Q.2 a. Explain various constituents of a Data Communication Model with the help of block diagram.

Answer: Key elements of a data communication channel:

The fundamental purpose of a communications system is the exchange of data between two parties. Figure shows communication between a workstation and a server over a public telephone network. Another example is the exchange of voice signals between two telephones over the same network.

The key elements of the model are as follows:

• **Source**. This device generates the data to be transmitted; examples are telephones and personal computers.

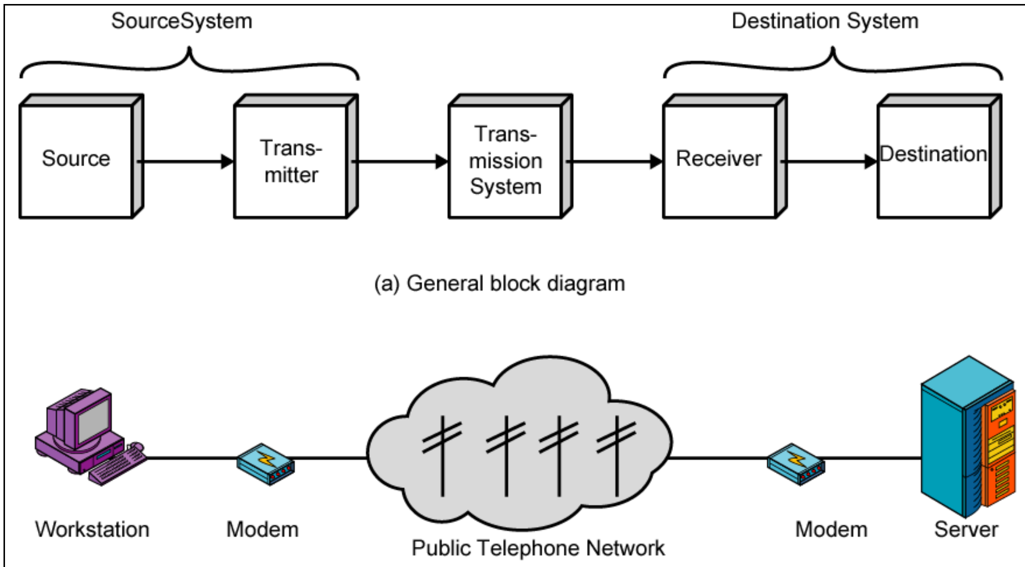
• **Transmitter**: Usually, the data generated by a source system are not transmitted directly in the form in which they were generated. Rather, a transmitter transforms and encodes the information in such a way as to produce electromagnetic signals that can be transmitted across some sort of transmission system.

For example, a modem takes a digital bit stream from an attached device such as a personal computer and transforms that bit stream into an analog signal that can be handled by the telephone network.

• **Transmission system**: This can be a single transmission line or a complex network connecting source and destination.

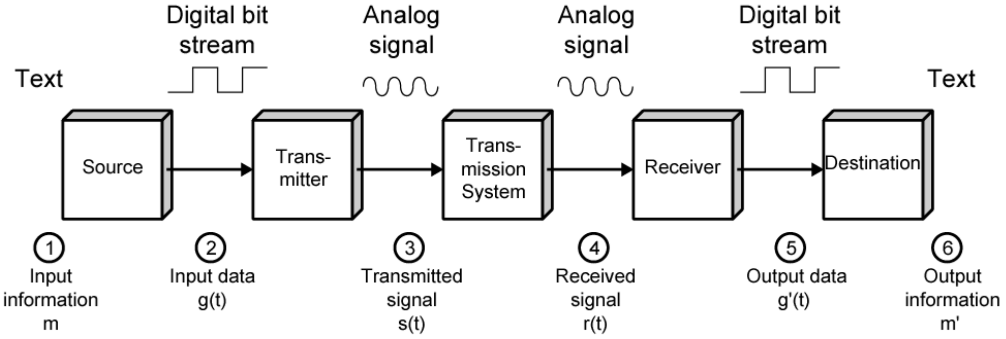
• **Receiver**: The receiver accepts the signal from the transmission system and converts it into a form that can be handled by the destination device. For example, a modem will accept an analog signal coming from a network or transmission line and convert it into a digital bit stream.

• **Destination**: Takes the incoming data from the receiver.



(a) General block diagram

(b) Example



A Data Communications Model

Suppose that the input device and transmitter are components of a personal computer. The user of the PC wishes to send a message m to another user. The user activates the electronic mail package on the PC and enters the message via the keyboard (input device). The character string is briefly buffered in main memory. We can view it as a sequence of bits (g) in memory. The personal computer is connected to some transmission medium, such as a local network or a telephone line, by an I/O device (transmitter), such as a local network transceiver or a modem. The input data are transferred to the transmitter as a sequence of voltage shifts [g(t)] representing bits on some communications bus or cable. The transmitter is connected directly to the medium and converts the incoming stream [g(t)] into a signal [s(t)] suitable for transmission;. The transmitted signal s(t) presented to the medium is subject to a number of impairments, before it reaches the receiver. Thus, the received signal r(t) may differ from s(t). The receiver will attempt to estimate the original s(t), based on r(t) and its knowledge of the medium, producing a sequence of bits These bits are sent to the output personal computer, where they are briefly buffered in memory as a block of bits In many cases, the destination system will attempt to determine if an error has occurred and, if so, cooperate with the source system to eventually obtain a complete, error-free block of data. These data are then presented to the user via an output device, such as a printer or screen. The message as viewed by the user will usually be an exact copy of the original message (m).

Now consider a telephone conversation. In this case the input to the telephone is a message (m) in the form of sound waves. The sound waves are converted by the telephone into electrical signals of the same frequency. These signals are transmitted without modification over the telephone line. Hence the input signal g(t) and the transmitted signal s(t) are identical. The signals (t) will suffer some distortion over the medium, so that r(t) will not be identical to s(t). Nevertheless, the signal r(t) is converted back into a sound wave with no attempt at correction or improvement of signal quality. Thus, is not an exact replica of m. However, the received sound message is generally comprehensible to the listener.

b. Explain TCP/IP Protocol Architecture.

