TUTORIAL 1

Deepraj Bhosale
181105016

Introduction to Computer Networks

1. Compare TCP/IP model with OSI model.

OSI(Open System Interconnection)	**TCP/IP(Transmission Control Protocol / Internet Protocol)**
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented	5. Transport Layer is both Connection Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol
10. Protocols are hidden in OSI model and are easily replaced as the technology changes.	10. In TCP/IP replacing protocol is not easy.
11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.

2. What is the requirement of Protocols? Why do we need standardization? Explain in detail

Standardization Process.

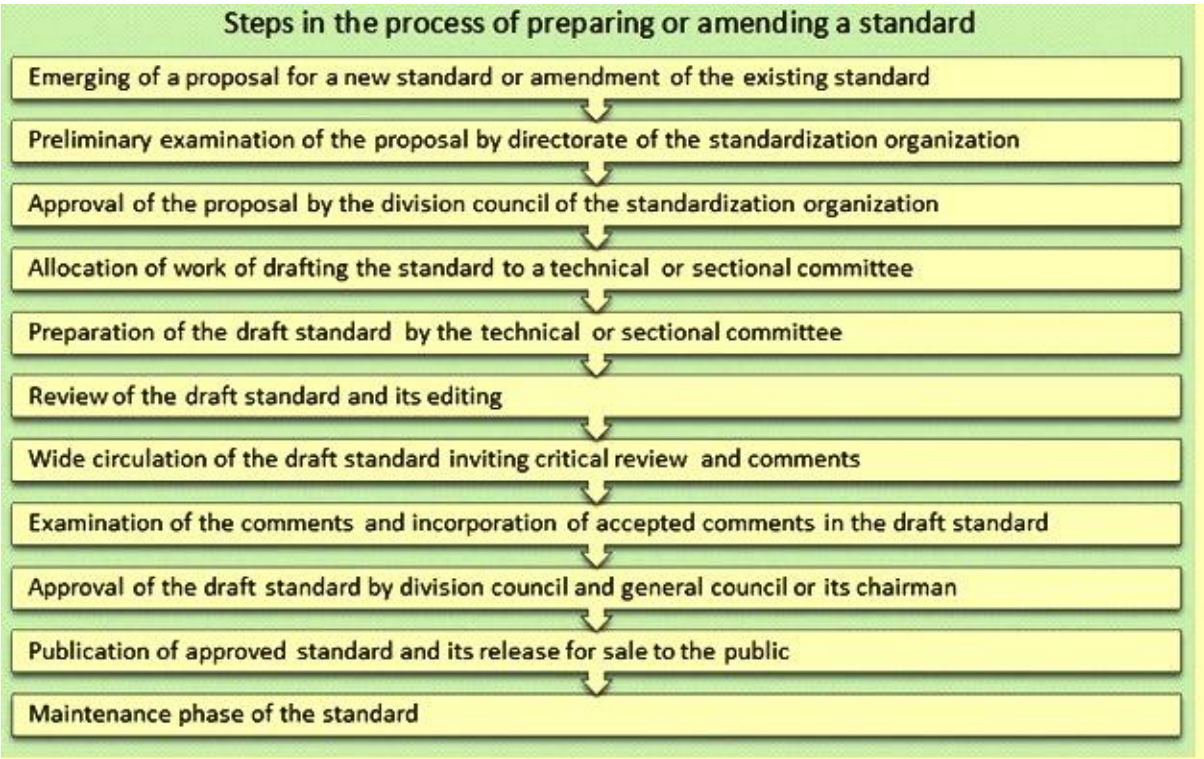
Network protocols are sets of rules for exchanging information. This exchange usually occurs much like a dialog between two computers. The exchange often begins with the client sending a signal to the server, providing key information about what kind of data is being requested.

Standardization: The primary reason for standards is to ensure that hardware and software produced by different vendors can work together. Without networking standards, it would be difficult—if not impossible—to develop networks that easily share information. Standards also mean that customers are not locked into one vendor. They can buy hardware and software from any vendor whose equipment meets the standard. In this way, standards help to promote more competition and hold down prices.

The use of standards makes it much easier to develop software and hardware that link different networks because software and hardware can be developed one layer at a time.

There are two types of standards: formal and de facto.

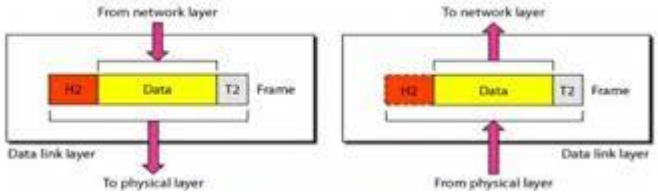
- De facto standards are those that emerge in the marketplace and are supported by several vendors but have no official standing. For example, Microsoft Windows is a product of one company and has not been formally recognized by any standards organization, yet it is a de facto standard. In the communications industry, de facto standards often become formal standards once they have been widely accepted.
- The formal standardization process has three stages: specification, identification of choices, and acceptance. The specification stage consists of developing a nomenclature and identifying the problems to be addressed. In the identification of choices stage, those working on the standard identify the various solutions and choose the optimum solution from among the alternatives. Acceptance, which is the most difficult stage, consists of defining the solution and getting recognized industry leaders to agree on a single, uniform solution. As with many other organizational processes that have the potential to influence the sales of hardware and software, standards-making processes are not immune to corporate politics and the influence of national governments.



3. Explain the functionality of Data Link, Network, Transport, Presentation and Applications Layers with clear diagrams.

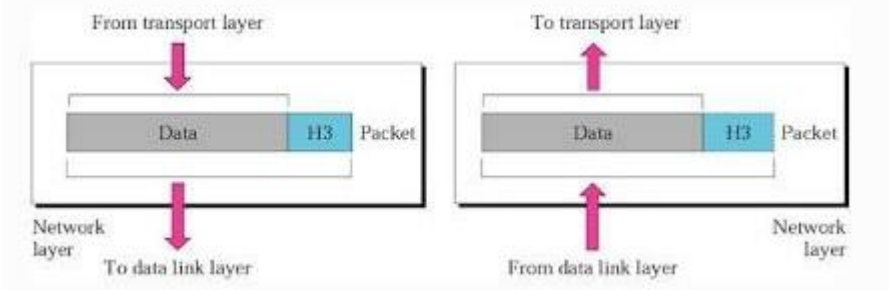
Data Link Layer:

- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.
- **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.



Network Layer:

- **Internetworking**: An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **Addressing**: A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- **Routing**: Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- **Packetizing**: A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

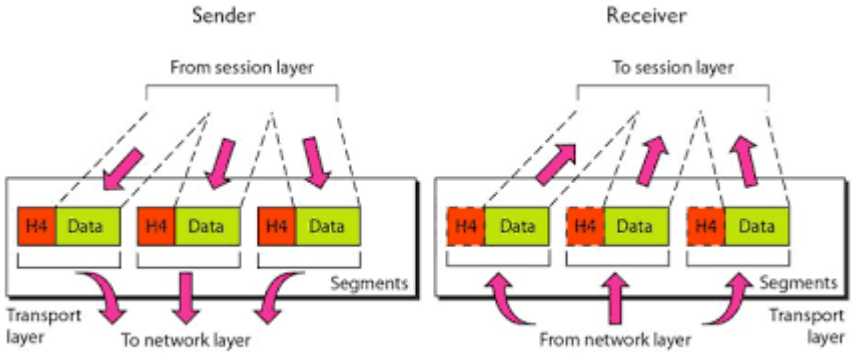


Transport Layer:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a

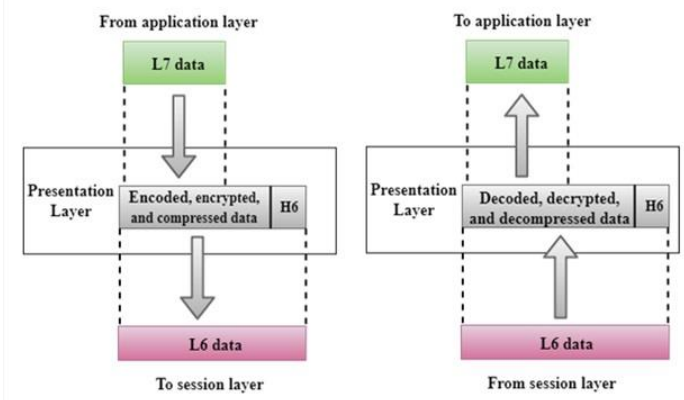
sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.

- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.



Presentation Layer:

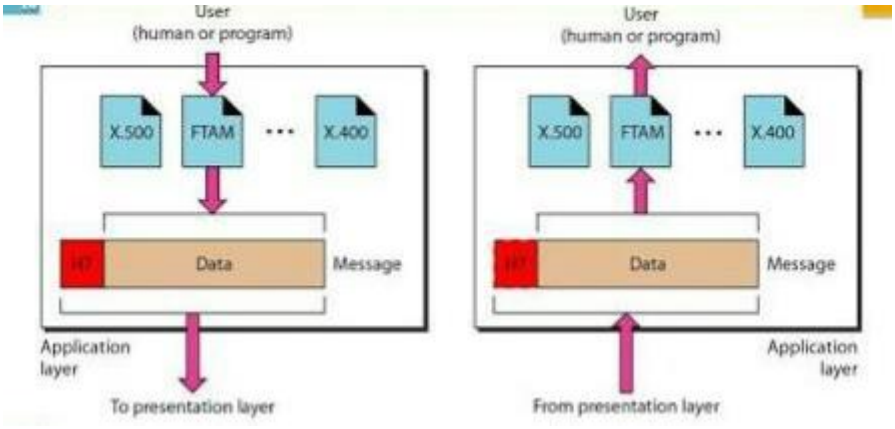
- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
- **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.



Application Layer:

- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.

- **Directory services:** An application provides the distributed database sources and is used to provide that global information about various objects.



4. Explain addressing with respect to TCP/IP. Explain each in detail.

TCP/IP includes an Internet addressing scheme that allows users and applications to identify a specific network or host to communicate with. An Internet address works like a postal address, allowing data to be routed to the chosen destination. TCP/IP provides standards for assigning addresses to networks, sub networks, hosts, and sockets, and for using special addresses for broadcasts and local loop back.

Four levels of addresses are used in an internet employing the TCP/IP protocols:

- Physical Addresses
- Logical Addresses
- Port Addresses
- Specific Addresses

Physical Address: A physical address is a binary number in the form of logical high and low states on an address bus that corresponds to a particular cell of primary storage(also called main memory), or to a particular register in a memory-mapped I/O(input/output) device

Logical Addresses: A logical address is the address at which an item (memory cell, storage element, network host) appears to reside from the perspective of an executing application program. A logical address may be different from the physical address due to the operation of an address translator or mapping function. In a computer with virtual memory that incorporates memory management, the physical address differs from the virtual address so a memory management unit (MMU) translates the virtual address into a physical address, enabling each running process to "think" that it has all the primary storage to itself.

Port Addresses: A port address is a way to identify a specific process to which an Internet or other network message is to be forwarded when it arrives at a server. For the Transmission Control Protocol and the User Datagram Protocol, a port number is a 16-bit integer that is put in the header appended to a message unit.

Specific Addresses: In the TCP/UDP/SCTP services it is also possible to set the parameter for a specific IP or Fully Qualified Domain Name address. The IP/FQDN field refers to the destination address of the traffic, not the source. This means for example, that you can set up a custom service that will describe in a policy the TCP traffic over port 80 going to the web site example.com, but you cannot set up a service that describes the TCP traffic over port 80 that is coming from the computer with the address 192.168.29.59

5. Explain ISO-OSI Reference Model with neat diagram.

The OSI Model (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a networking system. The OSI model characterizes computing functions into a universal set of rules and requirements in order to support interoperability between different products and software. In the OSI reference model, the communications between a computing system are split into seven different abstraction layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

Physical Layer

The lowest layer of the OSI Model is concerned with electrically or optically transmitting raw unstructured data bits across the network from the physical layer of the sending device to the physical layer of the receiving device. It can include specifications such as voltages, pin layout, cabling, and radio frequencies. At the physical layer, one might find “physical” resources such as network hubs, cabling, repeaters, network adapters or modems.

Data Link Layer

At the data link layer, directly connected nodes are used to perform node-to-node data transfer where data is packaged into frames. The data link layer also corrects errors that may have occurred at the physical layer.

The data link layer encompasses two sub-layers of its own. The first, media access control (MAC), provides flow control and multiplexing for device transmissions over a network. The second, the logical link control (LLC), provides flow and error control over the physical medium as well as identifies line protocols.

Network Layer

The network layer is responsible for receiving frames from the data link layer, and delivering them to their intended destinations among based on the addresses contained inside the frame. The network layer finds the destination by using logical addresses, such as IP (internet protocol). At this layer, routers are a crucial component used to quite literally route information where it needs to go between networks.

Transport Layer

The transport layer manages the delivery and error checking of data packets. It regulates the size, sequencing, and ultimately the transfer of data between systems and hosts. One of the most common examples of the transport layer is TCP or the Transmission Control Protocol.

Session Layer

The session layer controls the conversations between different computers. A session or connection between machines is set up, managed, and termined at layer 5. Session layer services also include authentication and reconnections.

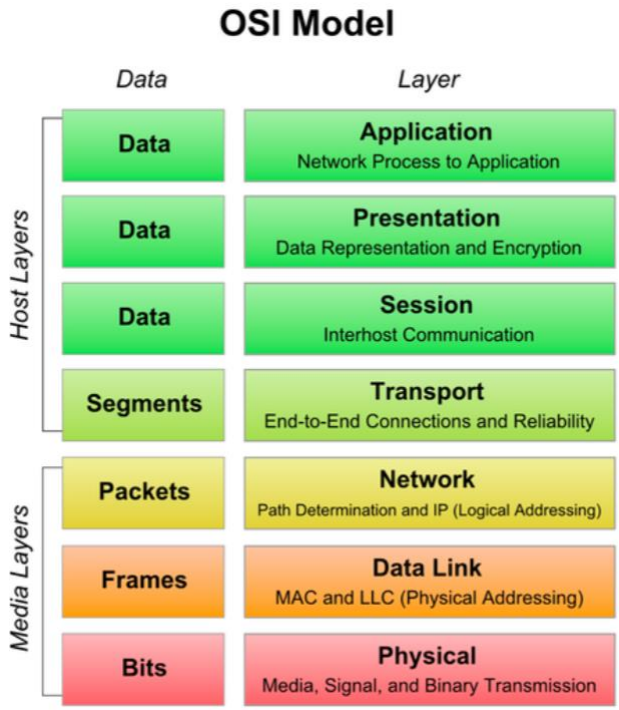
Presentation Layer

The presentation layer formats or translates data for the application layer based on the syntax or semantics that the application accepts. Because of this, it at times also called the syntax layer. This layer can also handle the encryption and decryption required by the application layer.

