1. What is data communication? What are different characteristic of data communication system?

The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data. Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics—

1) **Delivery:** The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

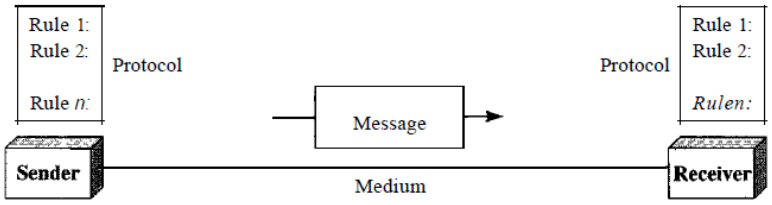
2) **Accuracy:** The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

3) **Timeliness:** The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

4) **Jitter:** Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

2. What are the different components of data communication model?

A data communication system has five components; shown in the following figure—



1) **Message:** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

2) **Sender:** The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

3) **Receiver**: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

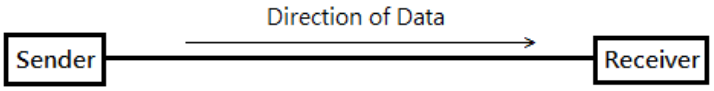
4) **Transmission medium:** The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

5) **Protocol:** A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

3. What are the different types of communication mode?

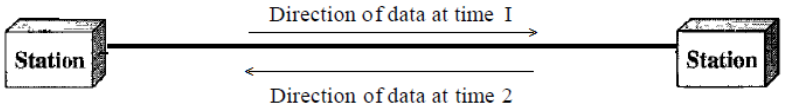
There are three types of communication mode—

1) **Simplex:** In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive. As shown in the following figure—



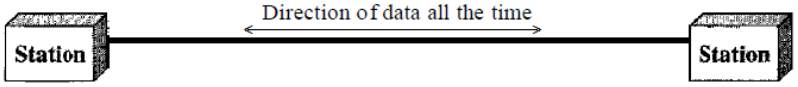
Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

2) **Half-Duplex:** In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa; as shown in following figure—



The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

3) **Full-Duplex:** In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously; as shown in the following figure—

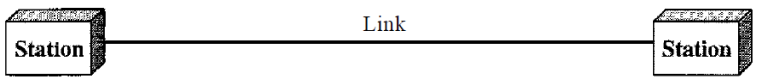


The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link: with signals going in the other direction. This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions. One common example of full-duplex communication is the telephone network.

4. What is Network? What are the different types of connection used in network?

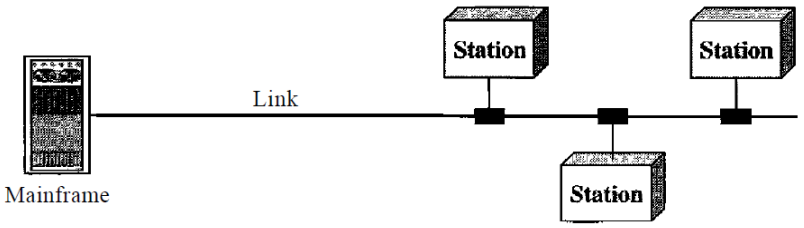
A network is a set of devices (nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network. A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections—

1) **Point-to-Point:** A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible as shown in the following figure—



When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

2) Multipoint: A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link as shown in the following figure—



In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.

5. How networks can be classified depending on the geographical area covered by the network?

Depending on the geographical area covered by the networks; networks can be classified into following three basic categories—

1) Local Area Network: A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus. Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company and include audio and video peripherals. Currently, LAN size is limited to a few kilometers. LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware, software or data. LANs are distinguished from other types of networks by their transmission media and topology. Today, speeds of LANs are normally 100 or 1000 Mbps.

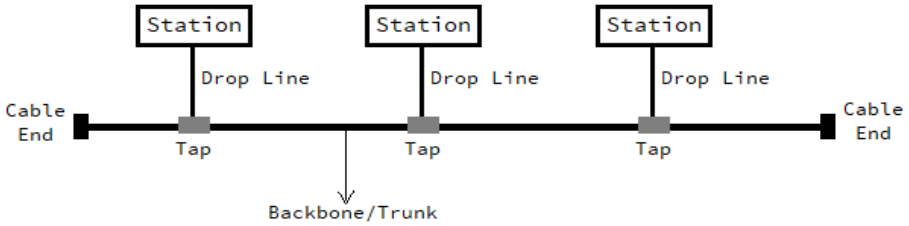
2) Metropolitan Area Networks: A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city. A good example of a MAN is the part of the telephone company network that can provide a high-speed DSL (Digital Subscriber Line) line to the customer. Another example is the cable TV network that originally was designed for cable TV, but today can also be used for high-speed data connection to the Internet.

3) Wide Area Network: A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world. A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet. We normally refer to the first as a switched WAN and to the second as a point-to-point WAN. The switched WAN connects the end systems, which usually comprise a router that connects to another LAN or WAN. The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (ISP). This type of WAN is often used to provide Internet access.

6. Define Topology? What are the different types of topologies available for LAN?

The term physical topology refers to the way in which a network is laid out physically. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies—

1) Liner or Bus Topology: In bus topology, there are multiple points and a long cable acts as a backbone to link all the devices in a network as shown in the following—



Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason, there is a limit on the number of taps a bus can support and on the distance between those taps.