Answer: THE TCP/IP PROTOCOL ARCHITECTURE

The TCP/IP protocol architecture is a result of protocol research and development conducted on the experimental packet-switched network, ARPANET, funded by the Defense Advanced Research Projects Agency (DARPA), and is generally referred to as the TCP/IP protocol suite. This protocol suite consists of a large collection of protocols that have been issued as Internet standards by the Internet Activities Board (IAB).

The TCP/IP Layers

In general terms, communications can be said to involve three agents: applications, computers, and networks. Examples of applications include file transfer and electronic mail. The applications that we are concerned with here are distributed applications that involve the exchange of data between two computer systems. These applications, and others, execute on computers that can often support multiple simultaneous applications. Computers are connected to networks, and the data to be exchanged are transferred by the network from one computer to another. Thus, the transfer of data from one application to another involves first getting the data to the computer in which the application resides and then getting the data to the intended application within the computer. With these concepts in mind, we can organize the communication task into five relatively independent layers.

- Physical layer
- Network access layer
- Internet layer
- Host-to-host, or transport layer
- Application layer

The physical layer covers the physical interface between a data transmission device (e.g., workstation, computer) and a transmission medium or network. This layer is concerned with specifying the characteristics of the transmission medium, the nature of the signals, the data rate, and related matters.

The network access layer is concerned with the exchange of data between an end system (server, workstation, etc.) and the network to which it is attached. The sending computer must provide the network with the address of the destination computer, so that the network may route the data to the appropriate destination. The sending computer may wish to invoke certain services, such as priority, that might be provided by the network. The specific software used at this layer depends on the type of network to be used; different standards have been developed for circuit switching, packet switching (e.g., frame relay), LANs (e.g., Ethernet), and others. Thus it makes sense to separate those functions having to do with network access into a separate layer. By doing this, the remainder of the communications software, above the network access layer, need not be concerned about the specifics of the network to be used. The same higher-layer software should function properly regardless of the particular network to which the computer is attached. The network access layer is concerned with access to and routing data across a network for two end systems attached to the same network.

In those cases where two devices are attached to different networks, procedures are needed to allow data to traverse multiple interconnected networks. This is the function of the internet layer. The Internet Protocol (IP) is used at this layer to provide the routing function across multiple networks. This protocol is implemented not only in the end systems but also in routers. A router is a processor that connects two networks and whose primary function is to relay data from one network to the other on its route from the source to the destination end system. Regardless of the nature of the applications that are exchanging data, there is usually a requirement that data be exchanged reliably. That is, we would like to be assured that all of the data arrive at the destination application and that the data arrive in the same order in which they were sent. As we shall see, the mechanisms for providing reliability are essentially independent of the nature of the applications. Thus, it makes sense to collect those mechanisms in a common layer shared by all applications; this is referred to as the host-to-host layer, or transport layer. The Transmission Control Protocol (TCP) is the most commonly used protocol to provide this functionality. Finally, the application layer contains the logic needed to support the various user applications. For each different type of application, such as file transfer, a separate module is needed that is peculiar to that application.

Q.3 a. Define Channel Capacity. What key factors affect channel capacity?

Answer:

CHANNEL CAPACITY

There are a variety of impairments that distort or corrupt a signal. For digital data, the question arises is to what extent these impairments limit the data rate that can be achieved. The maximum rate at which data can be transmitted over a given communication path, or channel, under given conditions, is referred to as the channel capacity.

There are four concepts here that we are trying to relate to one another.

- Data rate: The rate, in bits per second (bps), at which data can be communicated.
- Bandwidth: The bandwidth of the transmitted signal as constrained by the transmitter and the nature of the transmission medium, expressed in cycles per second, or Hertz
- Noise: The average level of noise over the communications path.
- Error rate: The rate at which errors occur, where an error is the reception of a 1 when a 0 was transmitted or the reception of a 0 when a 1 was transmitted.

Communications facilities are expensive and, in general, the greater the bandwidth of a facility, the greater the cost. Furthermore, all transmission channels of any practical interest are of limited bandwidth. The limitations arise from the physical properties of the transmission medium or from deliberate limitations at the transmitter on the bandwidth to prevent interference from other sources. Accordingly, we would like to make as efficient use as possible of a given bandwidth. For digital data, this means that we would like to get as high a data rate as possible at a particular limit of error rate for a given bandwidth. The main constraint on achieving this efficiency is noise.

b. Assuming that a PSTN has a bandwidth of 3000 Hz and a typical S/N power ratio of 30db, determine the maximum theoretical (data) rate that can be achieved.

Answer: B=3000Hz, (S/N) dB=30db

(S/N) ratio=Antilog (30/10) =1000

C=B log2(1+(S/N)r)=3000 log2(1+1000)=29884.32kbps

c. Differentiate between Shielded Twisted Pair and Un-shielded Twisted Pair.

Answer: STP vs UTP :

UnShielded Twisted Pair (UTP) Cable :

Unshielded twisted pair (UTP) is ordinary telephone wire. Office buildings, by universal practice, are prewired with excess unshielded twisted pair, more than is needed for simple telephone support. This is the least expensive of all the transmission media commonly used for local area networks and is easy to work with and easy to install.

Unshielded twisted pair is subject to external electromagnetic interference, including interference from nearby twisted pair and from noise generated in the environment.

A way to improve the characteristics of this medium is to shield the twisted pair with a metallic braid or sheathing that reduces interference. This shielded twisted pair (STP) provides better performance at higher data rates. However, it is more expensive and more difficult to work with than unshielded twisted pair.

Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks. The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated five categories of wire. Categories of Unshielded Twisted PairType:

Category 1	Voice Only (Telephone Wire)
Category 2	Data to 4 Mbps (LocalTalk)
Category 3	Data to 10 Mbps (Ethernet)
Category 4	Data to 20 Mbps (16 Mbps Token Ring)
Category 5	Data to 100 Mbps (Fast Ethernet)

One difference between the different categories of UTP is the tightness of the twisting of the copper pairs. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. Most schools purchase

Category 3 or Category 5. Category5 cable is highly recommended. For designing a 10 Mbps Ethernet network and are considering the cost savings of buying Category 3 wire instead of Category 5, remember that the Category 5 cable will provide more "room to grow" as transmission technologies increase. Both category 3 and category 5 UTP have a maximum segment length of 100 meters.