Application Layer

At this layer, both the end user and the application layer interact directly with the software application. This layer sees network services provided to end-user applications such as a web

browser or Office 365. The application layer identifies communication partners, resource availability, and synchronizes communication.



6. Explain TCP/IP Model with neat diagram.

TCP/IP Reference Model is a four-layered suite of communication protocols. It was developed by the DoD (Department of Defence) in the 1960s. It is named after the two main protocols that are used in the model, namely, TCP and IP. TCP stands for Transmission Control Protocol and IP stands for Internet Protocol.

The four layers in the TCP/IP protocol suite are −

- **Host-to- Network Layer** −It is the lowest layer that is concerned with the physical transmission of data. TCP/IP does not specifically define any protocol here but supports all the standard protocols.
- **Internet Layer** −It defines the protocols for logical transmission of data over the network. The main protocol in this layer is Internet Protocol (IP) and it is supported by the protocols ICMP, IGMP, RARP, and ARP.
- **Transport Layer** − It is responsible for error-free end-to-end delivery of data. The protocols defined here are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- **Application Layer** − This is the topmost layer and defines the interface of host programs with the transport layer services. This layer includes all high-level protocols like Telnet, DNS, HTTP, FTP, SMTP, etc.

7. Provide the classification of Network Topologies. Provide detailed figures, advantages and disadvantages for the same with clear description.

A network topology is the arrangement of a network, including its nodes and connecting lines. There are two ways of defining network geometry: the physical topology and the logical (or signal) topology. The physical topology of a network is the actual geometric layout of workstations. There are several common physical topologies, as given below:

Mesh:

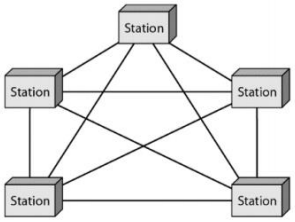
In the mesh topology, each workstation is connected directly to each of the others. In the partial mesh topology, some workstations are connected to all the others, and some are connected only to those other nodes with which they exchange the most

Types of Mesh Topology

1. Partial Mesh Topology: In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. Full Mesh Topology: Each and every nodes or devices are connected to each other.

Features of Mesh Topology

1. Fully connected.
2. Robust.
3. Not flexible.



Advantages of Mesh Topology

1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

Disadvantages of Mesh Topology

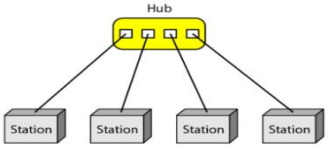
1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

Star:

In the star network topology, there is a central computer or server to which all the workstations are directly connected. Every workstation is indirectly connected to every other through the central computer.

Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.



Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity.

Bus:

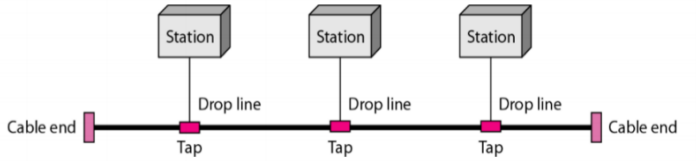
In the bus network topology, every workstation is connected to a main cable called the bus. Therefore, in effect, each workstation is directly connected to every other workstation in the network.

Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

Advantages of Bus Topology

1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.



Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

Ring:

In the ring network topology, the workstations are connected in a closed loop configuration. Adjacent pairs of workstations are directly connected. Other pairs of workstations are indirectly connected, the data passing through one or more intermediate nodes.

Features of Ring Topology

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called *Dual Ring Topology*.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

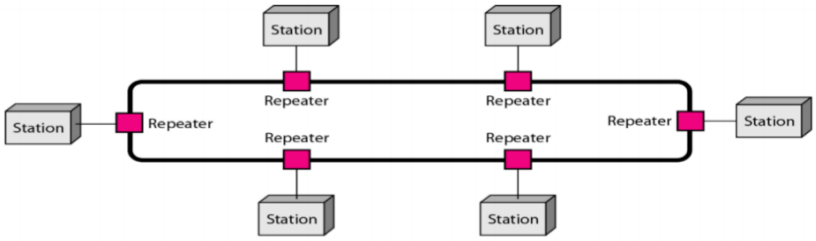
Advantages of Ring Topology

1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.

2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

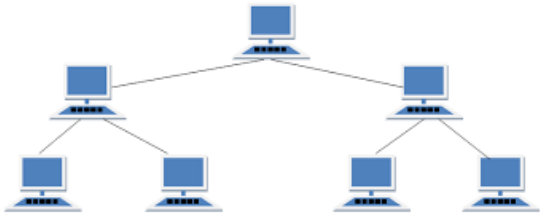


Tree:

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.

Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.



Advantages of Tree Topology

1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

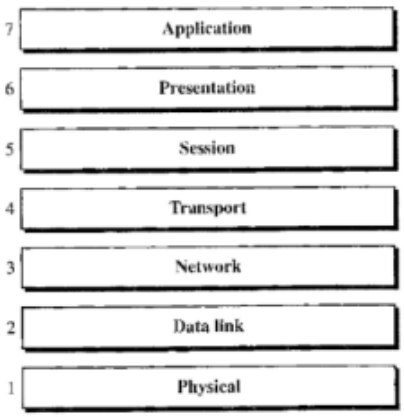
Disadvantages of Tree Topology

1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

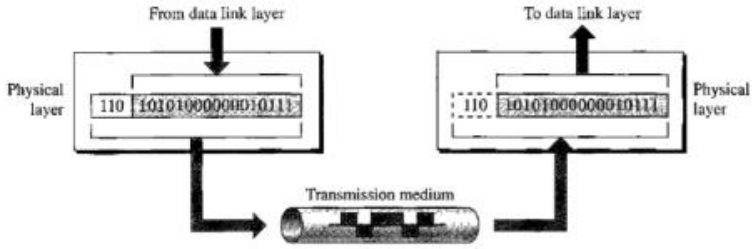
8. Write a brief note on OSI Model with clear listing of functionality of each layer of OSI Model. Also draw the figure providing summary of layers.

The OSI (Open Systems Interconnection) model defines a seven-layer network. The purpose of 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 a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of the seven separate but related layers, each of which defines a part of the process of moving information across a network. An understanding of the fundamentals f the OSI model provides a solid basis for exploring data communication.

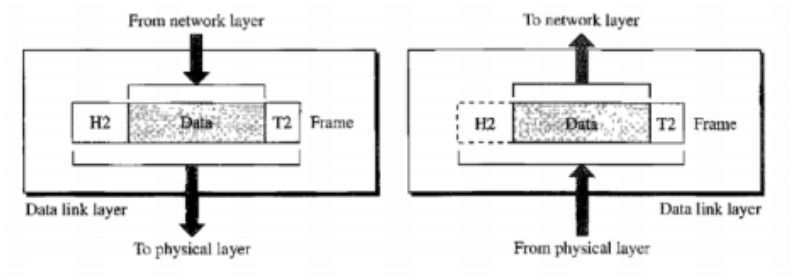
Layers in the OSI model:



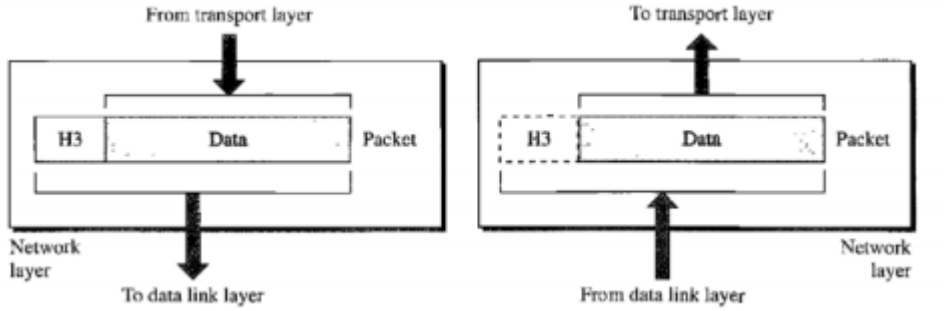
(1) **Physical layer:** The physical layer is responsible for movements of individual bits from one hop (node) to the next.