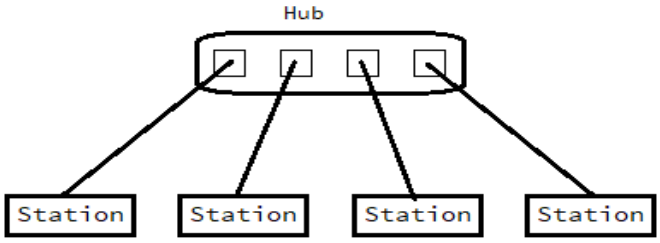
Advantages:

i. A bus topology is simple in structure, therefore, it can be easily implemented.
ii. A bus uses less cabling then mesh topology.
iii. In bus topology, redundancy of links is implemented, due to its backbone.

Disadvantages:

i. Reconnection and fault isolation is difficult.
ii. A fault or break in the backbone stopes all transmission, even between devices on the same side.
iii. Signal reflection at the taps can cause degradation in quality.

2) **Star Topology:** In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device as shown in the following figure—



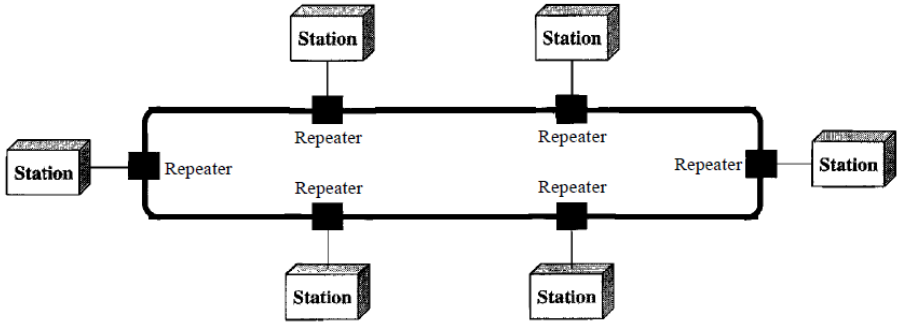
Advantages:

i. A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others.
ii. It is easy to install and reconfigure.
iii. It is robust. If one link fails, only that link will be effected.

Disadvantages:

i. A big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.
ii. Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies.

3) **Ring Topology:** In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along as shown in the following figure—



Advantages:

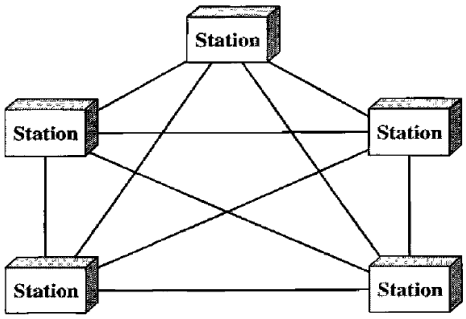
i. A ring is relatively easy to install and reconfigure.
ii. Fault isolation is simplified. Generally, in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

Disadvantages:

i. Unidirectional traffic can be a disadvantage. This weakness can be solved by using a dual ring or a switch capable of closing off the break, but it will be more expensive.
ii. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network.

4) Mesh Topology: In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node1 must be connected to n - I nodes, node2 must be connected to n – 1 nodes, and finally node n must be connected to n - 1 nodes. We need n(n - 1) physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need n(n -1) /2 duplex-mode links.

To accommodate that many links, every device on the network must have n – 1 input/output (I/O) ports to be connected to the other n - 1 stations as shown in the following figure—



Advantages:

i. In this topology the dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
ii. Mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
iii. There is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it.

Disadvantages:

i. Every device must be connected to every other device; therefore, more cabling is required.
ii. The hardware required to connect each link cab be very much expensive.
iii. Installation and reconnection are difficult due to the huge waring.

7. Write a short note on DQ.DB.

DQ.DB. is the abbreviation of Distributed Queue Dual Bus. This is a standard for implementation of MAN. DQ.DB. consist of two unidirectional buses to which all the computers are connected as shown in the following figure—

FIG

Each bus has a head-end, a device that initiates transmission accuracy. Traffic that is destined for computer write of the center uses the upper bus. Traffic to the left uses the lower bus. A key aspect of MAN is that there is a broadcast medium to which all the computers are attached. This greatly simplifies the design compare to other kinds of network.

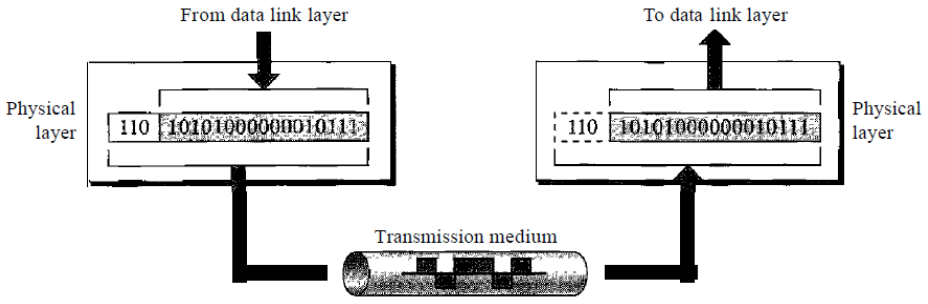
8. Explain ISO-OSI model with different layers.

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection model. It was first introduced in the late 1970s. An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

1) Physical Layer: The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to Occur. The following figure shows the position of the physical layer with respect to the transmission medium and the data link layer.



The physical layer is also concerned with the following:

i) Physical characteristics of interfaces and medium: The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.

ii) Representation of bits: The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of encoding (how 0s and 1s are changed to signals).

iii) Data rate: The transmission rate-the number of bits sent each second-is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.