Shielded Twisted Pair (STP) Cable :

A disadvantage of UTP is that it may be susceptible to radio and electrical frequency interference. Shielded twisted pair (STP) is suitable for environments with electrical interference; however, the extra shielding can make the cables quite bulky. Shielded twisted pair is often used on networks using Token Ring topology.

Q.4 a. What are various types of digital shift keying modulation? Illustrate your answer by drawing waveforms for binary data 01101.

Answer: Different digital shift keying modulation are

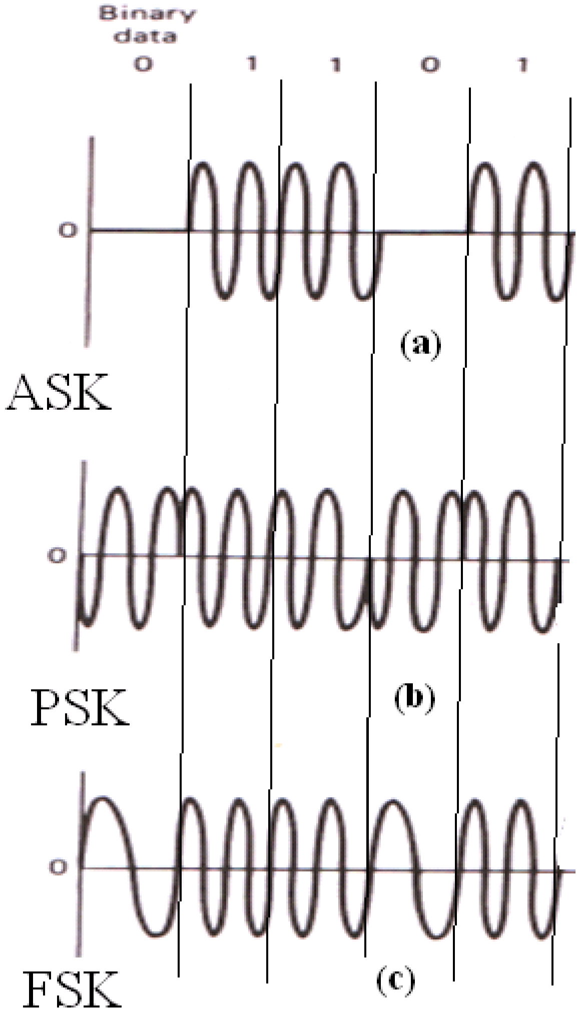
1. Amplitude Shift Keying[ASK]
2. Frequency Shift Keying[FSK]
3. Phase Shift Keying[PSK]

The waveform for the binary data 01101 for these modulations are as shown

Amplitude-shift-keying (ASK): ASK describes the technique the carrier wave is multiplied by the digital signal b(t). For symbol 1 carrier is transmitted, whereas for symbol 0 no carrier is transmitted.

Frequency-shift-keying (FSK): FSK describes the modulation of a carrier (or two carriers) by using a different frequency for a 1 or 0. The resultant modulated signal may be regarded as the sum of two amplitude-modulated signals of different carrier frequency.

Phase-shift-keying (PSK): In PSK for symbol 1 carrier is transmitted, whereas for symbol 0 carrier with 180 degree phase shift is transmitted.



b. **Explain the reasons for shifting towards the digital transmission despite a large analog base.**

Answer: The factors responsible for a shift towards digital transmission despite large analog base are:

- improving digital technology
- data integrity. Repeaters take out cumulative problems in transmission. Can thus transmit longer distances.
- easier to multiplex large channel capacities with digital
- easy to apply encryption to digital data
- better integration if all signals are in one form. Can integrate voice, video and digital data.

Both long-haul telecommunications facilities and intrabuilding services have moved to digital transmission and, where possible, digital signaling techniques. The most important reasons are as follows:

- Digital technology: The advent of large-scale integration (LSI) and very-largescale integration (VLSI) technology has caused a continuing drop in the cost and size of digital circuitry. Analog equipment has not shown a similar drop.
- Data integrity: With the use of repeaters rather than amplifiers, the effects of noise and other signal impairments are not cumulative. Thus it is possible to transmit data longer distances and over lower quality lines by digital means while maintaining the integrity of the data.
- Capacity utilization: It has become economical to build transmission links of very high bandwidth, including satellite channels and optical fiber. A high degree of multiplexing is needed to utilize such capacity effectively, and this is more easily and cheaply achieved with digital (time division) rather than analog (frequency division) techniques.
- Security and privacy: Encryption techniques can be readily applied to digital data and to analog data that have been digitized.
- Integration: By treating both analog and digital data digitally, all signals have the same form and can be treated similarly. Thus economies of scale and convenience can be achieved by integrating voice, video, and digital data.

c. What are the key factors that are to be considered while designing a data transmission system?

Answer: In considering the design of data transmission systems, key concerns are data rate and distance: the greater the data rate and distance the better. A number of design factors relating to the transmission medium and the signal determine the data rate and distance:

• **Bandwidth:** All other factors remaining constant, the greater the bandwidth of a signal, the higher the data rate that can be achieved.

• **Transmission impairments:** Impairments, such as attenuation, limit the distance. For guided media, twisted pair generally suffers more impairment than coaxial cable, which in turn suffers more than optical fiber.

• **Interference:** Interference from competing signals in overlapping frequency bands can distort or wipe out a signal. Interference is of particular concern for unguided media, but is also a problem with guided media. For guided media, interference can be caused by emanations from nearby cables. For example, twisted pairs are often bundled together and conduits often carry multiple cables. Interference can also be experienced from unguided transmissions. Proper shielding of a guided medium can minimize this problem.