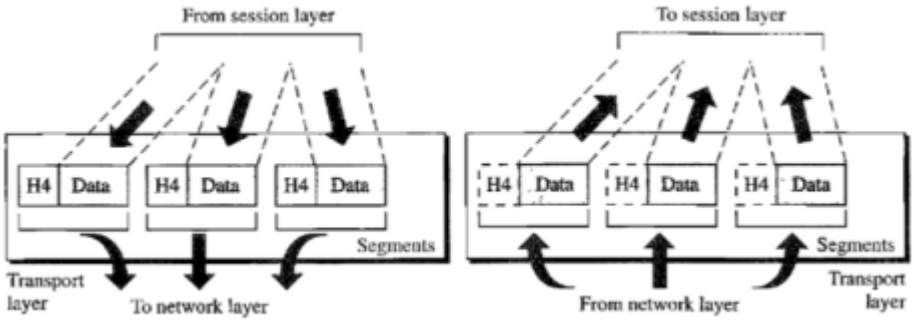
(2) **Data link layer**: The data link layer is responsible for moving frames from one hop (node) to the next.



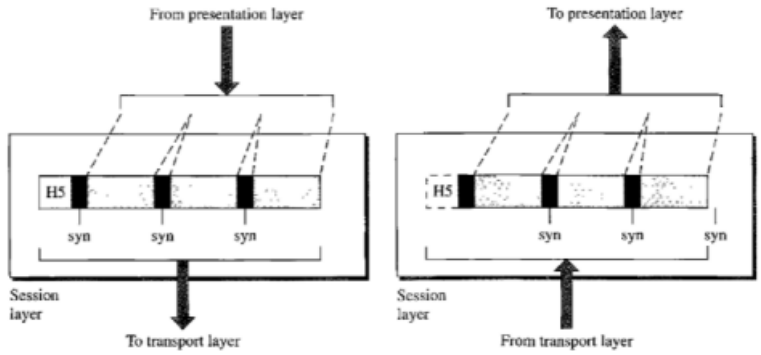
(3) **Network layer**: The network layer is responsible for the delivery of individual packets from the source host to the destination host.



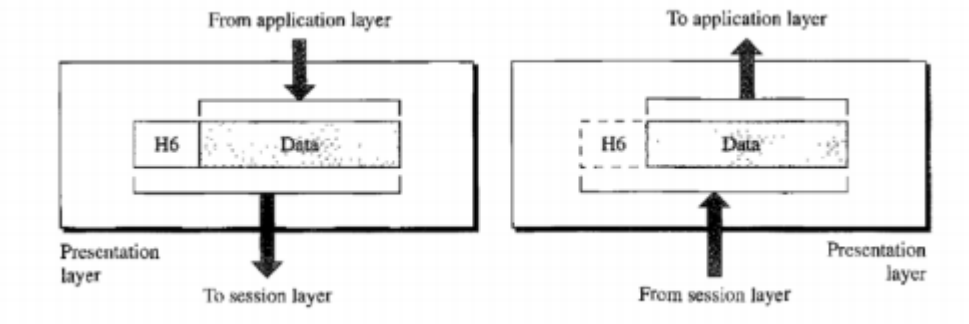
(4) **Transport layer**: The transport layer is responsible for the delivery of a message from one process to another



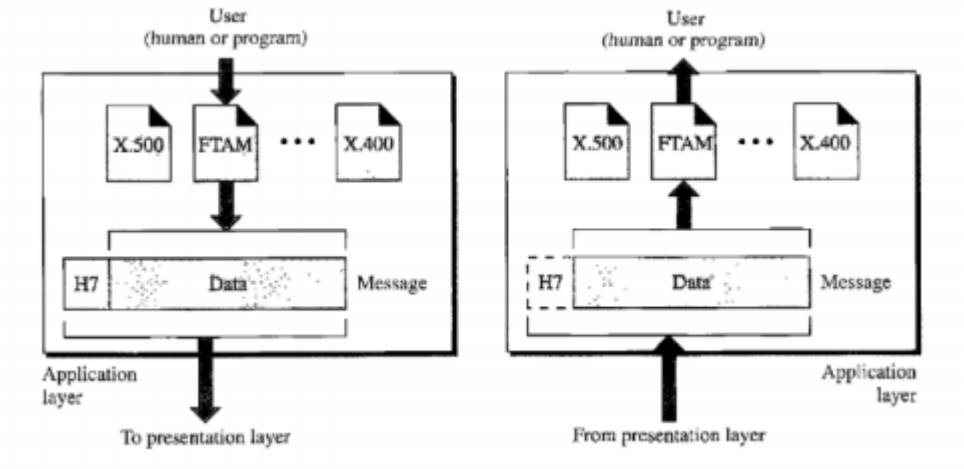
(5) **Session layer**: The session layer is responsible for dialog control and synchronization.



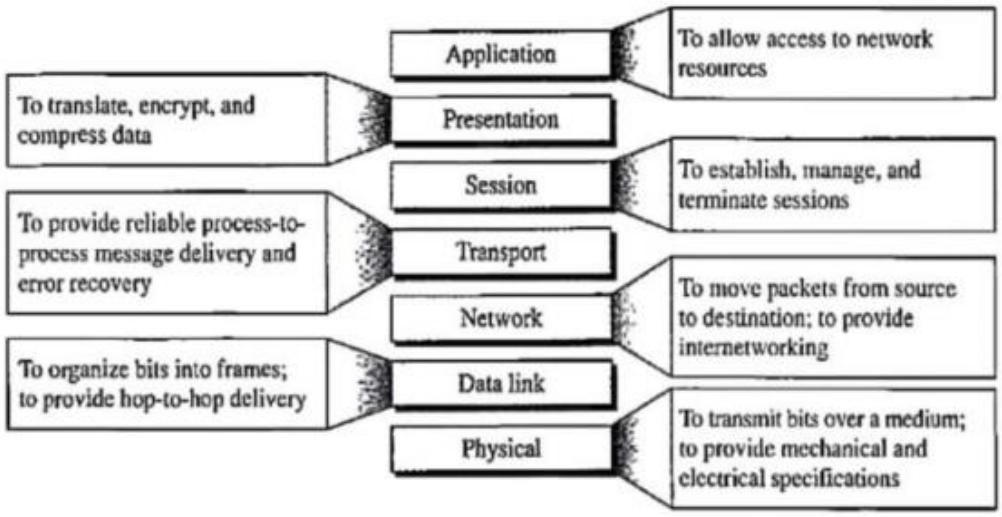
(6) **Presentation layer**: The presentation layer is responsible for translation, compression, and encryption.



(7) **Application layer**: The application layer is responsible for providing services to the user.



