Answer Key-

1. What do you understand by Data Communication? Explain the Application of Computer Networks?

DATA COMMUNICATIONS

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: delivery, accuracy, timeliness, and jitter.

Applications of Computer Network

There are multiple applications of computer networks including:

- **Business applications:** Computer networks are widely used in businesses to improve communication, share resources, and enable remote access.
- **Educational applications:** Computer networks are used extensively in educational institutions to facilitate distance learning, provide access to educational resources, and enable collaboration among students and teachers.
- **Healthcare applications:** Computer networks are used in healthcare to store and share patient information, enabling healthcare professionals to provide more personalized care.
- **Entertainment applications:** Computer networks are used for entertainment purposes such as online gaming, streaming movies and music, and social media.
- **Military applications:** Computer networks are used in military applications to provide secure communication and information sharing among military personnel.
- **Scientific applications:** Computer networks are used in scientific research to facilitate collaboration among researchers and share data and information.
- **Transportation applications:** Computer networks are used in transportation to manage traffic, track vehicles, and improve transportation efficiency.
- **Banking and finance applications:** Computer networks are used in banking and finance to process transactions, share information, and provide secure access to financial services.

2. With a neat diagram, Explain OSI Model.

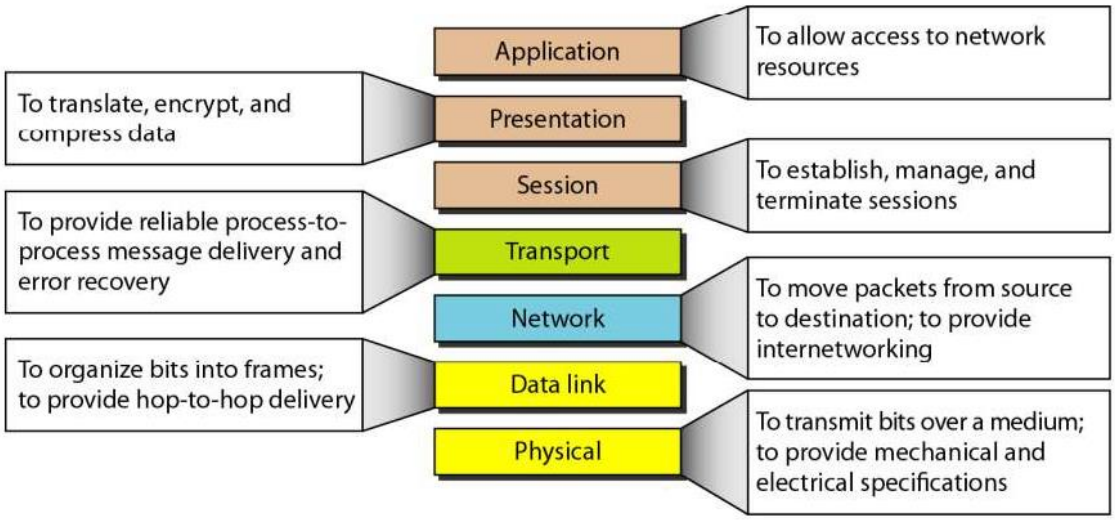
2-2 THE OSI MODEL

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 (OSI) model. It was first introduced in the late 1970s.

•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.

- **The OSI model is not a protocol;**
- **it is a model for understanding and designing a network architecture that is**
  - **flexible, robust, and interoperable.**



LAYERS IN THE OSI MODEL

Physical Layer: The physical layer is responsible for movements of individual bits from one hop (node) to the next.
Data Link Layer: The data link layer is responsible for moving frames from one hop (node) to the next.
Network Layer: The network layer is responsible for the delivery of individual packets from the source host to the destination host.
Transport Layer: The transport layer is responsible for the delivery of a message from one process to another.
Session Layer: The session layer is responsible for dialog control and synchronization.
Presentation Layer: The presentation layer is responsible for translation, compression, and encryption.
Application Layer: The application layer is responsible for providing services to the user.

