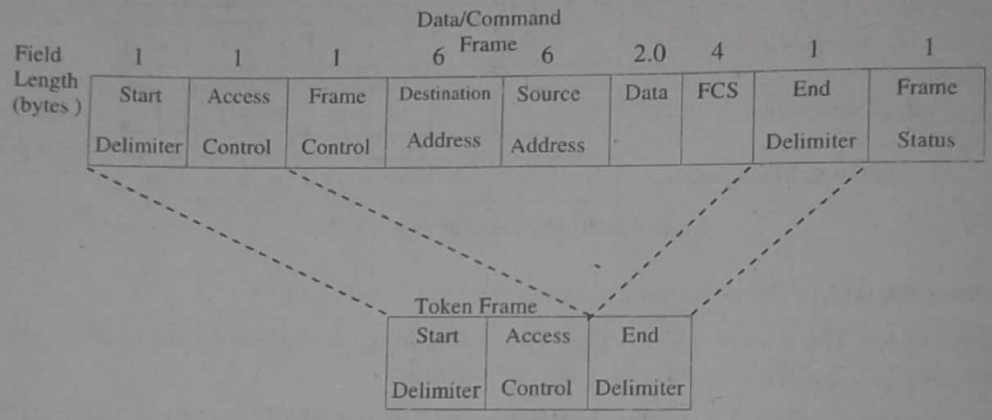


Figure 2.30: IEEE 802.5 and Token Ring Specify Tokens and Data/Command Frames

1) **Token Frame Fields:** The three token frame fields illustrated in Figure are summarized in the descriptions that follow:
   i) **Start Delimiter:** It alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.
   ii) **Access-control Byte:** It contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).
   iii) **End Delimiter:** It signals the end of the token or data/command frame. This field also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.
2) **Data/Command Frame Fields:** Data/command frames have the same three fields as Token Frames, plus several others. The Data/command frame fields illustrated in **figure 2.30** are described in the following summaries:
   i) **Start Delimiter:** Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.
   ii) **Access-Control Byte:** Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).
   iii) **Frame-Control Bytes:** Indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.
   iv) **Destination and Source Addresses:** Consists of two 6-byte address fields that identify the destination and source station addresses.
   v) **Data:** Indicates that the length of field is limited by the ring token holding time, which defines the maximum time a station can hold the token.

vi) **Frame-Check Sequence (FCS):** It is filed by the source station with a calculated value dependent on the frame contents. The destination station recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.

vii) **End Delimiter:** It signals the end of the token or data/command frame. The end delimiter also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.

viii) **Frame Status:** It is a 1-byte field terminating a command/data frame. The Frame Status field includes the address-recognised indicator and frame-copied indicator.

Ques 23) Discuss the working of token ring?

Ans: Working of Token Ring

The workings of token ring are as below:

1) Empty information frames are continuously circulated on the ring.
2) When a computer has a message to send, it inserts a token in an empty frame (this may consist of simply changing a 0 to a 1 in the token bit part of the frame) and inserts a message and a destination identifier in the frame.
3) The frame is then examined by each successive workstation. If the workstation sees that it is the destination for the message, it copies the message from the frame and changes the token back to 0.
4) When the frame gets back to the originator, it sees that the token has been changed to 0 and that the message has been copied and received. It removes the message from the frame.
5) The frame continues to circulate as an "empty" frame, ready to be taken by a workstation when it has a message to send.

Ques 24) What is the advantages and disadvantages of token ring?

Ans: Advantages of Token Ring

1) Simple engineering because it is point-to-point digital – no analog.
2) Easy detection and correction of cable failures.
3) No padding of data required in frame, so frames are short.
4) Excellent performance under conditions of heavy load.
5) Since rings can be bridged by their wiring concentrators into what is effectively one ring, ring size has no practical limit.

Disadvantages of Token Ring

1) Necessity of having a monitor function.
2) Under conditions of low load, substantial delay waiting for token to come around, even though network is idle.
3) Can require significantly more wire to be run than bus architecture.

Ques 25) What is difference between ethernet, token bus and token ring?

Ans: Comparison between 802.3, 802.4 and 802.5 Standards

802.3 (Ethernet)	802.4 (Token Bus)	802.5 (Token Ring)
Broadcast	Broadcast	Store and forward
Simple and robust protocol	Protocol not as simple as Ethernet	Protocol is somewhat complex
Low delays at low load	Finite delays at low load	Finite delays at low load
Delays increase exponentially at high load	Delays at high load are high, but are predictable	Delays at high load are high, but are predictable
No priorities	Priorities handled	Priorities handled
Size of the frame format is 1572 bytes	Size of the frame format is 8202 bytes	Variable size
Minimum frame required is 64 bytes	It can handle short minimum frames	It supports short minimum frames
Modems are not required	Modems are required	Modems are required

Ques 26) What are bridges? Discuss its types.

Ans: Bridges

A bridge is also a device which **works in the Data Link Layer**, but is more primitive when compared to a switch. Initial bridges were used to connect only 2 LAN's, but the most recent ones perform similar operation as the switches. It also works on the principle of transfer of information using the MAC addresses of the ports.

It can be noted is that the normal ADSL modem can be connected via bridging also. The only difference is that, when bridging is used, each time the device has to be connected to the internet, it has to dial to the internet and establish a connection.

Also, a bridge alone cannot be used to connect to the internet, because, the bridge works in the Data Link Layer, and has no knowledge of the IP Addresses, which are used in the Internet.

A bridge is used to connect the roads across a river or valley, so using bridge automobiles can continue the driving from one side to another. Similarly, in computer network, bridge also solves the same purpose.

Here bridges connect two or more networks (LANs). In case of computer network data travels from one network to other.