Summary of Layers:



9. What is standardization. In detail explain the process of Standardization.

Standardization is the process of implementing and developing technical standards based on the consensus of different parties that include firms, users, interest groups, standards organizations and government. Standardization can help to maximize compatibility, interoperability, safety, repeatability, or quality. It can also facilitate commoditization of formerly custom processes.

The process of standardization can itself be standardized. There are four levels of standardization: compatibility, interchangeability, commonality and reference. These standardization processes create compatibility, similarity, measurement and symbol standards.

There are typically four different techniques for standardization:

- Simplification or variety control
- Codification
- Value engineering
- Statistical process control

Types of standardization process:

- Emergence as de facto standard: tradition, market domination, etc.
- Written by a Standards organization:
  - in a closed consensus process: Restricted membership and often having formal procedures for due-process among voting members
  - in a full consensus process: usually open to all interested and qualified parties and with formal procedures for due-process considerations
- Written by a government or regulatory body
- Written by a corporation, union, trade association, etc.

There are many different standards used in networking today. Each standard usually covers one layer in a network. For a network to operate, many different standards must be used simultaneously. The sender of a message must use one standard at the application layer, another one at the transport layer, another one at the network layer, another one at the data link layer, and another one at the physical layer. Each layer and each standard is different, but all must work together to send and receive messages.

Layer	Common Standards
1. Physical layer	RS-232C cable (LAN) Category 5 cable (LAN) V.92 (56 Kbps modem)
2. Data link layer	Ethernet (LAN) Frame relay (WAN) T1 (MAN and WAN)
3. Network layer	IP (Internet and LANs) IPX (Novell LANs)
4. Transport layer	TCP (Internet and LANs) SPX (Novell LANs)
5. Application layer	HTTP, HTML (Web) MPEG, H.323 (audio/video) SMTP, IMAP, POP (e-mail)

Some of the common standard organizations of India are:

- Press Council of India (PCI)
- News Broadcasting Standards Authority (NBSA)
- Central Board of Film Certification (CBFC)
- Telecom Regulatory Authority of India (TRAI)
- Indian Broadcasters Federation (IBF)
- News Broadcasters Association (NBA)
- Indian Media Group (IMG)

10. Explain briefly how the layers of the Internet model correlate to the layers of the OSI model with the help of appropriate diagrams.

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:

A. host-to-network
B. internet
C. transport
D. application

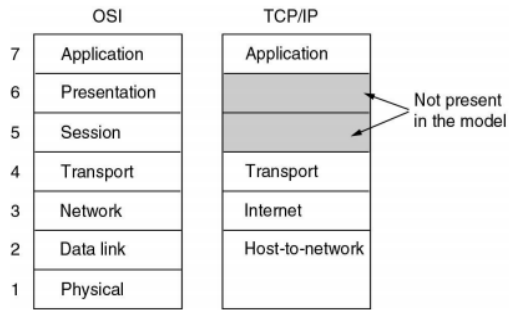
When TCP/IP model is compared to OSI, the host-to-network layer is equivalent to the combination of the physical and data link layers. The internet layer is equivalent to network layer, and the application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCP/IP taking care of part of the duties of the session layer.

So, TCP/IP protocol suite is made of five layers:

- physical
- data link
- network
- transport
- application

The first four layers provide physical standards, network interfaces, internetworking, and transport functions that corresponding to the first four layers of the OSI model. The three topmost layers in the OSI model are represented in TCP/IP by a single layer called the application layer.

TCP/IP reference model:



1. Physical and Data link layers At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all the standards and proprietary protocols. A network in a TCP/IP inter-network can be a local-area network or a wide area network.
2. Network layer At the network layer (or, more accurately, the inter-network layer), TCP/IP supports the inter-networking Protocol. IP uses four supporting protocols:
    i. ARP: - Address Resolution Protocol is used to associate a logical address with a physical address. It is used to find the physical address of the node when its internet address is known.

ii. RARP: - Reverse Address Resolution Protocol 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.

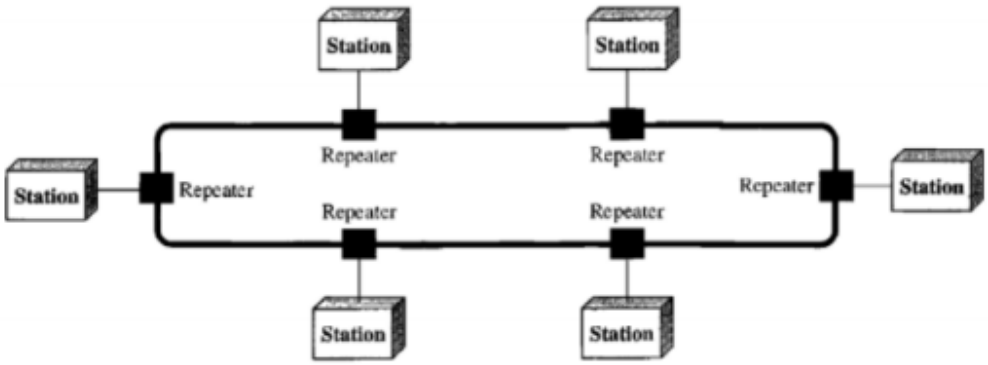
iii. ICMP: - The Internet Control Message Protocol is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender. It sends query and error reporting messages.

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

3. Transport Layer This layer was represented in TCP/IP by two protocols TCP [Transmission Control Protocol] and UDP [User Datagram Protocol]. These are transport level protocols responsible for delivery of a message from a process to another process. A new transport layer protocol, SCTP [Stream Control Transmission Protocol], has been devised to meet the needs of some newer applications.
4. Application Layer The application layer in TCP/IP is equivalent to the combined session, presentation and application layers in the OSI model. Many protocols are defined in this level.

11. Define RING and TREE Topology.

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.



Tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable.For example, tree topologies are frequently used to organize the computers in a corporate network, or the information in a database.

12. List the basic hardware components of computer networks.

Computer networks share common devices, functions, and features including servers, clients, transmission media, shared data, shared printers and other hardware and software resources, network interface card (NIC), local operating system (LOS), and the network operating system (NOS). The basic hardware components of computer networks are:

- Servers
- Clients
- Transmission Media
- Shared data
- Shared printers and other peripherals
- Network Interface Card
- Local Operating System
- Network Operating System
- Hub
- Switch
- Router
- LAN
- Cable

13. Write down Categories of Network.

The Network allows computers to connect and communicate with different computers via any medium. LAN, MAN and WAN are the three major types of the network designed to operate over the area they cover. There are some similarities and dissimilarities between them. One of the major differences is the geographical area they cover, i.e., LAN covers the smallest area; MAN covers an area larger than LAN and WAN comprises the largest of all.

There are other types of Computer Networks also, like:

- PAN (Personal Area Network)
- SAN (Storage Area Network)
- EPN (Enterprise Private Network)
- VPN (Virtual Private Network)

14. Define Data Communication.

Data communication is the exchange of data between two devices via some form of transmission medium like a wire or cable or other. 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).