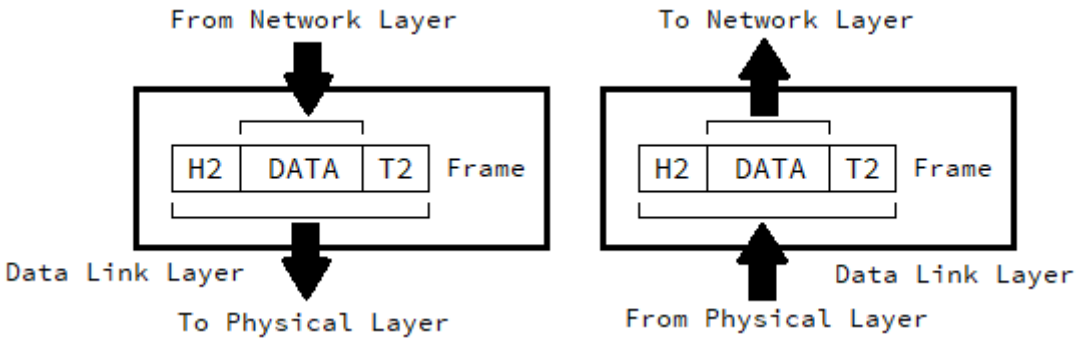
iv) Synchronization of bits: The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.

v) Line configuration: The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.

vi) Physical topology: The physical topology defines how devices are connected to make a network. Devices can be connected by using a mesh topology, a star topology, a ring topology, a bus topology, or a hybrid topology.

vii) Transmission mode: The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

2) Data Link Layer: The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer). The following figure shows the relationship of the data link layer to the network and physical layer.



The data link layer is responsible for moving frames from one hop (node) to the next. Other responsibilities of the data link layer include the following:

i) Framing: The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

ii) Physical addressing: If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.

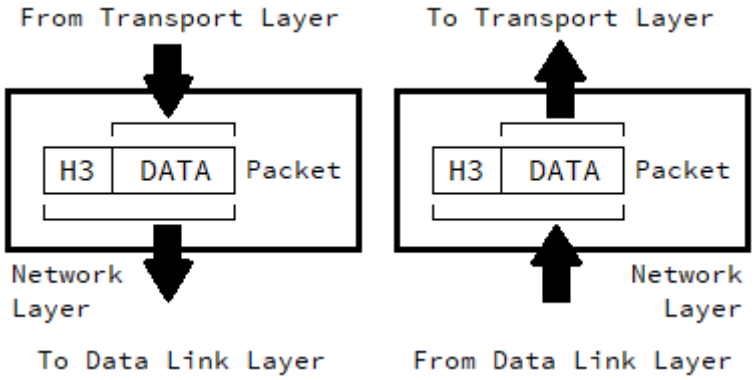
iii) Flow control: If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

iv) Error control: The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.

v) Access control: When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

3) Network Layer: The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.

If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery. The following figure shows the relationship of the network layer to the data link and transport layers.



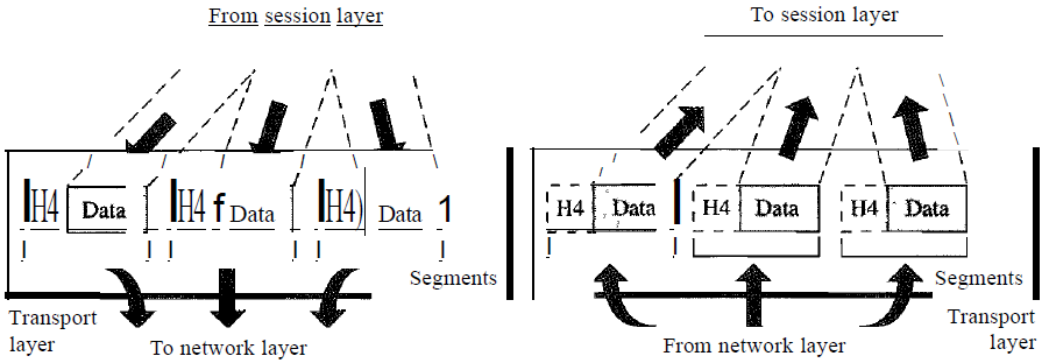
Other responsibilities of the network layer include the following:

i) Logical Addressing: The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.

ii) Routing: When independent networks or links are connected to create inter networks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

4) Transport Layer: The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

The following figure shows the relationship of the transport layer to the network and session layers.



Other responsibilities of the transport layer include the following:

i) Service-point addressing: Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

ii) Segmentation and reassembly: A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.

iii) Connection control: The transport layer can be either connectionless or connection-oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection-oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.

iv) Flow control: Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.

v) Error control: Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to-process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

5) Session Layer: The session layer is responsible for dialog control and synchronization. The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems.

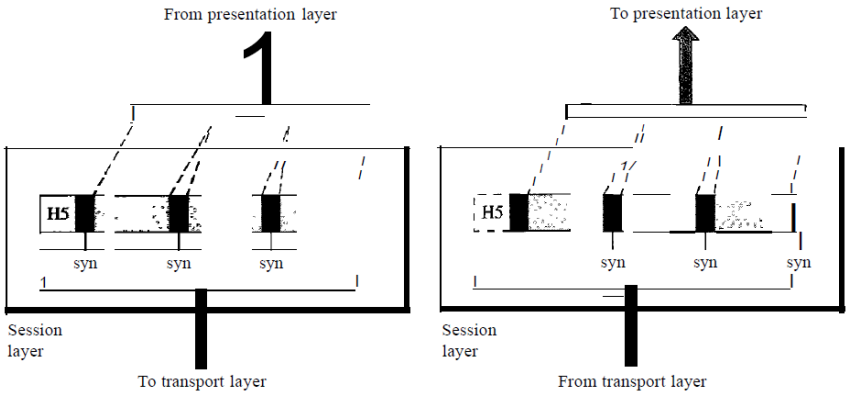
FIG

Specific responsibilities of the session layer include the following:

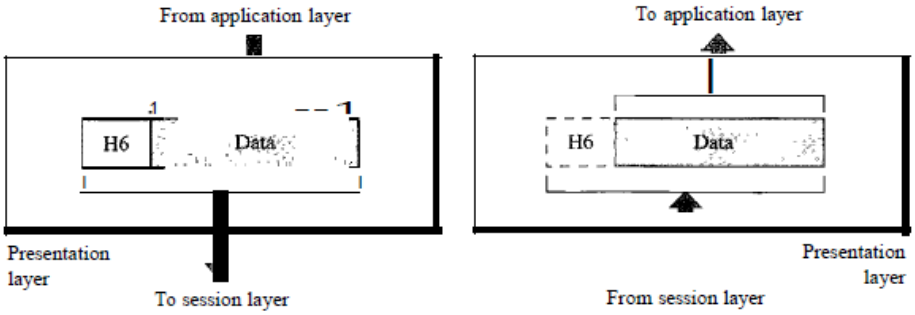
i) Dialog control: The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half-duplex (one way at a time) or full-duplex (two ways at a time) mode.

ii) Synchronization: The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

The following figure illustrates the relationship of the session layer to the transport and presentation layers—



6) Presentation Layer: The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems. The following figure shows the relationship between the presentation layer and the application and session layers—



Specific responsibilities of the presentation layer include the following:

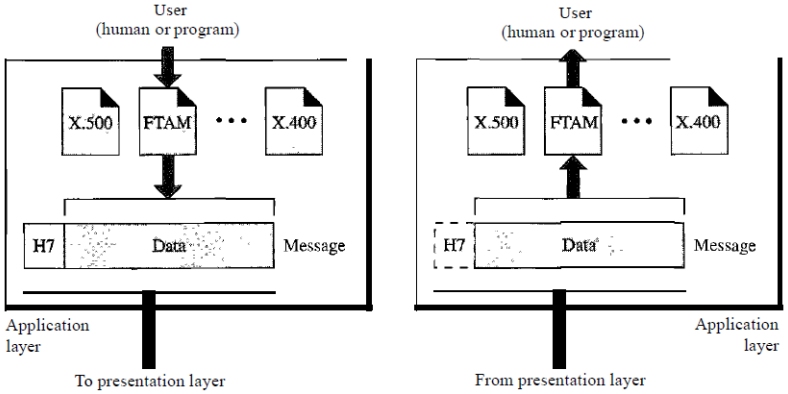
i) Translation: The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

ii) Encryption: To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

iii) Compression: Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

7) Application Layer: The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

The following figure shows the relationship of the application layer to the user and the presentation layer.



Specific services provided by the application layer include the following:

i) Network virtual terminal: A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.

ii) File transfer, access, and management: This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.

iii) Mail Services: This application provides the basis for e-mail forwarding and storage.

iv) Directory Services: This application provides distributed database sources and access for global information about various objects and services.

9. Explain TCP/IP Protocol suite.

The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. The following figure shows the different layers of TCP/IP protocol suite with their associated protocol.
FIG

TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality; however, the modules are not necessarily interdependent. The term hierarchical means that each upper-level protocol is supported by one or more lower-level protocols.

1) Host-to-Network Layer: At this layers, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a TCP/IP internetwork can be a local-area network or a wide-area network.

2) Network Layer (Inter-network Layer): At this layer, TCP/IP supports the Internetworking Protocol. IP, in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP.

i) Internetworking Protocol (IP): The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless protocol-a best-effort delivery service. The term *best effort* means that IP provides no error checking or tracking. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.

IP transports data in packets called *datagrams*, each of which is transported separately. Datagrams can travel along different routes and can arrive out of sequence or be duplicated. IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

ii) Address Resolution Protocol (ARP): The Address Resolution Protocol (ARP) is used to associate a logical address with a physical address. On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address, usually imprinted on the network interface card (NIC). ARP is used to find the physical address of the node when its Internet address is known.

iii) Reverse Address Resolution Protocol (RARP): The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address. It is used when a computer is connected to a network for the first time or when a diskless computer is booted.

iv) Internet Control Message Protocol (ICMP): The Internet Control Message Protocol (ICMP) is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender. ICMP sends query and error reporting messages.

iv) Internet Group Message Protocol (IGMP): The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

3) Transport Layer: Traditionally the transport layer was represented in TCP/IP by two protocols: TCP and UDP. IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another. UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process. A new transport layer protocol, SCTP, has been devised to meet the needs of some newer applications.

i) User Datagram Protocol (UDP): The User Datagram Protocol (UDP) is the simpler of the two standard TCP/IP transport protocols. It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

ii) Transmission Control Protocol (TCP): The Transmission Control Protocol (TCP) provides full transport-layer services to applications. TCP is a reliable stream transport protocol. The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data.

At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt, together with an acknowledgment number for the segments received. Segments are carried across the internet inside of IP datagrams. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

iii) Stream Control Transmission Control Protocol (SCTP): The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet. It is a transport layer protocol that combines the best features of UDP and TCP.

4) Application Layer: The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI mode. Many protocols are defined at this layer for the service for internet. Some of them are explained bellow—

i) Simple Mail Transfer Protocol (SMTP): The actual mail transfer is done through message transfer agents. To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA. The formal protocol that defines the MTA client and server in the Internet is called the Simple Mail Transfer Protocol (SMTP). As we said before, two pairs of MTA client/server programs are used in the most common situation.

SMTP is used two times, between the sender and the sender's mail server and between the two mail servers.

ii) File Transfer Protocol (FTP): File Transfer Protocol (FTP) is the standard mechanism provided by TCP/IP for copying a file from one host to another. Although transferring files from one system to another seems simple and straightforward, some problems must be dealt with first. For example, two systems may use different file name conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. All these problems have been solved by FTP in a very simple and elegant approach.