Bridges also filter the traffic. It divides the LAN into segment to reduce the amount of traffic.

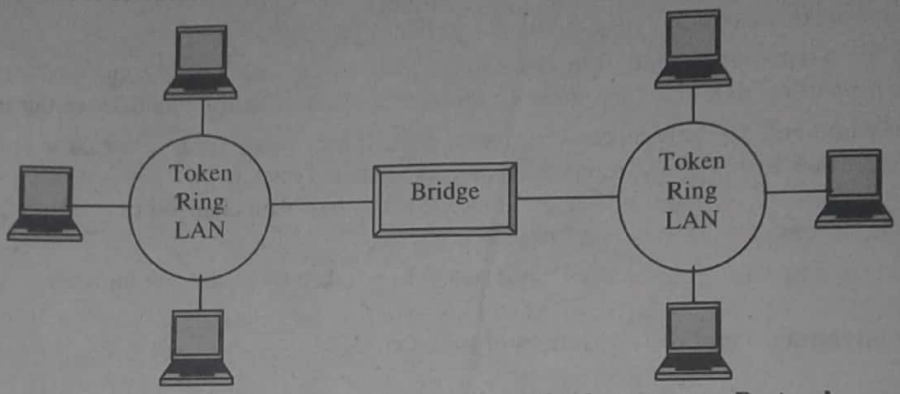


Figure 2.31: Bridges Connect Networks that use same Protocols

Incoming traffic are inspects by the bridges to decide whether data are forwarded or discarded. **For example,** each Ethernet frames (it contains source and destination MAC addresses) are inspects by the Ethernet Bridge to decide whether frames are forwarded or not.

Sometimes switches are also known as multiport bridges because traditional bridges support only one network boundary whereas switches provides four or more than four ports.

Types of Bridges

1) **Transparent Bridges:** Hardware network address (contains unique address) are used by the transparent bridges to identify that which data is to be passed and which to filter.

   A table is used to store the port information so when data is received then the stores table is used to compare against the destination address.

2) **Source-Route Bridges:** Generally source-route bridges are used by ring networks. They do not use the MAC address for the identification while they used the token ring frame's information for the identification (whether to pass the data or not).

3) **Translational Bridges:** To connect the dissimilar networks together, translational bridges are used. They have port for the various kinds of networks and the process used to pass the data depends on the connected networks.

   They consider the media access method to handle the conversation of the frame from the one type to another.

Ques 27) What are switches?

Ans: Switches

A switch is an intelligent device that **works in the data link layer**. The term intelligent refers to the decision making capacity of the Switch. Since it works in the Data link layer, it has knowledge of the MAC addresses of the ports in the network.

The digital switch is the heart (core) of the modern network system which provides a transparent signal path between any pair of attached devices. This connection allows full duplex transmissions.

The network interface stands for the functions and hardware required for connecting digital devices to the network. Digital switches are thus, single circuit-switching nodes.

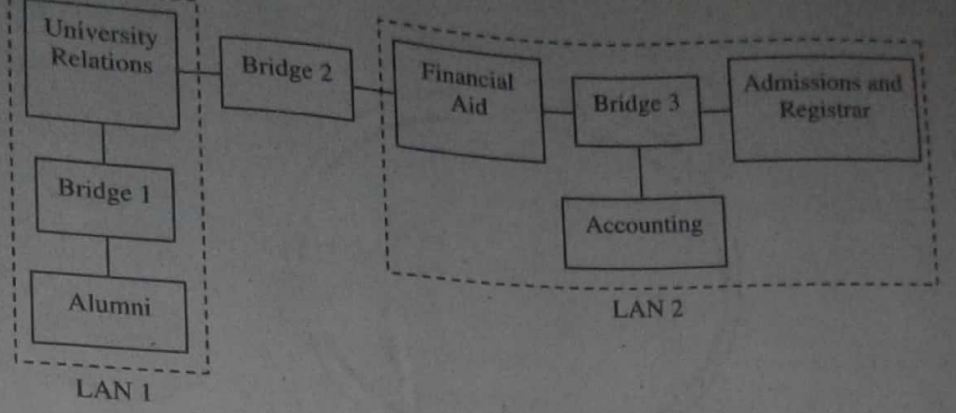


Figure 2.32: Bridges Connecting LANs with Frequent Traffic

In networks connected to a hub, scalability and latency problems occur. A switch provides an answer to this problem by ensuring growth without jeopardising performance. The switch connects two or more devices on the network and allows smooth communication between nodes.

Switches are executed in hardware and also software and as a result all connections operate simultaneously making the operations fast. Computers connected to a switch or hubs have no competition for bandwidth.

But there is one difference, the collisions and network failure are less in devices connected to a switch as they use full bandwidth compared to a hub where devices need to share the bandwidth with every device on the hub.

Ques 28) What do you understand by High Speed LANS?

Or

What is Fast and gigabit ethernet?

Or

What is FDDI?

Ans: High Speed LANS

For high speed and long distance LANS, fiber optics or highly parallel copper networks are used. Fiber have high bandwidth, is thin and light weight is not affected by electromagnetic interference from heavy machinery, power surges and have excellent security. Hence fast LANS use fiber.

Some of the common high speed LANS are:

1) **FDDI:** FDDI (Fiber Distributed Data Interface) is a set of ANSI and ISO standards for data transmission on fiber optic lines in a local area network (LAN) that can extend in range up to 200 km (124 miles). The FDDI protocol is based on the token ring protocol.

   In addition to being large geographically, an FDDI local area network can support thousands of users. FDDI is frequently used on the backbone for a wide area network (WAN).

   An FDDI network contains two token rings, one for possible backup in case the primary ring fails. The primary ring offers up to 100 Mbps capacity. If the secondary ring is not needed for backup, it can also carry data, extending capacity to 200 Mbps. The single ring can extend the maximum distance; a dual ring can extend 100 km (62 miles).