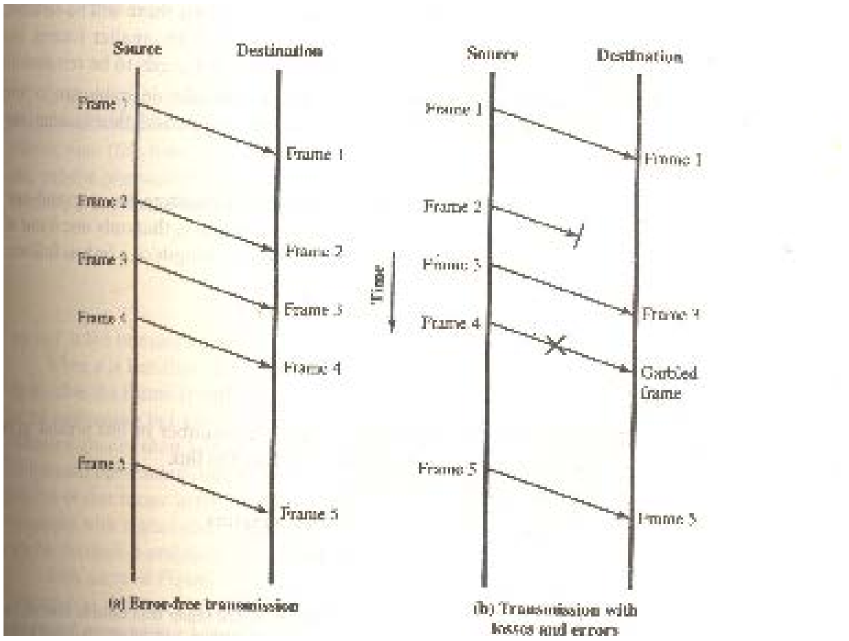
• **Number of receivers:** A guided medium can be used to construct a point-to-point link or a shared link with multiple attachments. In the latter case,each attachment introduces some attenuation and distortion on the line, limiting distance and/or data rate.

Q.5 a. What do you mean by flow control? What are techniques used for flow control?

Answer: FLOW CONTROL

Flow control is a technique for assuring that a transmitting entity does not overwhelm a receiving entity with data. The receiving entity typically allocates a data buffer of some maximum length for a transfer. When data are received, the receiver must do a certain amount of processing before passing the data to the higher-level software. In the absence of flow control, the receiver's buffer may fill up and overflow while it is processing old data.

To begin, we examine mechanisms for flow control in the absence of errors. The model we will use is depicted in Figure, which is a vertical-time sequence diagram. It has the advantages of showing time dependencies and illustrating the correct send-receive relationship. Each arrow represents a single frame transiting a data link between two stations. The data are sent in a sequence of frames, with each frame containing a portion of the data and some control information. The time it takes for a station to emit all of the bits of a frame onto the medium is the transmission time; this is proportional to the length of the frame. The propagation time is the time it takes for a bit to traverse the link between source and destination. For this section, we assume that all frames that are transmitted are successfully received; no frames are lost and none arrive with errors. Furthermore, frames arrive in the same order in which they are sent. However, each transmitted frame suffers an arbitrary and variable amount of delay before reception.



(a) Error-free transmission

(b) Transmission with losses and errors

In data communications, flow control is the process of managing the rate of data transmission between two nodes to prevent a fast sender from overwhelming a slow receiver. It provides a mechanism for the receiver to control the transmission speed, so that the receiving node is not overwhelmed with data from transmitting node. Flow control should be distinguished from congestion control, which is used for controlling the flow of data when congestion has actually occurred. Flow control mechanisms can be classified by whether or not the receiving node sends feedback to the sending node.

Flow control is important because it is possible for a sending computer to transmit information at a faster rate than the destination computer can receive and process it. This can happen if the receiving computers have a heavy traffic load in comparison to the sending computer, or if the receiving computer has less processing power than the sending computer.

- Stop-and-wait
- Stop-and-wait ARQ

Stop-and-wait flow control is the simplest form of flow control. In this method, the receiver indicates its readiness to receive data for each frame, the message is broken into multiple frames. The sender waits for an ACK (acknowledgement) after every frame for specified time (called time out). It is sent to ensure that the receiver has received the frame correctly. It will then send the next frame only after the ACK has been received.

Operations:

- Sender: Transmits a single frame at a time.
- Receiver: Transmits acknowledgement (ACK) as it receives a frame.
- Sender receive ACK within time out.
- Go to step 1.

If a frame or ACK is lost during transmission then it has to be transmitted again by sender. This retransmission process is known as ARQ (automatic repeat request).

The problem with Stop-and wait is that only one frame can be transmitted at a time and that often leads to inefficient transmission channel till we get the acknowledgement the sender can not transmit any new packet. During this time both the sender and the channel are unutilised.

Pros and cons of stop and wait :

Pros

- The only advantage of this method of flow control is its simplicity.

Cons

- The sender needs to wait for the ACK after every frame it transmits. This is a source of inefficiency, and is particularly bad when the propagation delay is much longer than the transmission delay.
- Stop and wait can also create inefficiencies when sending longer transmissions. When longer transmissions are sent there is more likely chance for error in this protocol. If the messages are short the errors are more likely to be detected early. More inefficiency is created when single messages are broken into separate frames because it makes the

transmission longer.

Sliding Window

Sliding Window Protocol

A method of flow control in which a receiver gives a transmitter permission to transmit data until a window is full. When the window is full, the transmitter must stop transmitting until the receiver advertises a larger window.

Sliding-window flow control is best utilized when the buffer size is limited and pre-established. During a typical communication between a sender and a receiver the receiver allocates buffer space for n frames (n is the buffer size in frames). The sender can send and the receiver can accept n frames without having to wait for an acknowledgement. The receiver acknowledges a frame by sending an acknowledgement that includes the sequence number of the next frame expected. This acknowledgement announces that the receiver is ready to receive n frames, beginning with the number specified. Both the sender and receiver maintain what is called a window. The size of the window is less than or equal to the buffer size.

Sliding window flow control has a far better performance than stop-and-wait flow control. For example in a wireless environment data rates are very low and noise level is very high, so waiting for an acknowledgement for every packet that is transferred is not very feasible. Therefore, transferring data as a bulk would yield a better performance in terms of higher throughput.