3. What are the different types/categories of the networks? Explain in detail and differentiate them.

Categories of Networks:

The category into which a network falls is determined by its size.
A LAN normally covers an area less than 2 mi;
A WAN can be worldwide. Networks of a size in between are normally referred to as metropolitan area networks and span tens of miles.
•

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 kilometres.
LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data. In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star. Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps.

Wide Area Network

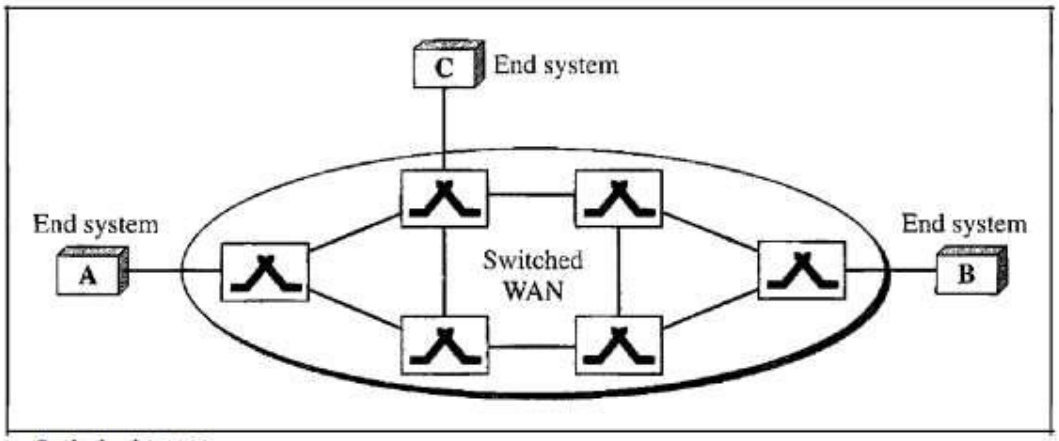
A wide area network (WAN) provides long distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world. A WAN can be as complex as the backbones that connect the Internet-->switched WAN or as simple as a dial up line that connects a home computer to the Internet -->point to point WAN.
The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) 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 (lSP). This type of WAN is often used to provide Internet access.
An early example of a switched WAN is X.25. A good example of a switched WAN is the asynchronous transfer mode (ATM) network, which is a network with fixed size data unit packets called cell.

Metropolitan Area Network:

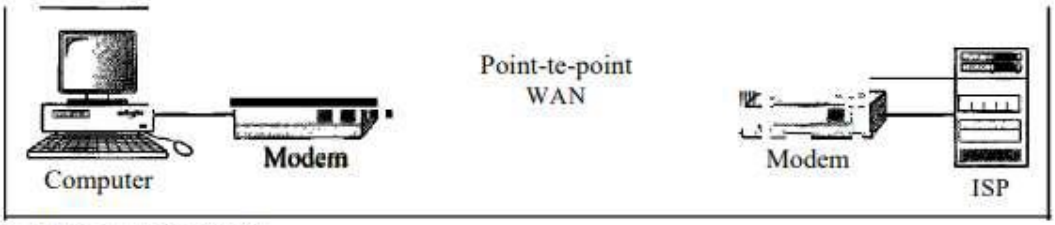
A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high-speed

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 line to the customer.

1.11 *WANs: a switched WAN and a point-to-point WAN*



a. Switched WAN



b. Point-to-point WAN

4. What is the difference between a port address, a logical address, and a physical address?

1. Physical Address

i. Physical Address is the lowest level of addressing, also known as link address.