FTP differs from other client/server applications in that it establishes two connections between the hosts. One connection is used for data transfer, the other for control information (commands and responses). Separation of commands and data transfer makes FTP more efficient. FTP uses two well-known TCP ports: Port 21 is used for the control connection, and port 20 is used for the data connection.

iii) Hyper Text Transfer Protocol (HTTP): The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web. HTTP functions as a combination of FTP and SMTP. It is similar to FTP because it transfers files and uses the services of TCP. However, it is much simpler than FTP because it uses only one TCP connection. There is no separate control connection; only data are transferred between the client and the server.

HTTP is like SMTP because the data transferred between the client and the server look like SMTP messages. Unlike SMTP, the HTTP messages are not destined to be read by humans; they are read and interpreted by the HTTP server and HTTP client (browser). SMTP messages are stored and forwarded, but HTTP messages are delivered immediately.

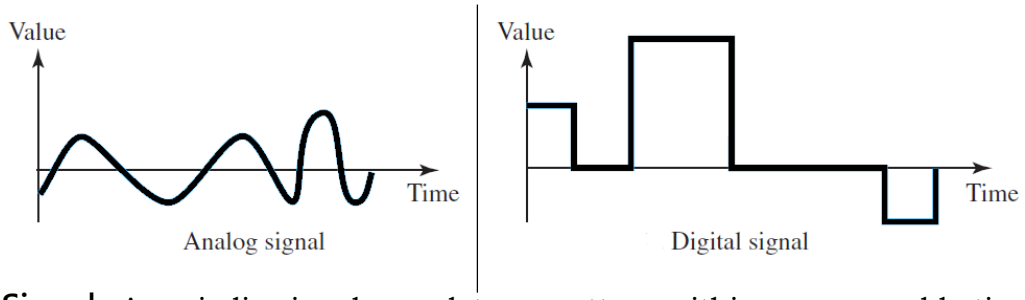
10. Define the following terms.

1) Digital Data: Digital data refers to information that has discrete states. For example, data stored in computer memory in the form of zeros and ones.

2) Analog Data: The term analog data refers to information that is continuous. For example, an analog clock that has hour, minute, and second hands gives information in a continuous form; the movements of the hands are continuous.

3) **Analog Signal:** An analog signal has infinitely many levels of intensity over a period of time. As the wave moves from value A to value B, it passes through and includes an infinite number of values along its path. The following figure shows an analog signal—

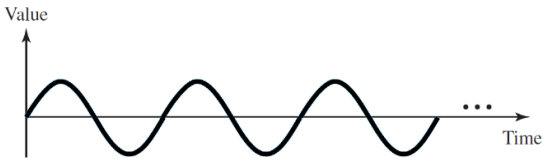
4) **Digital Signal:** A digital signal, on the other hand, can have only a limited number of defined values. Although each value can be any number, it is often as simple as 1 and 0. The following figure shows a digital signal—



5) **Periodic Signal:** A periodic signal completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle.

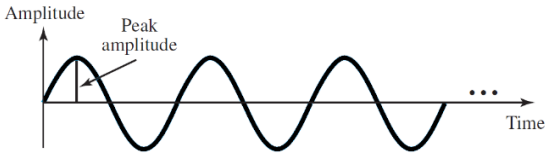
6) **Non-periodic Signal:** A non-periodic signal changes without exhibiting a pattern or cycle that repeats over time.

7) **Sine Wave:** The sine wave is the most fundamental form of a periodic analog signal. When we visualize it as a simple oscillating curve, its change over the course of a cycle is smooth and consistent, a continuous, rolling flow. The following figure shows a sine wave—



A sine wave can be represented by three parameters: the peak amplitude, the frequency, and the phase.

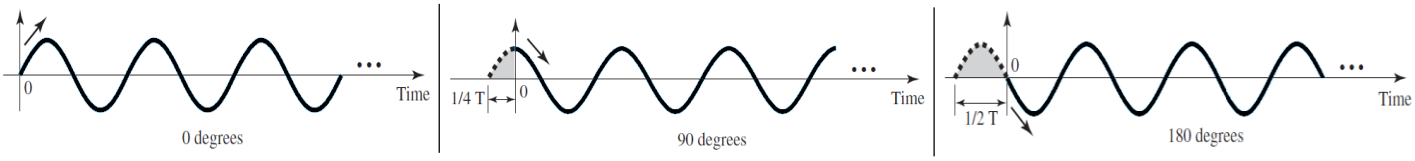
8) **Peak Amplitude:** The peak amplitude of a signal is the absolute value of its highest intensity, proportional to the energy it carries. For electric signals, peak amplitude is normally measured in volts. The following figure shows a signals and its peak amplitudes—



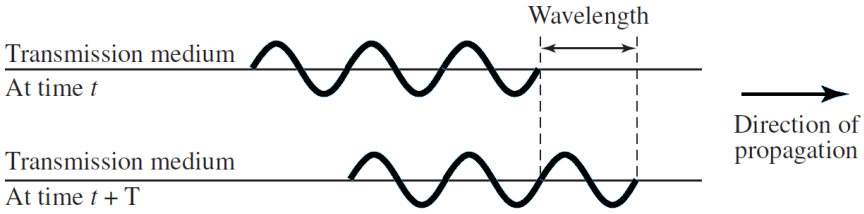
9) **Period:** Period refers to the amount of time, in seconds, a signal needs to complete 1 cycle. Period is the inverse of frequency. Therefore, we can write T=1/f. Period is formally expressed in seconds.