Sliding window flow control is a point to point protocol assuming that no other entity tries to communicate until the current data transfer is complete.

Go Back N

Go-Back-N ARQ

An automatic repeat request (ARQ) algorithm, used for error correction, in which a negative acknowledgement (NAK) causes retransmission of the word in error as well as the previous N–1 words. The value of N is usually chosen such that the time taken to transmit the N words is less than the round trip delay from transmitter to receiver and back again. Therefore a buffer is not needed at the receiver.

The normalized propagation delay (a) = propagation time (Tp)⁄transmission time (Tt), where Tp = Length (L) over propagation velocity (V) and Tt = bit rate (r) over Framerate (F).

So that a =Lr⁄VF.

To get the utilization a window size (N) is defined. If N is greater than or equal to 2a + 1 then the utilization is 1 (full utilization) for the transmission channel. If it is less than 2a + 1 then the equation N⁄1+2a must be used to compute utilization.

Selective Repeat

Selective Repeat ARQ

Selective Repeat is a connection oriented protocol in which both transmitter and receiver have a window of sequence numbers. The protocol has a maximum number of messages that can be sent without acknowledgement. If this window becomes full, the protocol is blocked until an acknowledgement is received for the earliest outstanding message. At this point the transmitter is clear to send more messages.

b. Given a channel of large capacity, how does one subdivide the channel into smaller logical channels for individual users?

Answer: Multiplex many conversations over same channel. Three flavors of solution:

Frequency division multiplexing (FDM): Divide the frequency spectrum into smaller subchannels, giving each user exclusive use of a subchannel (e.g., radio and TV). One problem with FDM is that a user is given all of the frequency to use, and if the user has no data to send, bandwidth is wasted | it cannot be used by another user.

Time division multiplexing (TDM): Use time slicing to give each user the full bandwidth, but for only a fraction of a second at a time (analogous to time sharing in operating systems). Again, if the user doesn't have data to sent during his timeslice, the bandwidth is not used (e.g., wasted).

Statistical multiplexing: Allocate bandwidth to arriving packets on demand. This leads to the most efficient use of channel bandwidth because it only carries useful data. That is, channel bandwidth is allocated to packets that are waiting for transmission, and a user generating no packets doesn't use any of the channel resources.

Q.6 a. Compare and contrast Circuit switching with Packet Switching.

Answer: Circuit Switching

The phone system uses a technique called circuit switching .

1. Once a call has been completed, the user sees a set of “virtual wires" between communicating endpoints.

2. The user sends a continuous stream of data, which the channel guarantees to deliver at a known rate.

3. Data transmission handled elegantly using TDM or FDM. Note that TDM/FDM work well because the data rate is predictable. The voice grade signal is sampled using PCM generating a steady stream of bits.

4. Call setup required before any data can be sent, allowing network to set up the path, allocate subchannels, etc. Call setup also used to decide who to charge for the call.

5. Call termination required when parties complete call, allowing the network to reclaim resources. At this point, a billing record is saved somewhere that records where the call was made, its duration, etc.

Advantages of Circuit Switching:

1. Fixed bandwidth, guaranteed capacity (e.g., no congestion).

2. Low-variance end-to-end delay (e.g., delay nearly constant).

Drawbacks:

1. Connection setup introduces delay before communication can begin.

2. User pays for circuit, even when not sending any data.

3. Other users cannot use bandwidth of other circuits that are not actually being used (e.g., in most conversations, only one person speaks at a time. Thus, half the

underlying bandwidth is wasted.

Packet Switching

In contrast, packet switching systems use statistical multiplexing to make better use of a
channel:

1. Data is sent in individual messages (packets).
2. Each message is forwarded from switch to switch, eventually reaching its destination.
3. Each switch has a small amount of buffer space to temporarily hold messages. If an outgoing line is busy, the packet is queued until the line becomes available.

Packet Switching vs Circuit switching:

1. (Current) packet switching system do not provide known delay or capacity characteristics. Some applications, like those making use of real-time voice and video, cannot tolerate high variation in delays.
2. If many sites send data at the same time, end-to-end delay increases. That is, per-user response and throughput drops as more users share a channel.
3. Packet switching utilizes resources more efficiently (similar to multiprocessing in operating systems). In particular, with circuit switching, bandwidth can be allocated but unused, as when no one talks.
4. Packet switching systems doesn't usually require opening a connection before sending data. This important for applications that send only a single packet of data; the cost of opening and closing a connection may exceed the cost of sending the data.
5. Billing algorithm more complex in packet switching systems. It's easy to bill for a connection, because one can figure out who to charge during the connection set up. With packet-switching, each packet must be accounted for individually.

b. Differentiate between Implicit Congestion signalling and Explicit Congestion Signalling for congestion control.

Answer: Implicit Congestion Signaling

When network congestion occurs, two things may happen:

(1) The transmission delay for an individual packet from source to destination increases, so that it is noticeably longer than the fixed propagation delay, and (2) packets are discarded. If a source is able to detect increased delays and packet discards, then it has implicit evidence of network congestion. If all sources can detect congestion and, in response, reduce flow on the basis of congestion, then the network congestion will be relieved. Thus, congestion control on the basis of implicit signaling is the responsibility of end systems and does not require action on the part of network nodes. Implicit signaling is an effective congestion control technique in connection-less or datagram, configurations, such as datagram packet-switching networks and IP based internets. In such cases, there are no logical connections through the internet on which flow can be regulated. However, between the two end systems, logical connections can be established at the TCP level. TCP includes mechanisms for acknowledging receipt of TCP segments and for regulating the flow of data between source and destination on a TCP connection.

Implicit signaling can also be used in connection-oriented networks. For example, in frame relay networks, the LAPF control protocol, which is end to end, includes facilities similar to those of TCP for flow and error control. LAPF control is capable of detecting lost frames and adjusting the flow of data accordingly.

Explicit Congestion Signaling

It is desirable to use as much of the available capacity in a network as possible but still react to congestion in a controlled and fair manner. This is the purpose of explicit congestion avoidance techniques. In general terms, for explicit congestion avoidance, the network alerts end systems to growing congestion within the network and the end systems take steps to reduce the offered load to the network.