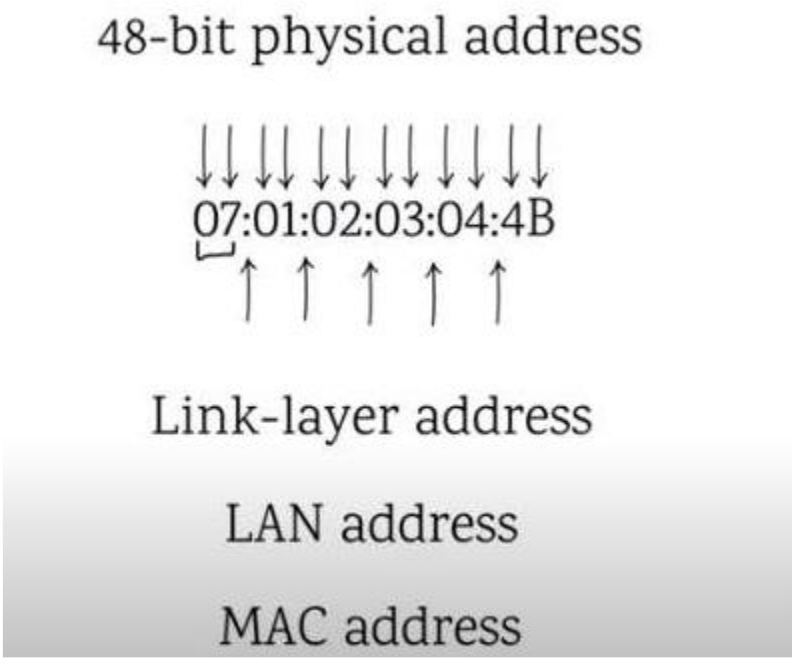
ii. It is local to the network to which the device is connected and unique inside it.

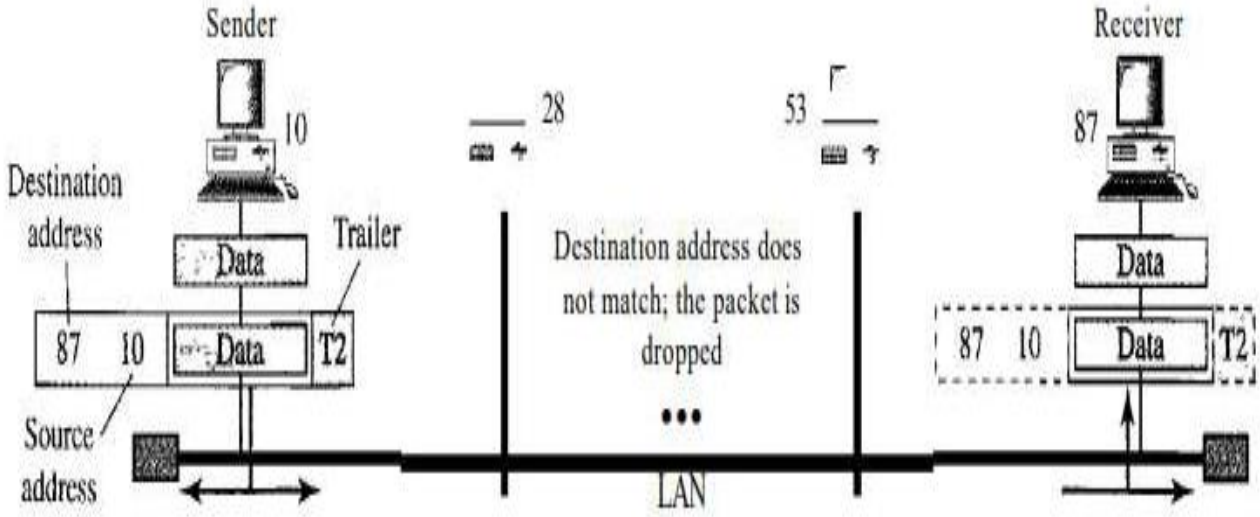
iii. The physical address is usually included in the frame and is used at the data link layer.

iv. MAC is a type of physical address that is 6 byte (48 bit) in size and is imprinted on the Network Interface Card (NIC) of the device.

v. The size of physical address may change depending on the type of network. Ex. An Ethernet network uses a 6 byte MAC address.