15. Define Network Criteria.

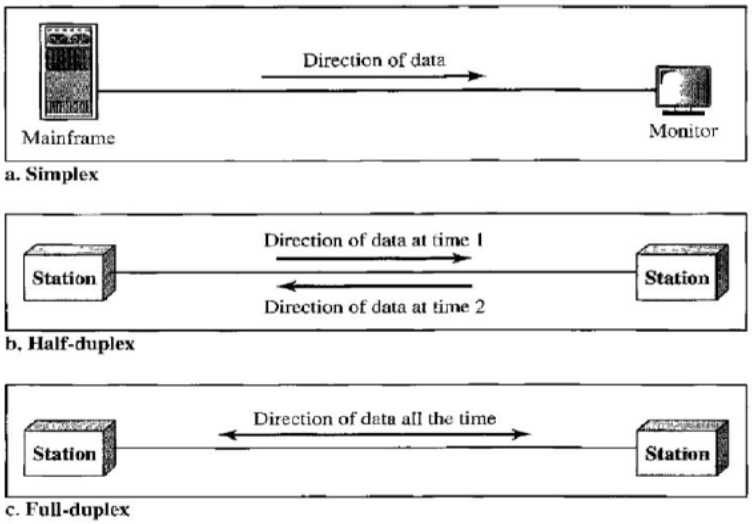
A network must be able to meet a certain number of criteria to serve a particular situation. The most important of these are performance, reliability, and security. Performance depends on various factors; e.g. the number of simultaneous users, the number of connected computers — and their traffic profiles. Given these factors, we can design a network to meet the performance criteria. If network traffic increases beyond the designed capacity, performance will deteriorate.

16. Give an example for the simplex, half duplex and full duplex transmission modes.

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.
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.

Half Duplex: 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.
Walkie-talkies and CB radios are both half-duplex systems.

Full-Duplex: In full-duplex mode, both stations can transmit and receive simultaneously
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 the same time.



17. Discuss about Network Models.

A network model is a database model that is designed as a flexible approach to representing objects and their relationships. A unique feature of the network model is its schema, which is viewed as a graph where relationship types are arcs and object types are nodes. Unlike other database models, the network model's schema is not confined to be a lattice or hierarchy; the hierarchical tree is replaced by a graph, which allows for more basic connections with the nodes.

18. Categorize the network based on the scale.

A local area network (LAN) is usually privately owned and connects some hosts in a single office, building, or campus.

A wide area network (WAN) is also an interconnection of devices capable of communication.

A Metropolitan Area Network (MAN) It is basically a bigger version of LAN. It is also called MAN and uses the similar technology as LAN.

A personal area network (PAN) refers to the interconnection of information technology devices or gadgets within the environment of an individual user (typically within 10 meters or 33 feed).

19. What are network criteria of evaluation?

A network must be able to meet certain criteria, these are mentioned below:

(1) **Performance** It is measured in terms of transit time and response time.

- Transit time is the time for a message to travel from one device to another
- Response time is the elapsed time between an inquiry and a response.

Performance is dependent on the following factors:

- The number of users
- Type of transmission medium
- Capability of connected network
- Efficiency of software

(2) **Reliability** It is measured in terms of

- Frequency of failure
- Recovery from failures
- Robustness during catastrophe

(3) **Security** It means protecting data from unauthorized access.

20. Define jitter.

Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. Jitter is an undesirable effect caused by the inherent tendencies of TCP/IP networks and components. Playback may experience gaps while waiting for the arrival of variable delayed packets. For example, let us assume that video packets are sent every 30 m/s. If some of the packets arrive with 30-ms delay and others with 40-ms delay, an uneven quality in the video is the result.

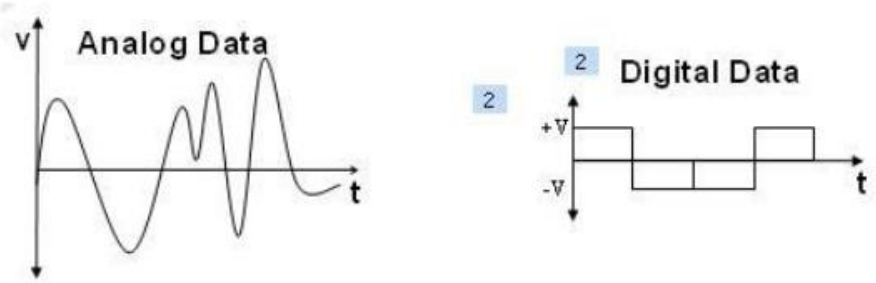
21. Define Internetworking.

Connecting several networks together using internetworking devices such as routers and gateways. Internetwork (internet) is a network of networks.
Internetworking is the practice of connecting a computer network with other networks through the use of gateways that provide a common method of routing information packets between the networks. Internetworking is a combination of the words inter ("between") and networking; not internet-working or international-network.

The smallest amount of effort to create an internet (an internetwork, not the Internet), is to have two LANs of computers connected to each other via a router. Simply using either a switch or a hub to connect two local area networks together doesn't imply internetworking; it just expands the original LAN.

22. Categorize data representation.

There are three types of data representation is of two types namely, analog and digital.



Analog data is continuous and can take infinite set of values. In the diagram, the data takes a wide set of voltage values at different points of time. Examples of analog data are audio from a speaker, video output from a camera etc.

Digital data is discrete and not continuous. It cannot take an infinite set of values and it only takes finite set of values. In the diagram above the data takes only two voltage values (+v and –v) at different points of time. Examples of digital data include Text files (finite set of characters), binary representation (in 0s & 1s), bitmap file, digitally converted audio, video data, digital images etc.

23. What are NSPs?

Stands for "Network Service Provider" is a business or organization that sells bandwidth or network access by providing direct Internet backbone access to providers and usually access to its network access points (NAPs). For such a reason, network service providers are sometimes referred to as backbone providers or *internet providers*.

Network service providers may consist of telecommunications companies, data carriers, wireless communications providers, Internet service providers, and cable television operators offering high-speed Internet access.

24. Compare internet and intranet.

Internet

The **Internet** is a global network that establishes a connection and provides transmission between various computers. It uses both wired and wireless mode of communication to send and receive any information such as data, audio, video, etc. Here, data travels through "fibre optic cables", which are owned by telephone companies. Nowadays everyone uses the Internet for acquiring information, communication, and transferring data over the network. It is a public network using which computers can connect and relay to each other. It provides an excellent source of information to the user. The origins of the Internet date back to research commissioned by the federal government of the United States in the 1960s to build robust, fault-tolerant communication with computer networks. The primary precursor network, the ARPANET, initially served as a backbone for interconnection of regional academic and military networks in the 1980s. The funding of the National Science Foundation Network as a new backbone in the 1980s, as well as private funding for other commercial extensions, led to worldwide participation in the development of new networking technologies, and the merger of many networks.

Intranet:

An **intranet** is a private network accessible only to an organization's staff. Often, a wide range of information and services are available on an organization's internal intranet that are unavailable to the public, unlike the Internet. A company-wide intranet can constitute an

important focal point of internal communication and collaboration, and provide a single starting point to access internal and external resources. In its simplest form, an intranet is established with the technologies for local area networks (LANs) and wide area networks (WANs). Many modern intranets have search engines, user profiles, blogs, mobile apps with notifications, and events planning within their infrastructure.

Internet	Intranet
Connects different network of computers together.	It is a part of Internet which is privately owned by a particular firm.
Anyone can access the Internet.	Accessible only by the organization members, having login details.
Is not as safe as compared to Intranet.	Safer compared to Internet.
Unlimited number of users.	Limited number of users.
Have large number of visitors' traffic.	Very less number of visitors' traffic.
Network type is public.	Network type is private.
Unlimited information is provided and can be viewed by everyone.	Limited, and circulates among the members of an organization.