10) **Frequency:** Frequency refers to the number of periods in 1 s. Frequency is the inverse of period. Therefore, we can write f=1/T. Frequency is formally expressed in Hertz (Hz), which is *cycle per second.*

11) **Phase:** The term phase, or phase shift, describes the position of the waveform relative to time 0. If we think of the wave as something that can be shifted backward or forward along the time axis, phase describes the amount of that shift. It indicates the status of the first cycle. Phase is measured in degrees or radians. A phase shift of 360° corresponds to a shift of a complete period; a phase shift of 180° corresponds to a shift of one-half of a period; and a phase shift of 90° corresponds to a shift of one-quarter of a period. The following figure shows sine wave with different phases—



12) **Wavelength:** Wavelength is another characteristic of a signal traveling through a transmission medium. Wavelength binds the period or the frequency of a simple sine wave to the propagation speed of the medium. The following figure shows the concept of wave length—



While the frequency of a signal is independent of the medium, the wavelength depends on both the frequency and the medium. Wavelength is a property of any type of signal. In data communications, we often use wavelength to describe the transmission of light in an optical fiber. The wavelength is the distance a simple signal can travel in one period.

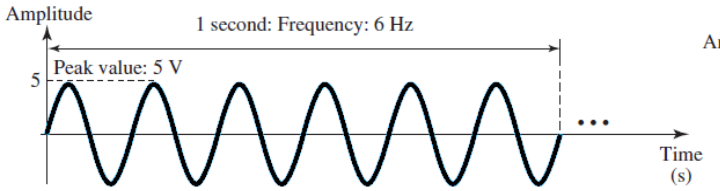
Wavelength can be calculated if one is given the propagation speed (the speed of light) and the period of the signal. However, since period and frequency are related to each other, if we represent wavelength by λ, propagation speed by c (speed of light), and frequency by f, we get

$$\text{Wavelength} = (\text{propagation speed}) \times \text{period} = \frac{\text{propagation speed}}{\text{frequency}}$$

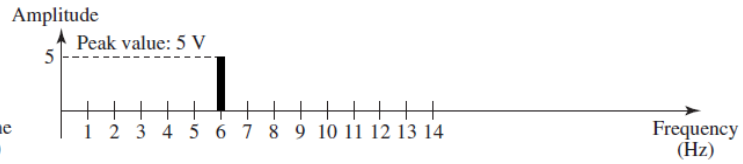
$$\lambda = \frac{c}{f}$$

13) **Time Domain:** We can show a sine wave by using a time domain plot. This time domain plot shows changes in signal amplitude with respect to time. The following the time domain of a sine wave.

14) **Frequency Domain:** The relationship between amplitude and frequency, is shown in the following graph, what is called a frequency-domain plot. A frequency-domain plot is concerned with only the peak value and the frequency.

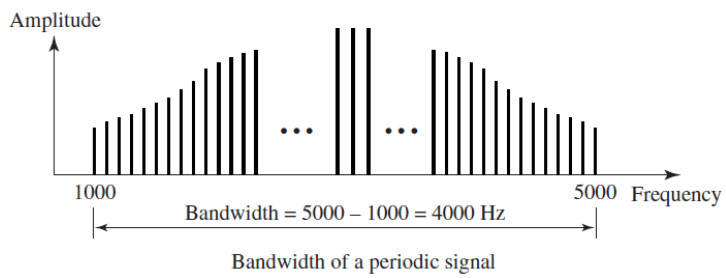


A sine wave in the time domain (peak value: 5 V, frequency: 6 Hz)

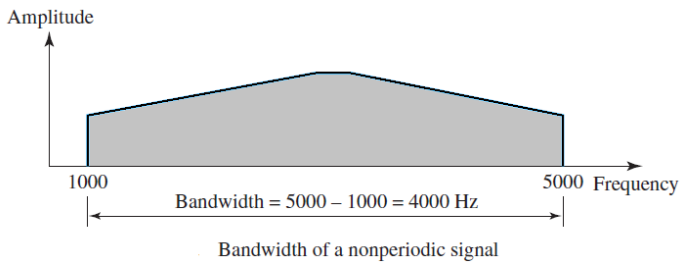


The same sine wave in the frequency domain (peak value: 5 V, frequency: 6 Hz)

15) **Bandwidth:** The range of frequencies contained in a composite signal is its bandwidth. The bandwidth is normally a difference between two numbers. For example, if a composite signal contains frequencies between 1000 and 5000, its bandwidth is 5000 − 1000, or 4000. The following figure shows the concept of bandwidth.

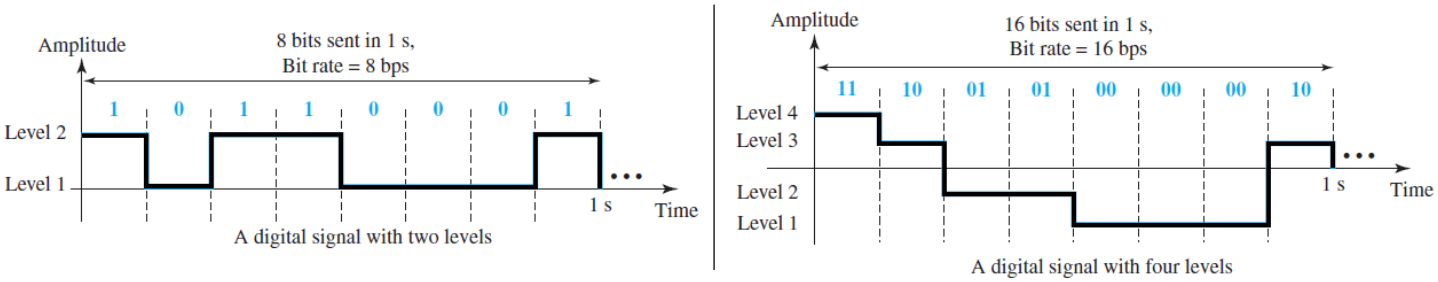


Bandwidth of a periodic signal



Bandwidth of a nonperiodic signal

16) **Bit Rate:** Most digital signals are non-periodic, and thus period and frequency are not appropriate characteristics. Another term—bit rate (instead of frequency)—is used to describe digital signals. The bit rate is the number of bits sent in 1s, expressed in bits per second (bps). Figure 3.17 shows the bit rate for two signals.