Physical address
hardware-level address
network interface card
Belkin, Nortel, Cisco


48-bit physical address
07:01:02:03:04:4B
Link-layer address
LAN address
MAC address



2. Logical Address

i. Logical Addresses are used for universal communication.

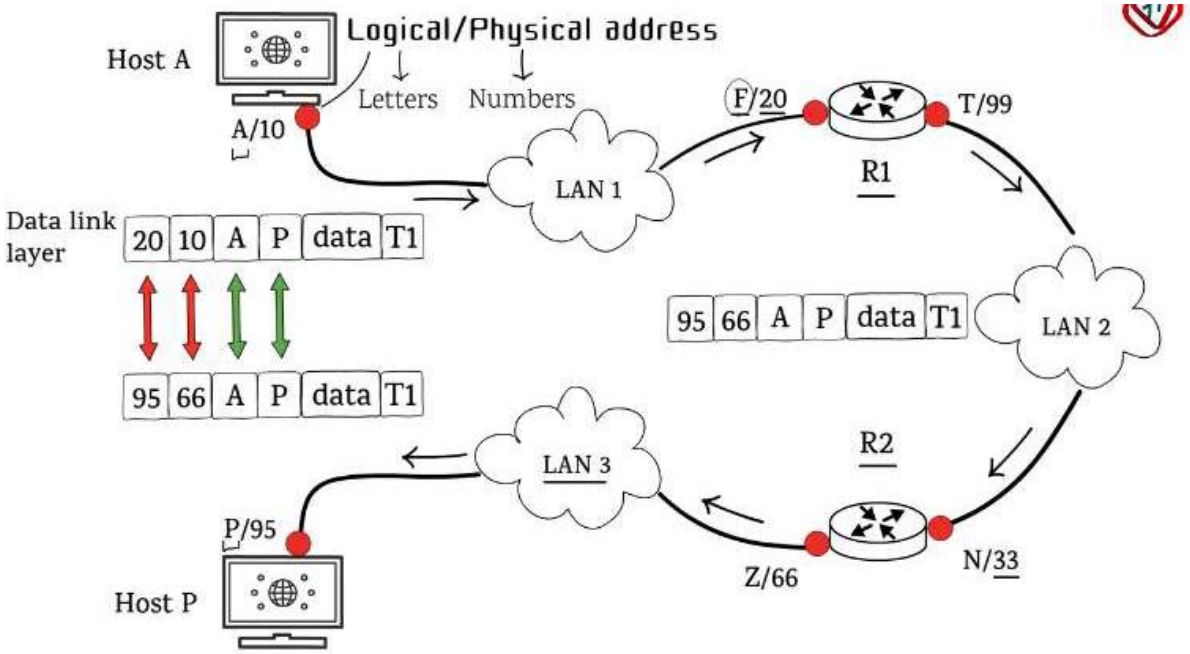
ii. Most of the times the data has to pass through different networks; since physical addresses are local to the network there is a possibility that they may be duplicated across multiples networks also the type of physical address being used may change with the type of network encountered. For ex: Ethernet to wireless to fiber optic. Hence physical addresses are inadequate for source to destination delivery of data in an internetwork environment.

iii. Logical Address is also called as IP Address (Internet Protocol address).

iv. At the network layer, device i.e. computers and routers are identified universally by their IP Address.

v. IP addresses are universally unique.

vi. Currently there are two versions of IP addresses being used:
   a. **IPv4**: 32 bit address, capable of supporting 2^{32} nodes
   b. **IPv6:** 128 bit address, capable of supporting 2^{128} nodes



3. Port Address

VIII. A logical address facilitates the transmission of data from source to destination device. But the source and the destination both may be having multiple processes communicating with each other.

Ex. Users A & B are chatting with each other using Google Talk, Users B & C are exchanging emails using Hotmail. The IP address will enable transmitting data from A to B, but still the data needs to be delivered to the correct process. The data from A cannot be given to B on yahoo messenger since A & B are communicating using Google Talk.