   FDDI was developed by the **American National Standards Institute** (ANSI) X3T9.5 standards committee in th mid-1980s. At the time, high-speed engineering workstations were beginning to tax the bandwidth of existing loca area networks (LANs) based on Ethernet and token ring.

   A new LAN media was needed that could easily support these workstations and their new distributed applications. the same time, network reliability had become an increasingly important issue as system managers migrated missio critical applications from large computers to networks. FDDI was developed to fill these needs.

   After completing the FDDI specification, ANSI submitted FDDI to the International Organisation for Standardisa (ISO), which created an international version of FDDI that is completely compatible with the ANSI standard versio

   Figure 2.33 the counter-rotating primary and secondary FDDI rings.

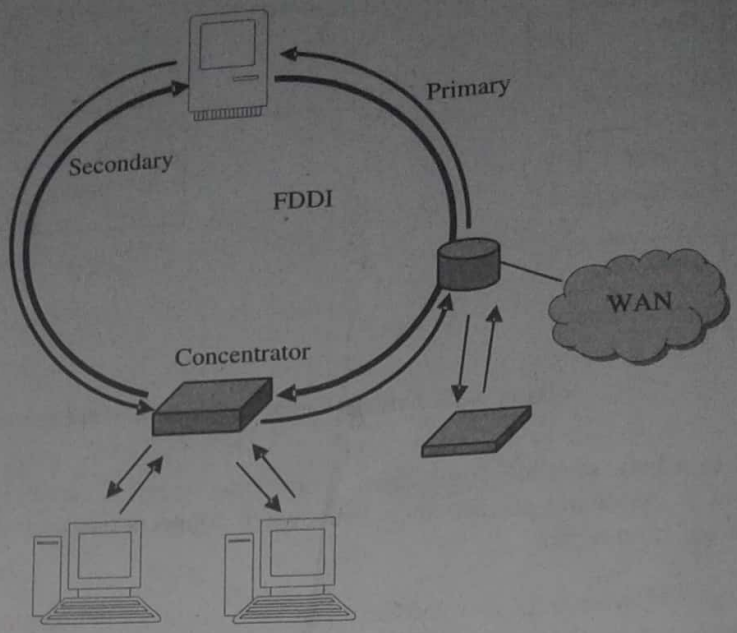


Figure 2.33: FDDI Uses Counter-Rotating Primary and Secondary Rings

2) **Fast Ethernet:** In computer networking, fast Ethernet is a collective term for a number of Ethernet standards that carry traffic at the nominal rate of 100 Mbit/s, against the original ethernet speed of 10 Mbit/s. Of the 100 megabit ethernet standards 100baseTX (T = "Twisted" Pair Copper) is by far the most common and is supported by the vast majority of Ethernet hardware currently produced.

   All fast ethernet uses hub in place of multi-hop cables or BNC connectors, also special category wires are used, generally a category-3 or category-5 twisted pair wires are used.

   Two kinds of hubs are possible a shared hub and a switched hub. In a shared hub, all incoming lines are logically connected forming a single collision domain. Only one station at a time can be transmitting. In a switched hub, each incoming frame is buffered on a plug-in-line card. All stations can transmit at the same time thus providing the bandwidth of the system.

   Fast ethernet are employed in high speed local area network and are comparable to FDDI local area networks.

   Fast Ethernet Cabling

   Different cable standards for fast ethernet cabling are mentioned below:

   i) **100BASE-T4:** Category 3 UTP cables can be used for 100BASE-T4. Its signaling speed is 25 MHz. To achieve necessary bandwidth, 100 BASE T4 requires four twisted pairs if Manchester encoding is used.

   ii) **100BASE-TX:** For 100BASE-TX category 5 wiring is used. Its signaling speed is 125 MHz. For Manchester encoding only two twisted pairs per stations are used. 100BASE-TX is a full duplex system.

   iii) **100BASE-FX:** 100BASE-FX uses two strands of multimode fiber. It is a full duplex system. The distance between a station and the hub can be upto 2 km.

3) **Gigabit Ethernet:** Gigabit Ethernet is expected to be deployed as a backbone in existing networks. It can be used to aggregate traffic between clients and "server farms" and for connecting Fast Ethernet switches. It can also be used for connecting workstations and servers for high – bandwidth applications such as medical imaging or CAD.

   Gigabit Ethernet is the third generation Ethernet technology offering a speed of 1000Mbps.

   It is fully compatible with existing Ethernets and promises to offer seamless migration to higher speeds. Existing networks will be able to upgrade their performance without having to change existing wiring, protocols or applications.

   Gigabit Ethernet is expected to give existing high speed technologies such as ATM and FDDI a run for their money. The layered structure of the Gigabit Ethernet is described below under physical layer and MAC layer.

Ques 29) What are the advantages and disadvantages of FDDI?

Ans: Advantages of FDDI

1) **High Bandwidth:** It has bandwidth as high as 250Gbps. High bandwidth allows for tremendous speed. FDDI implementation can handle data rates of 100Mbps.
2) **Security:** It is difficult to eavesdrop on fiber optic cable transmission.
3) **Physical Durability:** Fiber optic cable does not break as easily as do other kind of cables.
4) **Resistance to EMI:** Fiber optic cables are not susceptible to electromagnetic interference.
5) **Cable Distance:** Fiber optic cables transmit signals over 200kms.
6) **Weight:** Fiber optic cable weighs a lot less than copper wire with similar bandwidth.
7) **Use of Multiple Tokens:** FDDI uses multiple tokens to improve network speed.
8) **Ability to Prioritize Workstations:** FDDI can designate some workstations as low priority workstations.