17) **Bit Length:** Wave length is associated with an analog signal; similarly, for a digital signal bit length is used. The bit length is the distance one bit occupies on the transmission medium. Therefore,

Bit length = propagation speed x bit duration

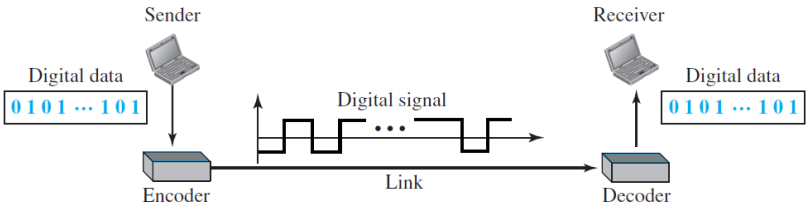
18) **Baseband Transmission:** Baseband transmission means sending a digital signal over a channel without changing the digital signal to an analog signal. Baseband transmission requires that we have a low-pass channel, a channel with a bandwidth that starts from zero. This is the case if we have a dedicated medium with a bandwidth constituting only one channel. For example, the entire bandwidth of a cable connecting two computers is one single channel.

19) **Broadband Transmission:** Broadband transmission or modulation means changing the digital signal to an analog signal for transmission. Modulation allows us to use a bandpass channel—a channel with a bandwidth that does not start from zero.

11. Explain different technique to convert digital data to digital signal.

The following are the different technique to convert digital data to digital signal—

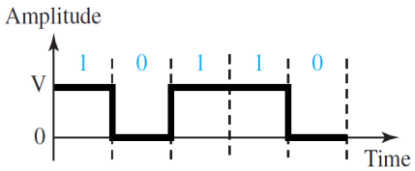
1) **Line Coding:** Line coding is the process of converting digital data to digital signals. We assume that data, in the form of text, numbers, graphical images, audio, or video, are stored in computer memory as sequences of bits (see Chapter 1). Line coding converts a sequence of bits to a digital signal. At the sender, digital data are encoded into a digital signal; at the receiver, the digital data are recreated by decoding the digital signal. The following figure shows the process.



We can roughly divide line coding schemes into five broad categories— Unipolar, Polar, Bipolar, Multilevel and Multitransition.

i) **Unipolar:** In a unipolar scheme, all the signal levels are on one side of the time axis, either above or below.

a) **NRZ (Non-Return-to-Zero):** Traditionally, a unipolar scheme was designed as a non-return-to-zero (NRZ) scheme in which the positive voltage defines bit 1 and the zero voltage defines bit 0. It is called NRZ because the signal does not return to zero at the middle of the bit. The following figure shows a unipolar NRZ scheme.

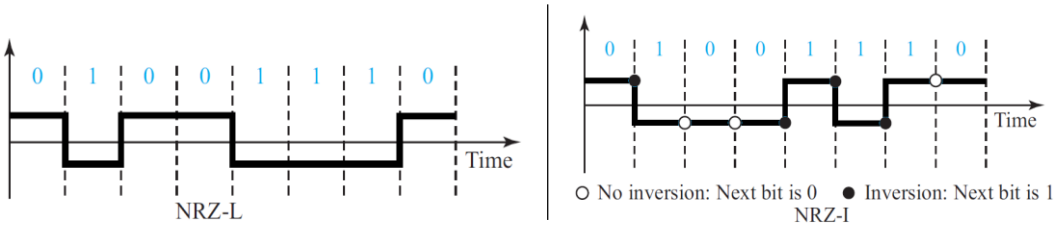


ii) Polar Schemes: In polar schemes, the voltages are on both sides of the time axis. For example, the voltage level for 0 can be positive and the voltage level for 1 can be negative.

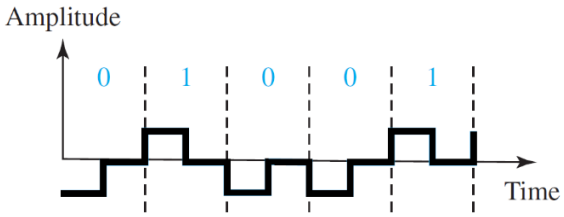
a) Non-Return-to-Zero (NRZ): In polar NRZ encoding, we use two levels of voltage amplitude. We can have two versions of polar NRZ—

I) NRZ-L (NRZ-Level): In this schema the level of voltage determines the value of bit. For example, consider the following encoding—

II) NRZ-I (NRZ-Invert): In this schema the change or lack of change in the level of the voltage determines the value of the bit. If there is no change the bit is zero. If there is a change, the bit is one.



b) Return-to-Zero (RZ): The main problem with NRZ encoding occurs when the sender and receiver clocks are not synchronized. The receiver does not know when one bit has ended and the next bit is starting. One solution is the return-to-zero (RZ) scheme, which uses three values: positive, negative, and zero. In RZ, the signal changes not between bits but during the bit. In the following figure we see that the signal goes to 0 in the middle of each bit. It remains there until the beginning of the next bit.