IX. Since the responsibility of the IP address is over here there is a need of addressing that helps identify the source and destination processes. In other words, data needs to be delivered not only on the correct device but also on the correct process on the correct device.

X. A Port Address is the name or label given to a process. It is a 16 bit address.

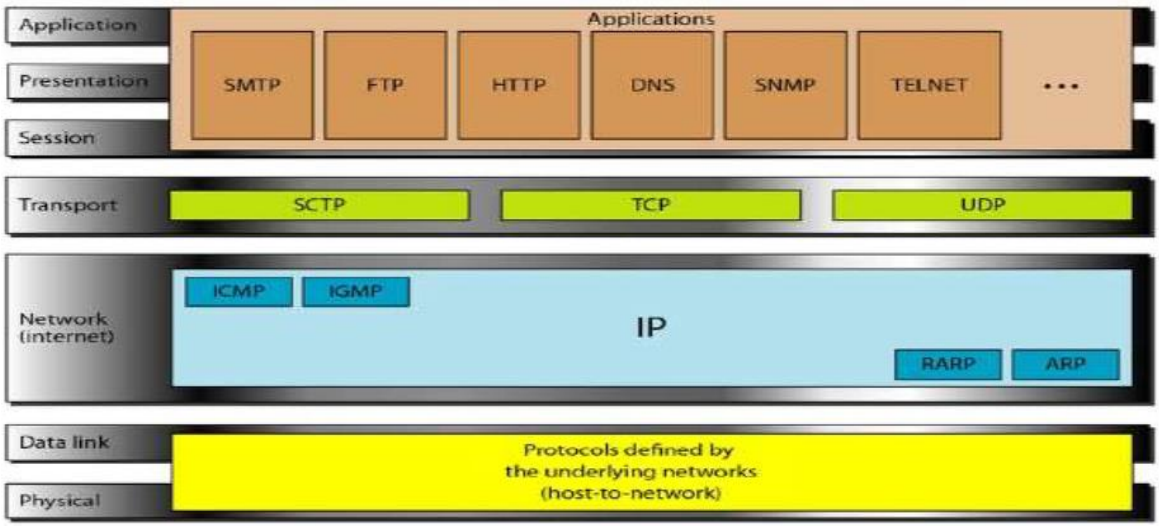
XI. Ex. TELNET uses port address 23, HTTP uses port address 80

5. With a neat diagram, Explain TCP/IP Protocol Suite.

TCP/IP MODEL

•It is also called as the TCP/IP protocol suite. It is a collection of protocols
•It is a hierarchical model, i.e. There are multiple layers and higher layer protocols are supported by lower layer protocols
•It existed even before the OSI model was developed.
•Originally had four layers (bottom to top):
•1. Host to Network Layer
•2. Internet Layer
•3. Transport Layer
•4. Application Layer

•The structure TCP/IP model is very similar to the structure of the OSI reference model. The OSI model has seven layers where the TCP/IP model has four layers. The Application layer of TCP/IP model corresponds to the Application Layer of Session, Presentation & Application Layer of OSI model. The Transport layer of TCP/IP model corresponds to the Transport Layer of OSI model, The Network layer of TCP/IP model corresponds to the Network Layer of OSI model. The Host to network layer of TCP/IP model corresponds to the Physical and Datalink Layer of OSI model.
The diagram showing the comparison of OSI model and TCP/IP model along with the protocols is as shown below



Functions of the Layers of TCP/IP model:

A. Host to Network Layer:

This layer is a combination of protocols at the physical and data link layers. It supports all standard protocols used at these layers

B. Network Layer:

•The network layer is responsible for source to destination transmission of data.

• The network layer is also responsible for routing the packet.

• The routers choose the best route for each packet.

•At the network layer (or, more accurately, the internetwork layer), TCP/IP supports the Internetworking Protocol.

•IP is a combination of four protocols:

•1. ARP

•2. RARP

•3. ICMP

•4. IGMP

•IP defines the format and the structure of addresses.