   This allows FDDI to bypass 1000 priority workstations when necessary, providing faster service to high priority stations.
9) **System Fault Tolerance:** FDDI can isolate faulty nodes with the use of wiring concentrators for instantaneous re-routing. Wiring concentrators function as centralized cabling connection devices for workstations.

Disadvantages of FDDI

1) **Complex:** FDDI is a complex technology. Installation and maintenance requires a great deal of expertise.
2) **Costly:** FDDI is costly. In addition to the fiber optic cable cost, the adapters and concentrators are also very expensive.

Ques 30) What are the advantages and disadvantages of fast ethernet?

Ans: Advantages of Fast Ethernet

1) Fast Ethernet is a standards based technology used widely in the world.
2) The performance is 10 times more than in traditional Ethernet.
3) There also is a broad support from network, system and semiconductor industry. It is usually also easy and cheap to implement.
4) It is very good for a company wanting fast data transfer fast, but a company might also want to consider the option of waiting for the ATM to settle in the industry and then taking it to use.

Disadvantages of Fast Ethernet

1) Limitation of fast Ethernet over UTP include distance (only 100 meters), inadequate shielding for some installations, and
2) Relative ease of intruder breaks-ins on the physical cable.

Ques 31) What are the advantages and disadvantages of gigabit ethernet?

Ans: Advantages of Gigabit Ethernet

1) Increased bandwidth for higher performance and elimination of bottlenecks.
2) Full-duplex capacity, allowing the effective bandwidth to be virtually doubled.
3) Aggregating bandwidth to multi-gigabit speeds using Gigabit server adapters and switches.
4) Quality of Service (QoS) features to help eliminate jittery video or distorted audio.
5) Low cost of acquisition and ownership.
6) Full compatibility with the large installed base of Ethernet and fast Ethernet nodes.
7) Transferring large amounts of data across a network quickly.

Disadvantages of Gigabit Ethernet

1) Cannot deliver specific bit rates or limit jitter to deliver effective QoS (Quality of Service).
2) Cannot prioritize traffic to deliver effective CoS (Class of Service)
3) Uses 802.1p and 802.1q to try and achieve QoS and CoS. These technologies are still in development.
4) RSVP protocol not well supported.
5) Not originally designed to support real-time voice or video traffic.
6) Not a WAN solution.

Ques 32) Discuss the IEEE 802.11 Standard in detail.

Or

What is wireless LAN? What do you understand by Infrastructure and Ad-hoc Networks?

Ans: IEEE 802.11 Standard: Wireless LAN

A wireless local area network (LAN) is a flexible data communications system implemented as an extension to or as an alternative for, a wired LAN. Using radio frequency (RF) technology, wireless LANs transmit and receive data over the air, minimizing the need for wired connections. Thus, wireless LANs combine data connectivity with user mobility. Wireless Local Area Networks (WLANs) are like traditional LANs having a wireless interface to enable wireless communication among the equipment that are part of the LAN.

The primary component of a wireless LAN is the wireless interface card that has an antenna. This interface card can be connected to the mobile unit as well as to the fixed network. Wireless LANs have limited range & are designed to be used only in local environments such as a building, hallway, park, or office complex.

Unlike cellular networks with allocated channels (frequencies), users in WLANs have to share frequencies, which may eventually lead to collisions. The choice of frequency depends on whether microwave, spread-spectrum, or infrared communication will be used. Interference and security depend on the type of communications method used in the WLAN.

Infrastructure and Ad-hoc Networks

Wireless networks are set-up to either communicate indirectly through a central place – an access point – or directly, one to the other. The first is called **Infrastructure mode** and the other is called **ad-hoc mode** (it is also called peer-to-peer):

1) **Infrastructure Network:** Communication typically takes place only between the wireless nodes and the access point. Not directly between the wireless nodes. Access point acts as a bridge. Access points with a fixed network can connect several wireless networks to form a larger network beyond the actual radio coverage

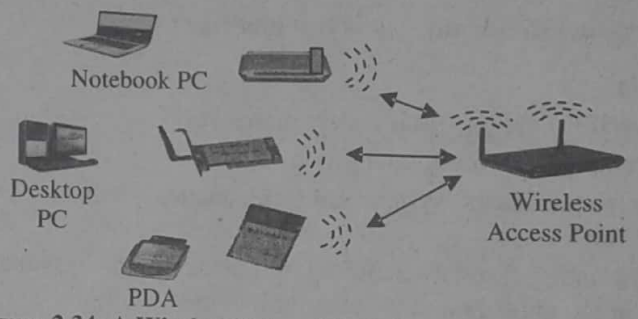


Figure 2.34: A Wireless Network in Infrastructure Mode

Infrastructure networks not only provide access to other networks, but also include forwarding functions, medium access control. Cellular phones are typically infrastructure-based networks for wide area. Also satellite-based cellular phones have an infrastructure (the satellites)

2) **Ad-Hoc Network:** A wireless ad-hoc network is a decentralized type of wireless network as shown in **figure 2.35**. The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks.

Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding the data. Ad hoc networks make sense when needing to build a small, all-wireless LAN quickly and spend the minimum amount of money on equipment.

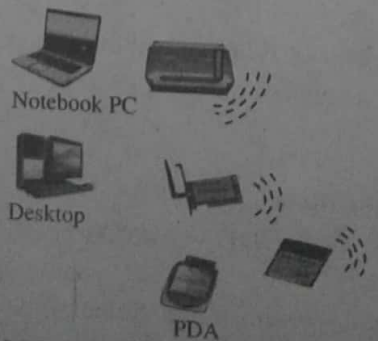


Figure 2.35: A Wireless Network in Ad-hoc Mode

Ques 33) What is the advantages and disadvantages of wireless LAN (WLAN)?