25. Illustrate about Inter Network protocols and standards.

TCP/IP

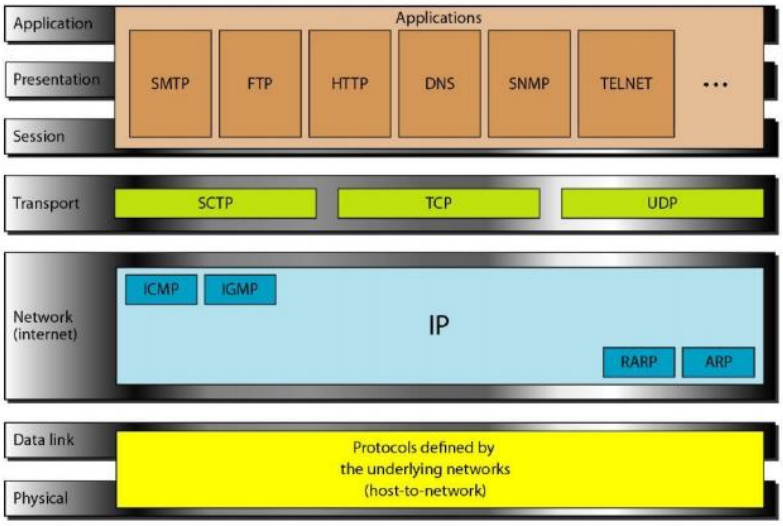
TCP/IP is the most commonly used network protocol worldwide and all nodes connected to the Internet use it. TCP/IP consists of the 3 main protocols TCP (Transmission Control Protocol), UDP (User Data Protocol) and IP (Internet Protocol). UDP is a less important protocol using the lower-level Protocol IP as well. For more details, have a look at ``Computer Networks'' by Andrew Tanenbaum.

TCP and UDP

TCP and UDP are transmission protocols that use IP to transmit their data. While IP is responsible for transmitting packets to the destination at best effort, TCP and UDP are used to prepare data for sending by splitting them in packets.

TCP (Transmission Control Protocol) provides a connection for bi-directional communication between two partners using two data streams. It is therefore called a connection-oriented protocol. Before sending or receiving any data, TCP has to establish a connection channel with the target node. To provide the channel for the two data streams it has to split the data into packets and ensure that packets arrive without error and are unpacked in the proper order. That way an application using TCP does not have to take precautions for corrupted data transfer. TCP will make sure data transfer is completed successfully or report an error otherwise.

UDP (User Data Protocol) on the other hand is a much simpler technique for delivering data packets. It just adds a header to the data and sends them to its destination, regardless whether that node exists or expects data. UDP does not guarantee that packets arrive, nor does it ensure they arrive in the order they were sent. If packets are transmitted between two networks using different paths they can arrive in a wrong order. It's the application that has to take care of that. However, for applications needing fast transfer without overhead for data that is still usable even if single packets are missing or not in order, UDP is the protocol in choice. Most voice and video streaming applications therefore use UDP.



ICMP - Internet Control Message Protocol

CMP (Internet Control Message Protocol) is an error-reporting protocol network device like routers use to generate error messages to the source IP address when network problems prevent delivery of IP packets. ICMP creates and sends messages to the source IP address indicating that a gateway to the Internet that a router, service or host cannot be reached for packet delivery. Any IP network device has the capability to send, receive or process ICMP messages.

IGMP - Internet Group Management Protocol

The Internet Group Management Protocol (IGMP) is an Internet protocol that provides a way for an Internet computer to report its multicast group membership to adjacent routers. Multicasting allows one computer on the Internet to send content to multiple other computers that have identified themselves as interested in receiving the originating computer's content. Multicasting can be used for such applications as updating the address books of mobile computer users in the field, sending out company newsletters to a distribution list, and "broadcasting" high-bandwidth programs of streaming media to an audience that has "tuned in" by setting up a multicast group membership.

RARP - Reverse Address Resolution Protocol

RARP (Reverse Address Resolution Protocol) is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address Resolution Protocol (ARP) table or cache. A network administrator creates a table in a local area networks gateway router that maps the physical machine (or Media Access Control - MAC address) addresses to corresponding Internet Protocol addresses. When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address. If an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.

ARP - Address Resolution Protocol Address Resolution Protocol

(ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. For example, in IP Version 4, the most common level of IP in use today, an address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. (The physical machine address is also known as a Media Access Control or MAC address.) A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

26. Define Standards. How does it differ from Protocols?

Standards — a set of rules that formally specify how communication should proceed in a particular domain for a particular purpose. Standards include communication protocols and, when appropriate, physical characteristics of devices and media.

Protocol — an agreed method of transaction, communication, and exchange between hardware and/or software agents. The protocol defines how each agent must behave, including the timing, format and content of messages that it sends and receives, in order to communicate effectively with other agents using the same protocol.

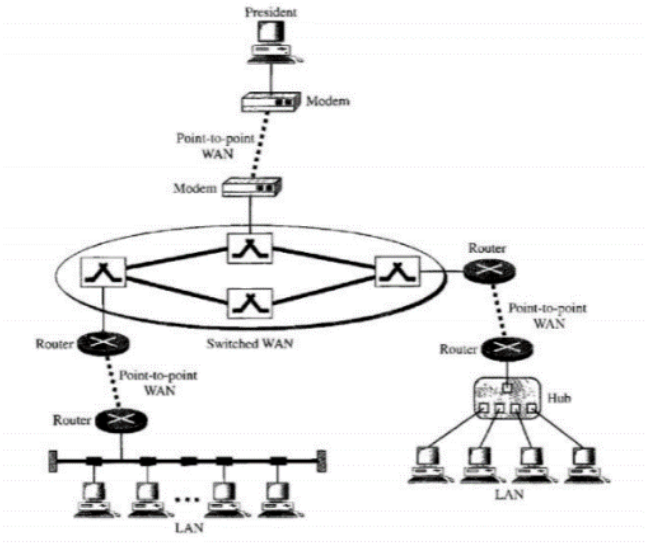
A protocol is a series of prescribed steps to be taken, usually in order to allow for the coordinated action of multiple parties. In the world of computers, protocols are used to allow different computers and/or software applications to work and communicate with one another. Because computer protocols are usually formalized, many people consider protocols to be standards. However, such is not actually the case. Standards are simply agreed-upon models for comparison, such as the meter and the gram. In the world of computers, standards are often used to define syntactic or other rule sets, and occasionally protocols, that are used as a basis for comparison. Some good examples include ANSI SQL, used to compare derivations of the SQL database query language, and ANSI C, used to compare derivations of the C programming language.

27. Explain Interconnection of Networks.

When two or more networks are connected, they become an internetwork, or internet. For example, assume that an organization has to offices, one on the east coast and the other on the west coast. The establishment office on the west has a bus topology LAN; the newly opened office on the east coast has a star topology LAN. The president of the company lives somewhere in the middle and needs to have a control over the company from her home.

To create a backbone WAN for connecting these three entities a switched WAN has been leased. To connect the LANs to this switched WAN, however, three point-to-point WANs are required. These point-to-point WANs can be high-speed DSL line offered by a telephone company or a cable modem line offered by a cable TV provider is as shown below:

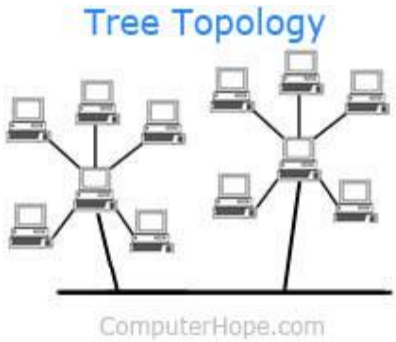
A heterogeneous network made of four WANs and two LANs



28. With suitable diagram explain the difference between BUS and TREE Topology.

A. **Bus Topology** The preceding examples all describe point-to-point connections. A bus topology, on the other hand, is multipoint. One long cable act as a backbone to link all the devices in a network. 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.