•IP transports data in packets called datagrams

- It is a connectionless & unreliable protocol.
  - i) Connection-less means there is no connection setup b/w the sender and the receiver.
  - ii) Unreliable protocol means → IP does not make any guarantee about delivery of the data. → Packets may get dropped during transmission. It provides a best-effort delivery service.
  - Best effort means IP does its best to get the packet to its destination, but with no guarantees. IP does not provide following services → flow control → error control → congestion control services.
  - If an application requires above services, the application should rely only on the transport layer protocol.

1. ARP – Address Resolution Protocol

ARP is used to find the physical-address of the node when its Internet-address is known. Physical address is the 48-bit address that is imprinted on the NIC or LAN card. Internet address (IP address) is used to uniquely & universally identify a device in the internet.

2. RARP– Reverse Address Resolution Protocol

It is used by a device on the network to find its Internet address when it knows its physical address.

3. ICMP- Internet Control Message Protocol

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.

4. IGMP- Internet Group Message Protocol

It is a mechanism that allows to send the same message to a group of recipients.

- **C. Transport Layer :**

Transport layer protocols are responsible for transmission of data running on a process of one machine to the correct process running on another machine.

The transport layer contains three protocols:

1. TCP
2. UDP
3. SCTP

1. **TCP – Transmission Control Protocol**
   - I. TCP is a reliable connection-oriented, reliable protocol. i.e. a connection is established between the sender and receiver before the data can be transmitted.
   - II. It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data.
2. **UDP – User Datagram Protocol**
   - I. UDP is a simple protocol used for process to process transmission.
   - II. It is an unreliable, connectionless protocol for applications that do not require flow control or error control.
   - III. It simply adds port address, checksum and length information to the data it receives from the upper layer.
3. **SCTP – Stream Control Transmission Protocol**
   - I. SCTP is a relatively new protocol added to the transport layer of TCP/IP protocol suite.
   - II. It combines the features of TCP and UDP.
   - III. It is used in applications like voice over Internet and has a much broader range of applications

D. Application Layer

The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and define high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

6.What are the types of Data Representation and Transmission Modes?

Data Representation

Text :

- In data communications, text is represented as a bit pattern, a sequence of bits (Os or Is)
- Different sets of bit patterns have been designed to represent text symbols.
- Each set is called a code, and the process of representing symbols is called coding.

Numbers :

Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations.

Images : Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the resolution. For example, an image can be divided into 1000 pixels or 10,000 pixels.

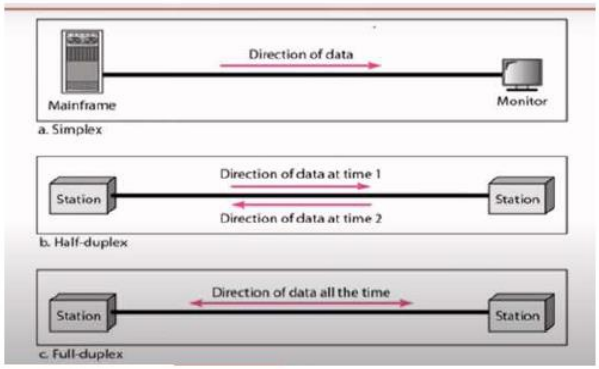
Audio : Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete. Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal.

Video : Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion.

Data Flow [Transmission Mode]:

Communication between two devices can be

1. Simplex
2. Half Duplex
3. Full Duplex



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.

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.

Full-Duplex

In full-duplex **mode** (also called duplex), both stations can transmit and receive simultaneously

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. When two people are communicating by a telephone line, both can talk and listen at the same time.

7.Explain any two in detail- a) Internetworking b) the Internet c) Protocol & Standards.

A) Internetworking-

Internetworking is combined of 2 words, inter and networking which implies an association between totally different nodes or segments. This connection area unit is established through intercessor devices akin to routers or gateway. The first term for associate degree internetwork was catenet. This interconnection is often among or between public, private, commercial, industrial, or governmental networks. Thus, associate degree internetwork could be an assortment of individual networks, connected by intermediate networking devices, that function as one giant network. Internetworking refers to the trade, products, and procedures that meet the challenge of making and administering internet works.