Ans: Advantages of WLAN

1) **Mobility:** Wireless LAN systems can provide LAN users with access to real-time information anywhere in their organization. This mobility supports productivity and service opportunities not possible with wired networks.
2) **Simplicity:** Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.
3) **Flexibility:** Wireless technology allows the network to go where wire cannot go.
4) **Reduced Cost-of-Ownership:** While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves and changes.
5) **Scalability:** Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users that enable roaming over a broad area.

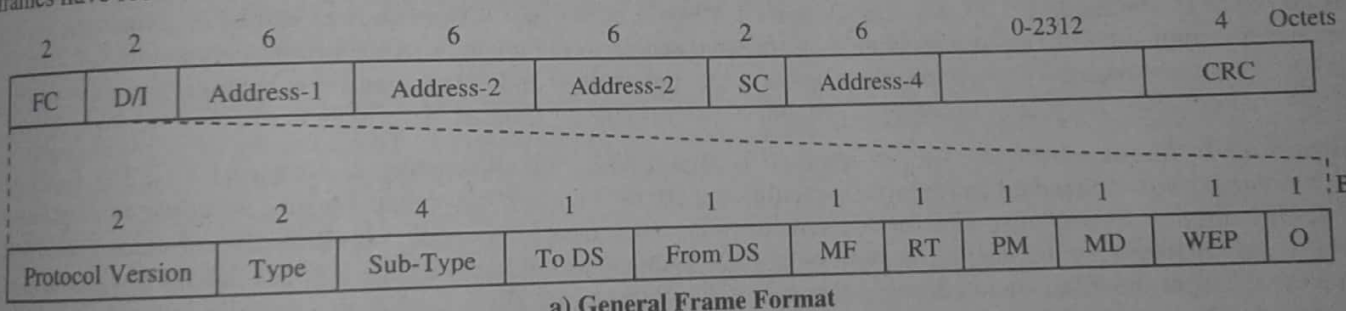
Disadvantages of WLAN

1) **Quality of Service (QoS):** WLANs offer typically lower QoS. Lower bandwidth due to limitations in radio transmission (1–10 Mbit/s) and higher error rates due to interference.
2) **Proprietary Solutions:** Slow standardization procedures lead to many proprietary solutions only working in a homogeneous environment.
3) **Safety and Security:** Using radio waves for data transmission might interfere with other high-tech equipment.
4) **Distance:** Devices will only operate at a limited distance from an access point, with the distance determined by the standard used and buildings and other obstacles between the access point and the user.
5) **Cost:** Long-term cost benefits are harder to achieve in static environments that require few moves and changes.

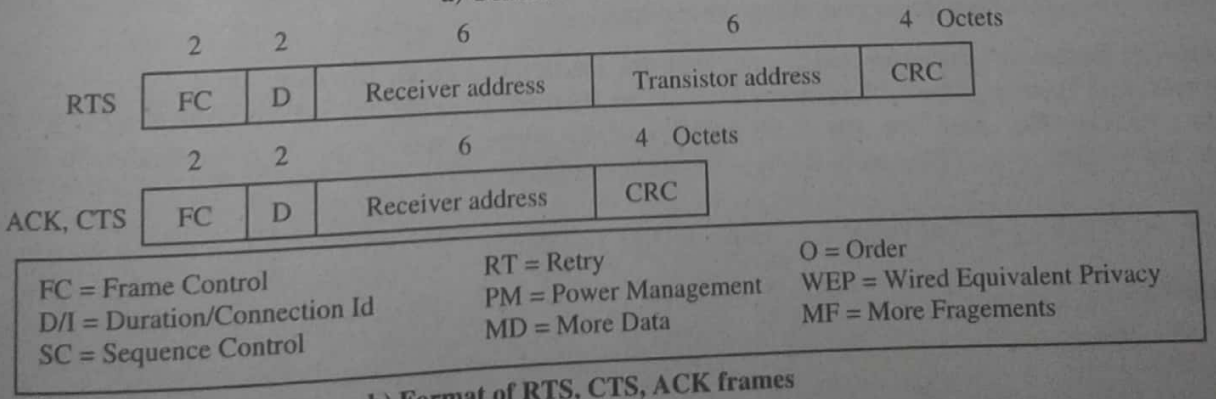
Ques 34) What is the frame format of 802.11 frame?

Ans: 802.11 Frame Format

Figure 2.36(a) shows the general format of the control and data of IEEE 802.11 frames. Formats of RTS, CTS and ACK frames have reduced number of fields as shown in **figure 2.36 (b)**.



a) General Frame Format



b) Format of RTS, CTS, ACK frames

Figure 2.36: Format of IEEE 802.11 Frame

1) **Frame Control (FC, 2 octets):** It indicates the type of frame. Some of its important subfields are as under:
   i) **Protocol version (2 bits):** This field indicates the version of IEEE 802.11 protocol being used.
   ii) **Type (2 bits):** This field indicates the type of frame (control, data, management).

iii) **Sub-type (4 bits):** This field indicates the sub-type of the frame.
iv) **To DS (1 bit):** This bit is set to 1 if the frame is destined for DS.
v) **From DS (I bit):** This bit is set 1 if the frame is coming from DS.
vi) **MF (More Fragment, 1 bit):** This bit is set to 1 if more fragments are to follow.
vii) **RT (Retry, 1 bit):** This bit is set to 1 if this frame is retransmission of previous frame.
viii) **PM (Power management, 1 bit):** This bit is set to 1 if the transmitting station is in sleep mode.
ix) **MD (More data, 1 bit):** This bit when set 1 indicates that the transmitting station has more data to send.
x) **WEP (Wired equivalent privacy, 1 bit):** This bit is 1 if the wired equivalent privacy protocol is implemented.
xi) **Order (1 bit):** If the service provided by the MAC sublayer is 'Strictly Ordered' service, this bit is set to 1.