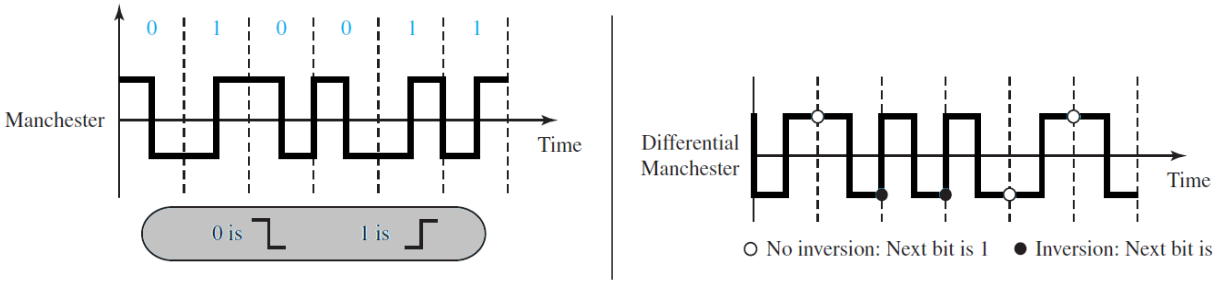


The main disadvantage of RZ encoding is that it requires two signal changes to encode a bit and therefore occupies greater bandwidth. Another problem is the complexity: RZ uses three levels of voltage, which is more complex to create and discern.

c) Biphase:

I) Manchester: The idea of RZ (transition at the middle of the bit) and the idea of NRZ-L are combined into the Manchester scheme. In Manchester encoding, the duration of the bit is divided into two halves. The voltage remains at one level during the first half and moves to the other level in the second half. The transition at the middle of the bit provides synchronization. The following figure shows the Manchester encoding.

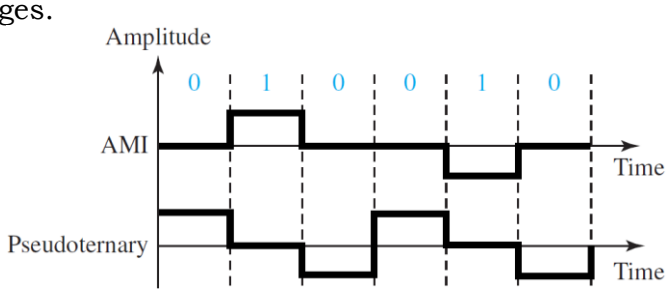
II) Differential Manchester: Differential Manchester, on the other hand, combines the ideas of RZ and NRZ-I. There is always a transition at the middle of the bit, but the bit values are determined at the beginning of the bit. If the next bit is 0, there is a transition; if the next bit is 1, there is none. The following figure shows the Differential Manchester encoding.



iii) Bipolar Schemes: In bipolar encoding (sometimes called multilevel binary), there are three voltage levels: positive, negative, and zero. The voltage level for one data element is at zero, while the voltage level for the other element alternates between positive and negative.

***. AMI and Pseudoternary:** The following figure shows two variations of bipolar encoding: AMI and pseudoternary. A common bipolar encoding scheme is called bipolar alternate mark inversion (AMI). In the term alternate mark inversion, the word mark comes from telegraphy and

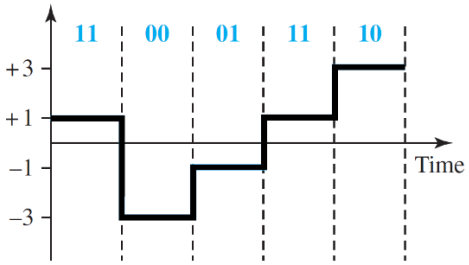
means 1. So AMI means alternate 1 inversion. A neutral zero voltage represents binary 0. Binary 1s are represented by alternating positive and negative voltages. A variation of AMI encoding is called pseudoternary in which the 1 bit is encoded as a zero voltage and the 0 bit is encoded as alternating positive and negative voltages.



iv) Multilevel Schemes: The desire to increase the data rate or decrease the required bandwidth has resulted in the creation of many schemes. The goal is to increase the number of bits per baud by encoding a pattern of m data elements into a pattern of n signal elements. We only have two types of data elements (0s and 1s), which means that a group of m data elements can produce a combination of 2m data patterns. We can have different types of signal elements by allowing different signal levels. If we have L different levels, then we can produce Ln combinations of signal patterns. If 2m = Ln, then each data pattern is encoded into one signal pattern. If 2m < Ln, data patterns occupy only a subset of signal patterns. The subset can be carefully designed to prevent baseline wandering, to provide synchronization, and to detect errors that occurred during data transmission. Data encoding is not possible if 2m > Ln because some of the data patterns cannot be encoded.

The code designers have classified these types of coding as mBnL, where m is the length of the binary pattern, B means binary data, n is the length of the signal pattern, and L is the number of levels in the signaling. A letter is often used in place of L: B (binary) for L = 2, T (ternary) for L = 3, and Q (quaternary) for L = 4. Note that the first two letters define the data pattern, and the second two define the signal pattern.

a) 2B1Q (two binary, one quaternary): 2B1Q uses data patterns of size 2 and encodes the 2-bit patterns as one signal element belonging to a four-level signal. In this type of encoding m = 2, n = 1, and L = 4 (quaternary). The following figure shows an example of a 2B1Q signal—



	Previous Level (+)ve	Previous Level (-)ve
Next Bits	Next Level	Next Level
00	+1	-1
01	+3	-3
10	-1	+1
11	-3	+3

Transaction Table

v) Multiline transmission (MLT-3): NRZ-I and differential Manchester are classified as differential encoding but use two transition rules to encode binary data (no inversion, inversion). If we have a signal with more than two levels, we can design a differential encoding scheme with more than two transition rules. MLT-3 is one of them. The multiline transmission, three-level (MLT-3) scheme uses three levels (+V, 0, and −V) and three transition rules to move between the levels—

i. If the next bit is 0, there is no transition.
ii. If the next bit is 1 and the current level is not 0, the next level is 0.
iii. If the next bit is 1 and the current level is 0, the next level is the opposite of the last nonzero level.