To enable communication, every individual network node or phase is designed with a similar protocol or communication logic, that is Transfer Control Protocol (TCP) or Internet Protocol (IP). Once a network communicates with another network having constant communication procedures, it's called Internetworking. Internetworking was designed to resolve the matter of delivering a packet of information through many links.

There is a minute difference between extending the network and Internetworking. Merely exploitation of either a switch or a hub to attach 2 local area networks is an extension of LAN whereas connecting them via the router is an associate degree example of Internetworking.

B) Internet:

1.3 THE INTERNET

- The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time.
- The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.

A Brief History :

- A network is a group of connected communicating devices such as computers and printers.
- An internet (note the lowercase letter i) is two or more networks that can communicate with each other.
- The most notable internet is called the Internet (uppercase letter I), a collaboration of more than hundreds of thousands of interconnected networks.
- In the mid-1960s, mainframe computers in research organizations were standalone devices. Computers from different manufacturers were unable to communicate with one another.

- The Advanced Research Projects Agency (ARPA) in the Department of Defense (DoD) was interested in finding a way to connect computers.
- In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers.
- The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an inteiface message processor (IMP).
- The IMPs, in tum, would be connected to one another. Each IMP had to be able to communicate with other IMPs as well as with its own attached host.
- By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of Utah, were connected via the IMPs to form a network. Software called the Network Control Protocol (NCP) provided communication between the hosts.
- In 1972, Vint Cerf and Bob Kahn, outlined the protocols(TCP) to achieve end-to-end delivery of packets.
- Shortly thereafter, authorities made a decision to split TCP into two protocols: Transmission Control Protocol (TCP) and Internetworking Protocol (IP). IP would handle datagram routing while TCP would be responsible for higher-level functions such as segmentation, reassembly, and error detection. The internetworking protocol became known as TCPIIP

c) Protocol & Standards-

1.4 PROTOCOLS AND STANDARDS

- A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated.
- The key elements of a protocol are syntax, semantics, and timing.
- Syntax :
  - The term syntax refers to the structure or format of the data, meaning the order in which they are presented. How to read the bits.
    - Eg: a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.
- Semantics:
  - semantics interprets the meaning of each section of bits.
  - what action is to be taken based on that interpretation.

    For example, does an address identify the route to be taken or the final destination of the message?
- Timing:
  - Timing refers to two characteristics: when data should be sent and how fast they can be sent.
  - For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

Standards:

- Standards provide guidelines to product manufacturers and vendors to ensure national and international interconnectivity.
- Data communications standards are classified into two categories:

1. De facto Standard
2. De jure standard

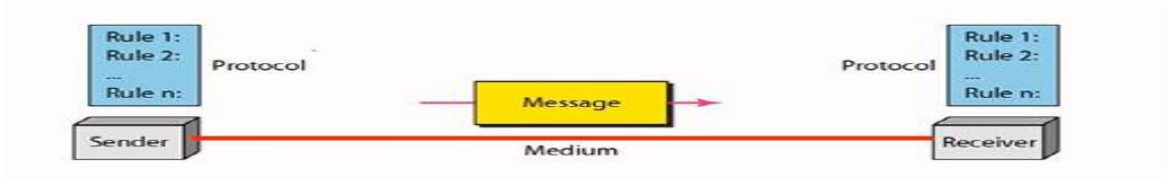
- Standard organizations
  - International Organization for Standardization (ISO)
  - International Telecommunication Union-Telecommunication standards sector (ITU-T)
    - Consultative Committee for International Telegraphy and Telephony (CCITT)
  - American National Standards Institute (ANSI)
  - Institute of Electrical and Electronics Engineers (IEEE)
  - Electronic Industries Association (EIA)

8. What are the Fundamental Characteristics and Components of Data Communication.

- 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 (program)**.
- Fundamental characteristics influence the effectiveness of a data communications system
  - Delivery
  - Accuracy
  - Timeliness
  - Jitter

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. For example, let us assume that video packets are sent every 3D ms. If some of the packets arrive with 3D-ms delay and others with 4D-ms delay, an uneven quality in the video is the result.