2) **O/I (Duration/connection Id, 2 octets):** As duration field, it indicates the time in microseconds, the channel is reserved for reliable transmission of a MAC frame and its acknowledgement. As connection-id field, it identifies an association or a connection.

3) **Address fields (6 octets each):** There can be up to four address fields. Their number and use depend on the context. DA and SA are the destination address and source address respectively. The remaining terminology is as follows:

BSS-Id	BSS Identifier
RA	Receiver Address
TA	Transmitter Address

RA and TA refer to addresses of APs within the Distribution System (DS).

4) **Sequence control (SC, 2 octets):** It contains 4-bit fragment number subfield which is used for fragmentation and reassembly. The other 12-bit subfield is the sequence number of the frame sent between a given pair of transmitter and receiver.

5) **CRC:** It is 32-bit frame CRC sequence for detection of errors.

Ques 35) What is the different wireless LAN Standard?

Ans: Wireless LAN Standards
The main standards of wireless LAN are:

1) **IEEE 802.11:** The IEEE 802.11 standard supports 1 Mbps data rate and several choices of physical medium such as spread spectrum and infrared. It also supports prioritized access to the medium. An additional feature of this standard is battery conservation for inactive or idle wireless users, universities and companies are encouraging the use of IEEE 802.11-based LANs for accessing campus computing systems and the Internet.

2) **HiperLAN2:** Another emerging WLAN standard is HiperLAN2, which is being standardised by ETSI (European Telecommunications Standard Institute). An exciting feature of this standard is that it provides for use of connections that offer different quality of service for different applications. It uses time-division multiplexing of unicast, multicast and broadcast connections. Many major players in the WLAN area have formed HiperLAN2 Global Forum to advance and complement the ETSI standardization process. **IEEE 802.11** and **HiperLAN2** are typically infrastructure based networks, which additionally support ad-hoc networking.

3) **Bluetooth:** Bluetooth was promoted by big industry leaders like IBM, Ericsson, Intel, Lucent, Microsoft, Nokia, Motorola, and Toshiba. Bluetooth is more of a wireless Personal Area Network (PAN) operating at 2.4 GHz band and offers a peak 1 Mbps data rate. Bluetooth uses frequency hopping spread spectrum modulation with relatively low power and smaller range. **Bluetooth** is a typical wireless ad-hoc network.

Ques 36) What are the different versions of IEEE 802.11 standard?

Or

Explain the following in detail:
1) IEEE 802.11a
2) IEEE 802.11b
3) IEEE 802.11g
4) IEEE 802.11n

Ans; Versions of IEEE 802.11 Standard
The versions of IEEE 802.11 are as follows:

1) **IEEE 802.11a:** IEEE 802.11a, ratified in 1999, is the amendment to the IEEE 802.11 specification with a higher throughput upto 54Mbps. IEEE 802.11a operates on 5GHz. As compared to other IEEE 802.11 standards, such as

IEEE 802.11b/g, it has less interference, since the 2.4GHz band is heavily used. However, its penetration is also reduced, due to its higher carrier frequency, so the signals are absorbed readily by solid objects along its propagation path.

The modulation of IEEE 802.11a uses Orthogonal Frequency-Division Multiplexing (OFDM) with 52 sub-carriers spanning over a 20MHz spectrum. The attribution of OFDM technology provides fundamental advantages in utilizing multi-path transmission, which is common for an indoor environment. Each sub-carrier can be modulated with BPSK, QPSK, 16-QAM, or 64-QAM, depending on the wireless environment.

2) **IEEE 802.11b :** In August 1999, a group of industry leaders formed a non-profit organisation called the Wireless Ethernet Compatibility Alliance (WECA) to promote the IEEE 802.11 high-rate standard (which eventually became IEEE 802.11b) as a commercial standard to ensure the interoperability of different vendors' products. WECA selected an independent test lab to test and certify the interoperability of the IEEE 802.11b products.

IEEE 802.11b operates on 2.4GHz band with throughput of upto 11Mbps, which was released in 1999 and was marketed under the name Wi-Fi. IEEE 802.11b uses a direct extension of Direct-Sequence Spread Spectrum DSSS on the PHY layer. DSSS uses a continuous string of Pseudonoise (PN) code symbols to module information, which allows multiple transmitters to share the same channel with orthogonal PN codes. WECA was later re-named the Wi-Fi alliance and certifies all the IEEE 802.11 high-rate standards (which include the IEEE 802.11b, IEEE 802.11a, and IEEE 802.11g) products. Almost all companies selling the IEEE 802.11 equipment are members of the Wi-Fi alliance.

3) **IEEE 802.11g:** The IEEE's 802.11g standard is a higher-bandwidth successor to the popular 802.11b, or Wi-Fi standard. 802.11g operates at a maximum speed of 54Mbps whereas 802.11b has a maximum speed of 11Mbps (Megabits/sec). An 802.11g access point compatible with both 802.11b and 802.11g clients. As a result, a laptop computer with an 802.11g card will be able to access existing 802.11b access points as well as new 802.11g access points.

4) **IEEE 802.11n:** The latest wireless standard is called 802.11n. 802.11n implements a technology called **multiple-input multiple-output (MIMO)** that uses multiple transmitters and receivers in each device. This enables multiple data streams on a single device, which will greatly improve WLAN performance. For example, using three transmitters and two receivers (the standard configuration), 802.11n promises a theoretical transmission speed of up to 248 Mbps. 802.11n also promises to double the wireless range to about 230 feet.

This is the next generation of high-speed wireless connectivity promising data transfer rates over 200+ Mbps. It operates at 2.4 GHz and 5 GHz.