Typically, explicit congestion control techniques operate over connection-oriented networks and control the flow of packets over individual connections. Explicit congestion signaling approaches can work in one of two directions:

- **Backward:** Notifies the source that congestion avoidance procedures should be initiated where applicable for traffic in the opposite direction of the received notification. It indicates that the packets that the user transmits on this logical connection may encounter congested resources. Backward information is transmitted either by altering bits in a header of a data packet headed for the source to be controlled or by transmitting separate control packets to the source.

• **Forward:** Notifies the user that congestion avoidance procedures should be initiated where applicable for traffic in the same direction as the received notification. It indicates that this packet, on this logical connection, has encountered congested resources. Again, this information may be transmitted either as altered bits in data packets or in separate control packets. In some schemes, when a forward signal is received by an end system, it echoes the signal back along the logical connection to the source. In other schemes, the end system is expected to exercise flow control upon the source end system at a higher layer (e.g.,TCP).

We can divide explicit congestion signaling approaches into three general categories:

• **Binary:** A bit is set in a data packet as it is forwarded by the congested node. When a source receives a binary indication of congestion on a logical connection, it may reduce its traffic flow.

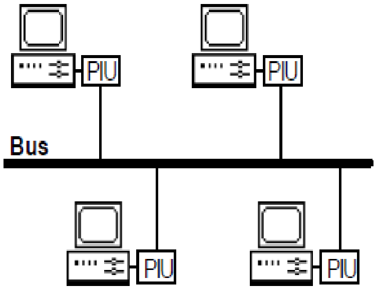
• **Credit based:** These schemes are based on providing an explicit credit to a source over a logical connection. The credit indicates how many octets or how many packets the source may transmit. When the credit is exhausted, the source must await additional credit before sending additional data. Credit-based schemes are common for end-to-end flow control, in which a destination system uses credit to prevent the source from overflowing the destination buffers, but credit-based schemes have also been considered for congestion control.

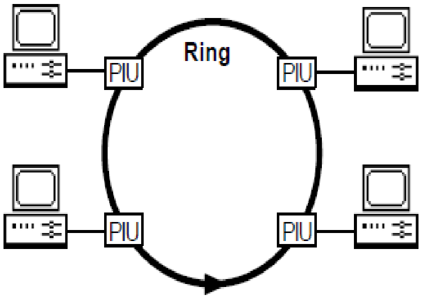
• **Rate based:** These schemes are based on providing an explicit data rate limit to the source over a logical connection. The source may transmit data at a rate up to the set limit. To control congestion, any node along the path of the connection can reduce the data rate limit in a control message to the source.

Q.7 a. What are the basic topologies used in LAN? Describe LAN protocol

architecture.

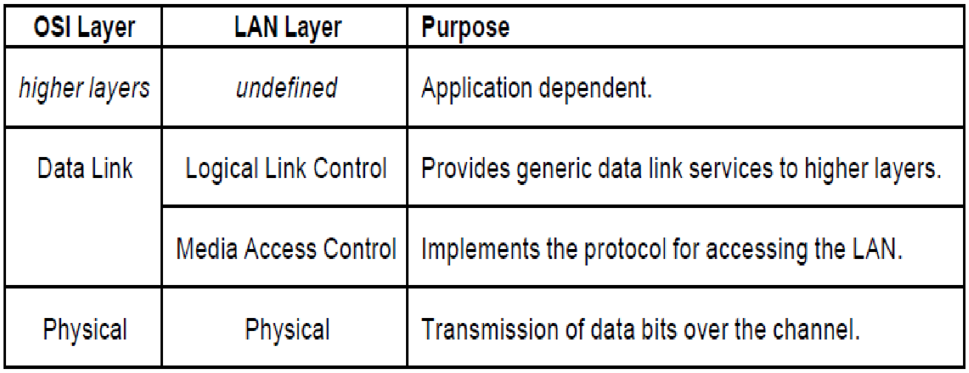
Answer: LAN topologies: There are two general categories of LAN topologies: bus and ring .The bus topology uses a broadcast technique, hence only one station at a time can send messages and all other station listen to the message. A listening station examines the recipient address of the message and if it matches its own address, copies the message; otherwise, it ignores the message. The ring topology uses a closed, point-to-point-connected loop of stations. Data flows in one direction only, from one station to the next. As with the bus topology, transmission is restricted to one user at a time. When a station gains control and sends a message, the message is sent to the next station in the ring. Each receiving station in the ring examines the recipient address of the message and if it matches its own address, copies the message. The message is passed around the ring until it reaches the originator which removes the message by not sending it to the next station.





LAN Protocol Architecture : The role of the physical layer is the same as in the OSI model. It includes the connectors used for connecting the PIU to the LAN and the signaling circuitry provided by the PIU. The OSI data link layer is broken into two sublayers. The Media Access Control (MAC) layer is responsible for implementing a specific LAN access protocol. This layer is therefore highly dependent on the type of the LAN. Its aim is to hide hardware and access protocol dependencies from the next layer. A number of MAC standards have been devised, one for each popular type of access protocol. The Logical Link Control (LLC) layer provides data link services independent of the specific MAC protocol involved. LLC is a subset of HDLC and is largely compatible with the data link layer of OSI-compatible WANs. LLC is only concerned with providing Link Service Access

Points (LSAPs). All other normal data link functions (i.e., link management, frame management, and error handling) are handled by the MAC layer. LANs are not provided with a network layer (or any other higher layer) because such a layer would be largely redundant. Because the stations are directly connected, there is no need for switching or routing. In effect, the service provided by the LLC is equivalent to the OSI network layer service.



OSI Layer	LAN Layer	Purpose
higher layers	*undefined*	Application dependent.
Data Link	Logical Link Control	Provides generic data link services to higher layers.
	Media Access Control	Implements the protocol for accessing the LAN.
Physical	Physical	Transmission of data bits over the channel.

b. Briefly explain why Wireless LANs are required.