Components of Data Communications



- Message:
  - The information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
- Sender:
  - The device that sends the data message.
  - It can be a computer, workstation, telephone handset, video camera, and so on.
- Receiver:
  - The device that receives the data message.
- Transmission medium:
  - The physical path by which a message travels from sender to receiver.
  - e.g., twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
- Protocol:
  - A set of rules that govern data communications.
  - It represents an agreement between the communication devices.

9. What are the Criteria to analyze the Network? Explain Different Network Metrics with proper definition.

Network Criteria :

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

1. **Performance** :

Performance can be measured in many ways, including transit time and response time.

Transit time is the amount of time required for a message to travel from one device to another.

Response time is the elapsed time between an inquiry and a response.

The performance of a network depends on a number of factors:

- number of users,
- the type of transmission medium,
- the capabilities of the connected hardware,
- the efficiency of the software.

Performance is often evaluated by two networking metrics:

- Throughput
- delay

We often need more throughput and less delay. However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

2. **Reliability:**

Network reliability is measured by the

- frequency of failure
- the time it takes a link to recover from a failure
- the network's robustness in a catastrophe.

3. **Security :**

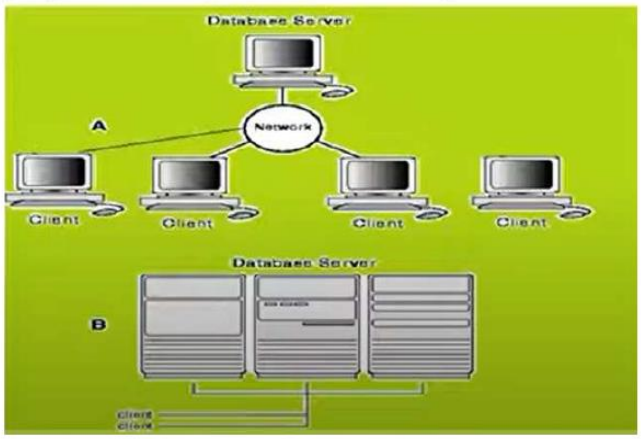
Network security issues include

- protecting data from unauthorized access
- protecting data from damage and development
- implementing policies and procedures for recovery from breaches and data losses

10. Explain Distribute and Centralized Processing with example.

Distributed Processing :

Most networks use distributed processing, in which a task is divided among multiple computers. Instead of one single large machine being responsible for all aspects of a process, separate computers (usually a personal computer or workstation) handle a subset.



Centralised Processing:

Centralized systems are the most intuitive and easy to understand and define.
Centralized systems are systems that use client/server architecture where one or more client nodes are directly connected to a central server. This is the most commonly used type of system in many organizations where a client sends a request to a company server and receives the response.

Characteristics of Centralized Systems

- Run on a single computer system and do not interact with another computer system.
- A modern, general-purpose computer system consists of one to a few processors and a number of device controllers that are connected through a common bus that provides access to shared memory.
- The processors have local cache memories that store local copies of parts of the memory, to speed up access to data.
- Centralized systems have specialized device controllers responsible for managing various hardware components, such as disk drives and audio devices
- A typical single-user system is a desktop unit used by a single person, usually with only one processor and one or two hard disks, and usually only one person using the machine at a time.

- A typical multiuser system, has more disks and more memory and may have multiple processors. It serves a large number of users who are connected to the system remotely.
- Database systems designed for use by single users usually do not provide many of the facilities that a multiuser database provides.
- Centralized systems can have multiple processors, and fine-grained parallelism is a characteristic that may be present in some centralized systems to improve performance.