802.11n uses Multiple-Input / Multiple-Output (MIMO) technology and a wider radio frequency channel. It also provides a mechanism called frame aggregation to decrease time between transmissions. Current WLAN technologies require that the sending station request the channel, send one packet, release the channel, and then request again in order to send the next packet.

With frame aggregation, once a station requests the channel and has the authority to transmit, it can transmit a series of frames without having to release the channel and regain authority for each frame. With 802.11n, raw data throughput is expected to reach as much as 600 Mbps – that's more than 10 times the throughput of 802.11g.

Ques 37) Discuss 802.15 Standard in Detail.

Or

What is PAN? What are the advantages and disadvantages of PAN?

Ans: 802.15 Standard: Personal Area Networks (PAN)

A personal area network is a computer network organized around an individual person. Personal area networks typically involve a mobile computer, a cell phone and/or a handheld computing device such as a PDA.

Personal area networks generally cover a range of less than 10 meters (about 30 feet). PANs can be viewed as a special type (or subset) of local area network (LAN) that supports one person instead of a group.

PANs can be used for communication among the personal devices themselves (intra-personal communication), or for connecting to a higher level network and the Internet (an uplink). One can use these networks to transfer files including email and calendar appointments, digital photos and music.

The IEEE 802.15 group was set up in March 1999 to reflect on wireless networks with a range of ten meters, or WPAN (Wireless Personal Area Network), with the aim of making connections between different portable one user or multiple

users. This type of network can connect a laptop, cell phone, PDA or any other device of this type. Three service groups were defined, A, B and C:

1) **Group A:** Group A uses the band of unlicensed spectrum use (2.4GHz) targeting a low cost of implementation and use. The size of the cell around the point of emission is of the order of one meter. Power consumption should be particularly low for the terminal to keep several months without electric charging. The selected transmission mode is connectionless. The network must be able to work in parallel with an IEEE 802.11 network. On a single physical location, it may therefore be simultaneously a network of each type, both of which can possibly function degraded way.
2) **Group B:** Group B shows performance increase, with a MAC level up to a rate of at least 100 Mbit / s. The core network must be able to interconnect at least six machines and offer a QoS algorithm, or quality of service, to authorize the operation of some applications, such as telephone speech, which requires a fairly strict QoS. The range between the transmitter and receiver reaches ten meters, and the maximum time to connect to the network must not exceed the second. Finally, this network class must have bridges with other categories of 802.15 networks.
3) **Group C:** Group C introduces important new features for individuals or businesses, such as communication security, video transmission and the possibility of roaming or roaming between wireless networks.

To meet these objectives, industrial groups have set up, such as Bluetooth or WiMedia Alliance. Bluetooth brings together more than 800 companies that have made an open specification for wireless connection between personal devices. Bluetooth is based on a radio link between two devices, while the WiMedia Alliance is interested in very high speed connections over a short range.

Advnatages of PAN

1) Dynamic network setup
2) Usually quick and relatively simple to set up
3) PAN enabled devices are usually portable
4) Typically need less technical skills to deploy than LANs.

Disadvantages of PAN

1) Typically have a limited range
2) Limited to relatively slow data rates when compared with WLAN technologies.
3) Devices with inbuilt PAN technologies can be considerably more expensive than devices without PAN technologies.

Ques 38) What is bluetooth? What are the advantages and disadvantages of bluetooth?

Ans: Bluetooth

802.15.1, more commonly known as **Bluetooth**, is a low-data-rate, low-power wireless networking standard aimed at replacing cables between lightweight devices. Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, and so on. A Bluetooth LAN is an ad-hoc network, which means that the network is formed spontaneously.

Bluetooth is an industrial specification for wireless personal area networks (PANs). Bluetooth provides a way to connect and exchange information between devices like personal digital assistants (PDAs), mobile phones, laptops, PCs, printers and digital cameras via a secure, low-cost, globally available short range radio frequency. A Bluetooth device has a built-in short-range radio transmitter. The current data rate is 1 Mbps with a 2.4-GHz bandwidth. This means that there is a possibility of interference between the IEEE 802.11b wireless LANs and Bluetooth LANs.

Advantages of Bluetooth

1) It creates ad-hoc connection immediately without any wires. Connection establishment is very quick.
2) It has low power consumption.
3) It can pass through walls.
4) It has range better than Infrared communication.
5) It is used for voice and data transfer.
6) It uses FHSS and hence data communication is more secure.
7) Bluetooth devices are available at very cheap cost.

Disadvantages of Bluetooth

1) One of the big disadvantages of bluetooth is security. This is due to the fact that it operates on Radio frequency and hence can penetrate through walls. It is advisable not to use it for critical business or personal data transfer.
2) The bandwidth is lower compare to WiFi.
3) Battery usage is more compare to the condition when bluetooth is powered OFF.

Ques 39) What is the frame format of bluetooth?