Answer: Wireless LAN Requirements

A wireless LAN must meet the same sort of requirements typical of any LAN, including high capacity, ability to cover short distances, full connectivity among attached stations, and broadcast capability. In addition, there are a number of requirements specific to the wireless LAN environment.

The following are among the most important requirements for wireless LANs:

• **Throughput:** The medium access control protocol should make as efficient use as possible of the wireless medium to maximize capacity.

• **Number of nodes**: Wireless LANs may need to support hundreds of nodes across multiple cells.

• **Connection to backbone LAN:** In most cases, interconnection with stations on a wired backbone LAN is required. For infrastructure wireless LANs, this is easily accomplished through the use of control modules that connect to both types of LANs. There may also need to be accommodation for mobile users and ad hoc wireless networks.

• **Service area:** A typical coverage area for a wireless LAN has a diameter of 100 to 300 m.

• **Battery power consumption**: Mobile workers use battery-powered workstations that need to have a long battery life when used with wireless adapters.

This suggests that a MAC protocol that requires mobile nodes to monitor access points constantly or engage in frequent handshakes with a base station is inappropriate. Typical wireless LAN implementations have features to reduce power consumption while not using the network, such as a sleep mode.

• **Transmission robustness and security**: Unless properly designed, a wireless LAN may be especially vulnerable to interference and eavesdropping. The design of a wireless LAN must permit reliable transmission even in a noisy environment and should provide some level of security from eavesdropping.

• **Collocated network operation**: As wireless LANs become more popular, it is quite likely for two or more wireless LANs to operate in the same area or in some area where interference between the LANs is possible. Such interference may thwart the normal operation of a MAC algorithm and may allow unauthorized access to a particular LAN.

• **License-free operation**: Users would prefer to buy and operate wireless LAN products without having to secure a license for the frequency band used by the LAN.

• **Handoff/roaming**: The MAC protocol used in the wireless LAN should enable mobile stations to move from one cell to another.

• **Dynamic configuration**: The MAC addressing and network management aspects of the LAN should permit dynamic and automated addition, deletion,and relocation of end systems without disruption to other users.

Q.8 a. Explain Internet Protocol. Differentiate between IPv4 and IPv6.

Answer: Internet Protocol (IP):

- IP (short for Internet Protocol) specifies the technical format of packets and the addressing scheme for computers to communicate over a network. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.
- IP by itself can be compared to something like the postal system. It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time.

Internet Protocol Versions

There are currently two version of Internet Protocol (IP): *IPv4* and a new version called *IPv6.* IPv6 is an evolutionary upgrade to the Internet Protocol. IPv6 will coexist with the older IPv4 for some time.

Internet Protocol Version 4:

- IPv4 (*I*nternet **P**rotocol **V**ersion **4**) is the fourth revision of the Internet Protocol (IP) used to to identify devices on a network through an addressing system. The Internet Protocol is designed for use in interconnected systems of packet-switched computer communication networks .
- IPv4 is the most widely deployed Internet protocol used to connect devices to the Internet. IPv4 uses a 32-bit address scheme allowing for a total of 2^32 addresses (just over 4 billion addresses). With the growth of the Internet it is expected that the number of unused IPv4 addresses will eventually run out because every device -- including computers, smartphones and game consoles -- that connects to the Internet requires an address.

A new Internet addressing system Internet Protocol version 6 (IPv6) is being deployed to fulfill the need for more Internet addresses.

Internet Protocol Version 6:

- IPv6 (*I*nternet **P**rotocol **V**ersion **6**) is also called IPng (*I*nternet **P**rotocol ***n***ext *generation*) and it is the newest version of the Internet Protocol (IP) reviewed in the IETF standards committees to replace the current version of IPv4 (Internet Protocol Version 4).

- IPv6 is the successor to Internet Protocol Version 4 (IPv4). It was designed as an evolutionary upgrade to the Internet Protocol and will, in fact, coexist with the older IPv4 for some time. IPv6 is designed to allow the Internet to grow steadily, both in terms of the number of hosts connected and the total amount of data traffic transmitted.
- IPv6 is often referred to as the "next generation" Internet standard and has been under development now since the mid-1990s. IPv6 was born out of concern that the demand for IP addresses would exceed the available supply.

While increasing the pool of addresses is one of the most often-talked about benefit of IPv6, there are other important technological changes in IPv6 that will improve the IP protocol:

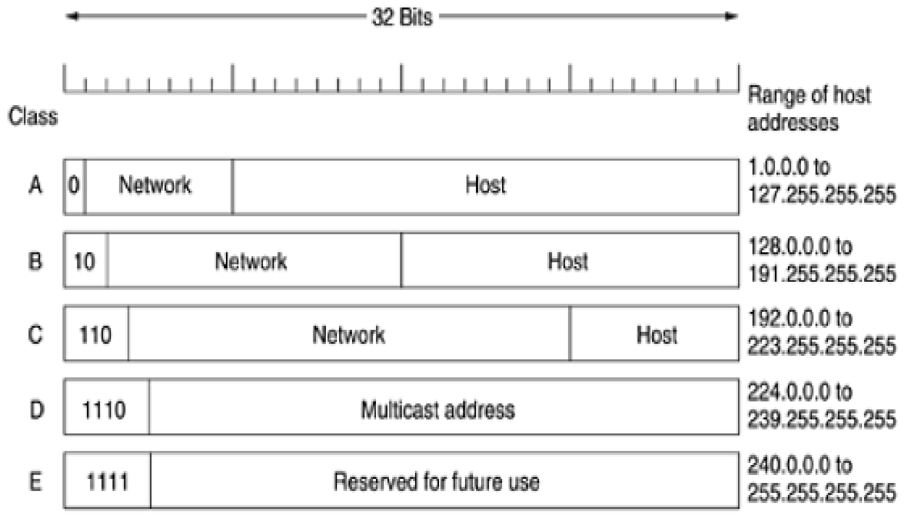
- No more NAT (Network Address Translation)
- Auto-configuration
- No more private address collisions
- Better multicast routing
- Simpler header format
- Simplified, more efficient routing
- True quality of service (QoS), also called "flow labeling"
- Built-in authentication and privacy support
- Flexible options and extensions
- Easier administration (say good-bye to DHCP)

Subjects	**IPv4**	**IPv6**
Address Space	4 Billion Addresses	2^128
Configuration	Manual or use DHCP	Universal Plug and Play (UPnP) with or without DHCP
Broadcast / Multicast	Uses both	No broadcast and has different forms of multicast

Any cast support	Not part of the original protocol	Explicit support of any cast
Mobility	Uses Mobile IPv4	Mobile IPv6 provides fast handover, better router optimization and hierarchical mobility

b. What is meant by dotted decimal notation used in network addressing?