Ans: Bluetooth Frame Format

The various fields of Bluetooth frame format are:

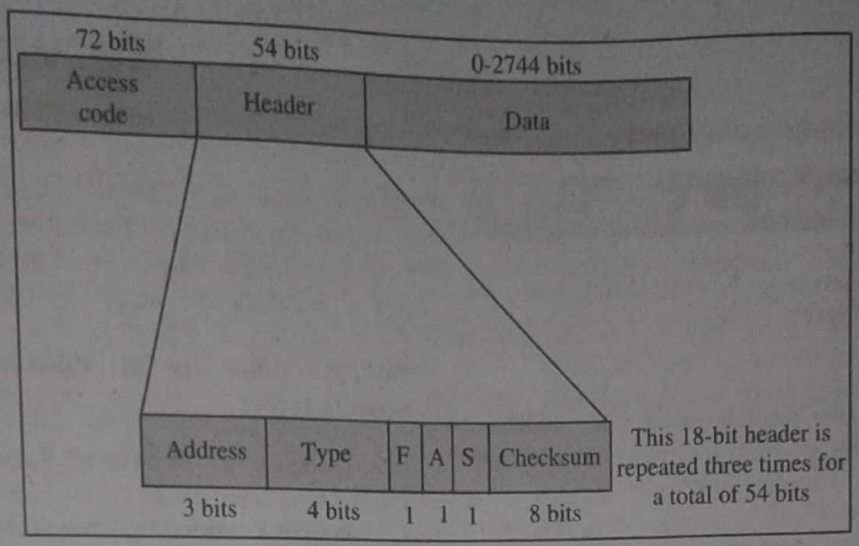


Figure 2.37: Bluetooth Frame Format

1) **Access Code:** It is 72 bit field that contains synchronisation bits. It identifies the master.
2) **Header:** This is 54-bit field. It contain 18 bit pattern that is repeated for 3 times.

The header field contains following sub-fields:

i) **Address:** This 3 bit field can define up to seven slaves (1 to 7). If the address is zero, it is used for broadcast communication from primary to all secondary.

ii) **Type:** This 4 bit field identifies the type of data coming from upper layers.

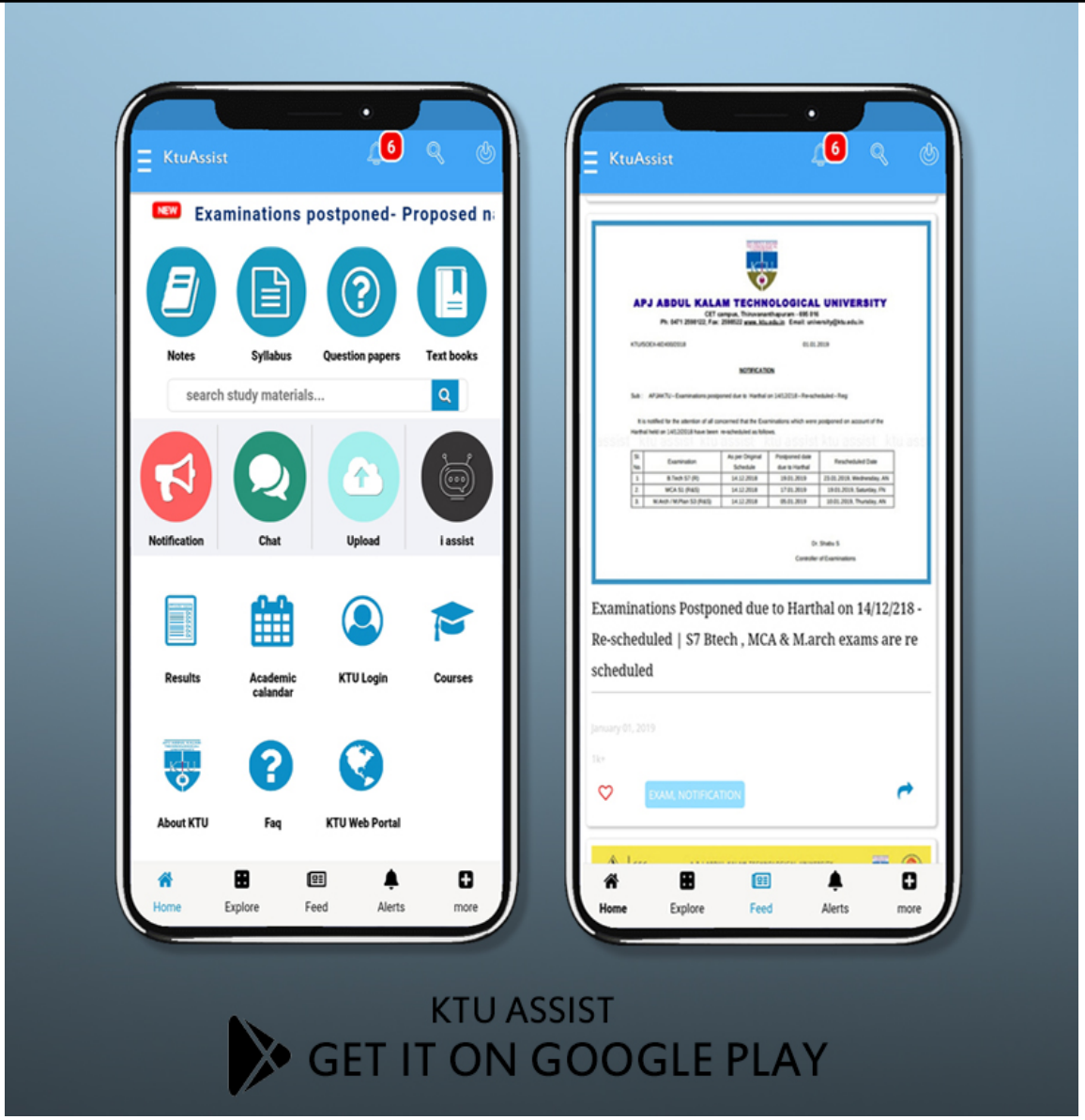
iii) **F:** This flow bit is used for flow control. When set to 1, it means the device is unable to receive more frames.

iv) **A:** This bit is used for acknowledgement.

v) **S:** This bit contains a sequence number of the frame to detect retransmission. As stop and wait protocol is used, one bit is sufficient.

vi) **Checksum:** This 8 bit field contains checksum to detect errors in header.

3) **Data:** This field can be 0 to 2744 bits long. It contains data or control information coming from upper layers.



END

facebook.com/ktuassist

instagram.com/ktu_assist