Answer: Every host and router on the Internet has an IP address, which encodes its network number and host number. The combination is unique: in principle, no two machines on the Internet have the same IP address. All IP addresses are 32 bits long and are used in the Source address and Destination address fields of IP packets. It is important to note that an IP address does not actually refer to a host. It really refers to a network interface, so if a host is on two networks, it must have two IP addresses. However, in practice, most hosts are on one network and thus have one IP address. The class A, B, C, and D formats allow for up to 128 networks with 16 million hosts each, 16,384 networks with up to 64K hosts, and 2 million networks (e.g., LANs) with up to 256 hosts each (although a few of these are special). Also supported is multicast, in which a datagram is directed to multiple hosts. Addresses beginning with 1111 are reserved for future use. Over 500,000 networks are now connected to the Internet, and the number grows every year. Network numbers are managed by a nonprofit corporation called ICANN (Internet Corporation for Assigned Names and Numbers) to avoid conflicts. In turn, ICANN has delegated parts of the address space to various regional authorities, which then dole out IP addresses to ISPs and other companies. Network addresses, which are 32-bit numbers, are usually written in dotted decimal notation. In this format, each of the 4 bytes is written in decimal, from 0 to 255. For example, the 32-bit hexadecimal address C0290614 is written as 192.41.6.20. The lowest IP address is 0.0.0.0 and the highest is 255.255.255.255.


32 Bits
Class
Range of host addresses
A
0
Network
Host
1.0.0.0 to 127.255.255.255
B
10
Network
Host
128.0.0.0 to 191.255.255.255
C
110
Network
Host
192.0.0.0 to 223.255.255.255
D
1110
Multicast address
224.0.0.0 to 239.255.255.255
E
1111
Reserved for future use
240.0.0.0 to 255.255.255.255

Q.9 Write short notes on:

(i) Manchester Encoding
(ii) Guided and Unguided Transmission Media
(iii) Optical Fiber
(iv) Multicasting

Answer:

(i). Manchester encoding is one technique that provides clocking information. The encoding splits each sampling unit into 2 halves where:

a binary “1" is sent as a high-low voltage sequence

a “0" is sent as a low-high sequence because each sampling time contains one transition, the receiver can easily synchronize its clock to the sender's.

In a related technique, differential Manchester encoding, a “1" bit is indicated by the absence of a transition at the start of the bit time, while a “0" is indicated by the presence of a transition.

Drawback of Manchester encoding:

Half the bandwidth is wasted because it takes two transitions to represent one bit

Advantages:

Reduced complexity of transmitter and receiver components

(ii). The transmission media that are used to convey information can be classified as guided or unguided. Guided media provide a physical path along which the signals are propagated; these include twisted pair, coaxial cable, and optical fiber. Unguided media employ an

antenna for transmitting through air, vacuum, or water.

- Traditionally, twisted pair has been the workhorse for communications of all sorts. Higher data rates over longer distances can be achieved with coaxial cable, and so coaxial cable has often been used for high speed local area network and for high-capacity long-distance trunk applications. However, the tremendous capacity of optical fiber has made that medium more attractive than coaxial cable, and thus optical fiber has taken over much of the market for high-speed LANs and for long-distance applications.
- Unguided transmission techniques commonly used for information communications include broadcast radio, terrestrial microwave, and satellite. Infrared transmission is used in some

(iii). Optical Fiber

Physical Description An optical fiber is a thin (2 to 125 µm diameter), flexible medium capable of guiding an optical ray. Various glasses and plastics can be used to make optical fibers. The lowest losses have been obtained using fibers of ultrapure fused silica. Ultrapure fiber is difficult to manufacture; higher-loss multicomponent glass fibers are more economical and still provide good performance. Plastic fiber is even less costly and can be used for short-haul links, for which moderately high losses are acceptable.

An optical fiber cable has a cylindrical shape and consists of three concentric sections: the core, the cladding, and the jacket. The core is the innermost section and consists of one or more very thin strands, or fibers, made of glass or plastic; the core has a diameter in the range of 8 to 50 µm .Each fiber is surrounded by its own cladding, a glass or plastic coating that has optical properties different from those of the core and a diameter in the range of 8 to 50 µm . The interface between the core and cladding acts as a reflector to confine light that would otherwise escape the core. The outermost layer, surrounding one or a bundle of cladded fibers, is the jacket. The jacket is composed of plastic and other material layered to protect against moisture, abrasion, crushing, and other environmental dangers.

Applications Optical fiber already enjoys considerable use in long-distance telecommunications, and its use in military applications is growing. The continuing improvements in performance and decline in prices, together with the inherent advantages of optical fiber, have made it increasingly attractive for local area networking.

(iv). Typically, an IP address refers to an individual host on a particular network. IP also accommodates addresses that refer to a group of hosts on one or more networks. Such addresses are referred to as multicast addresses, and the act of sending a packet from a source to the members of a multicast group is referred to as multicasting.

Multicasting has a number of practical applications. For example,

- Multimedia: A number of users “tune in” to a video or audio transmission from a multimedia source station.
- Teleconferencing: A group of workstations form a multicast group such that a transmission from any member is received by all other group members.
- Database: All copies of a replicated file or database are updated at the same time.
- Distributed computation: Intermediate results are sent to all participants.
- Real-time workgroup: Files, graphics, and messages are exchanged among active group members in real time.

TEXT BOOK

I. Data and Computer Communications, Eight Edition (2007), William Stallings, Pearson Education Low Price Edition.