B. In computer networks, a **tree topology** is also known as a *star bus topology*. It incorporates elements of both a bus topology and a star topology. Below is an example network diagram of a tree topology, in which the central nodes of two star networks are connected to one another.



In the picture above, if the main cable or trunk between each of the two star topology networks were to fail, those networks would be unable to communicate with each other. However, computers on the same star topology would still be able to communicate.

29. What is standardization? Why it is necessary? List and explain the standardization bodies. Clearly state the process of standardization with its advantages and disadvantages.

Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunication technology and processes. Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of inter-connectivity necessary in today's marketplace and in international communications.

Data communication standards fall into two categories: de facto and de jure.

1. **De facto** (meaning "by fact" or "by convention"): Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto

standards. De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.
2. **De jure** (meaning "by law" or "by regulation"): Those standards that have been legislated by an officially recognized body are de jure standards.

Standards Organization:

1. Standards are developed through the cooperation of standards creation, committees, forums, and government regulatory agencies (FCC).
2. Many organizations are dedicated to the establishment of standards, data telecommunications in North America rely primarily on those published by the following:
3. International Organization for standardization (ISO) The ISO is active in developing cooperation in the realms of scientific, technological, and economic activity.
4. International Telecommunication Union -Telecommunication Standards Sector (ITU-T) The standards for telecommunications in general and for phone and data systems in particular. On March 1, 1993, the Union-Telecommunication Standard. The United Nations formed a committee as a part of its International Telecommunication Union (ITU), the Consultative Committee for International Telegraphy and Telephone (CCITT). This committee was devoted to the research and establishments rds Sector (ITU-T) 14. American National Standards Institute (ANSI) It is a completely private, nonprofit corporation not affiliated with the U.S. federal government.
5. Institute of Electrical and Electronics Engineers (IEEE) This institute is the largest professional engineering society in the world. It aims to advance theory, creativity, and product quality in the fields of electrical engineering, electronics, and radio as well.
6. Electronic Industries Association (EIA).
7. EIA is a non-profit organization devoted to the promotion of electronics manufacturing concerns. Its activity include public awareness education and lobbying efforts in addition to standards development.

Advantage of Standardization:

1. Many computers from all the world can connect together, because they are using the international standard.
2. Easier maintenance and installation because you get used on the standard.

Disadvantages of Standardization:

1. Problems Occur in Standards, it will be international problem.
2. All companies and manufactures must follow the standards instead of developing new techniques.

30. Draw clear figure having a heterogeneous network made up of four WANs and two LANs. Explain each portion of the network clearly in accordance with the provided figure. Label each device in the provided network.

Modem: The term *modem* is a composite word that refers to the two functional entities that make up the device: a signal *mo*dulator and a signal *dem*odulator. A *modulator* creates a bandpass analog signal from binary data. A *demodulator* recovers the binary data from the modulated signal.

Router: a device which forwards data packets to the appropriate parts of a computer network.

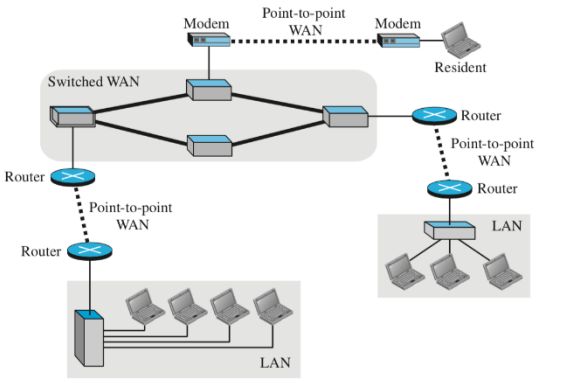
Switch: A switch, in the context of networking is a high-speed device that receives incoming data packets and redirects them to their destination on a local area network (LAN). A LAN switch operates at the data link layer (Layer 2) or the network layer of the OSI Model and, as such it can support all types of packet protocols.

LAN: A *local area network (LAN)* is usually privately owned and connects some hosts in a single office, building, or campus.

WAN: A *wide area network (WAN)* is also an interconnection of devices capable of communication.

However, there are some differences between a LAN and a WAN. A LAN is normally limited in size, spanning an office, a building, or a campus; a WAN has a wider geographical span, spanning a town, a state, a country, or even the world. A LAN interconnects hosts; a WAN interconnects connecting devices such as switches, routers, or modems.

Figure 1.12 *A heterogeneous network made of four WANs and three LANs*



31. Explain different criteria for evaluating the performance of a computer network.

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

The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.

- **Number of users:** Having a large number of concurrent users can slow response time in a network not designed to coordinate heavy traffic loads. The design of a given network is based on an assessment of the average number of users that will be communicating at any one time. In peak load periods, however, the actual number of users can exceed the average and thereby decrease performance. How a network responds to loading is measure of its performance.

- **Types of transmission medium:** The medium defines the speed at which data can travel through a connection. Today's network is moving to faster and faster transmission media, such as fibre-optic cabling, a medium that can carry data at only megabits per second. However, the speed of light imposes an upper bound on the data rate.

- **Hardware:** The types of hardware included in a network affect both the speed and capacity of transmission. A higher-speed computer with greater storage capacity provides better performance.

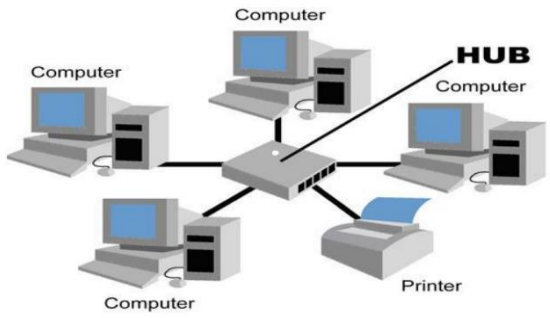
- **Software:** The software used to process data at the sender, receiver, and intermediate nodes affects network performance. Moving a message from node to node through a network requires

processing to transform the raw data into transmittable signals, to route these signals to the proper destination, to ensure error-free delivery, and to recast the signals into a form the receiver can use. The software that provides these services affects both the speed and the reliability of a network link. Well-designed software can speed the process and make transmission more effective and efficient.

32. Explain LAN and MAN with an example.

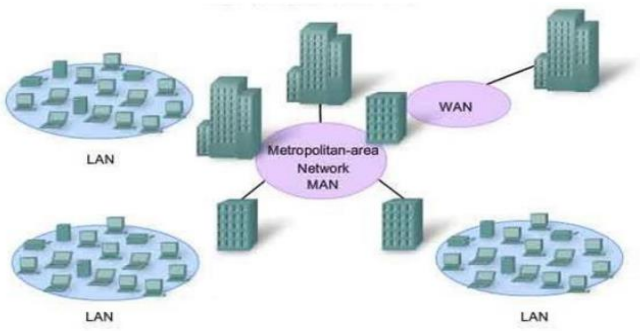
A **LAN** or local area network is a group of computers and associated devices that share a common communications line or wireless link to a server. Typically, a LAN encompasses computers and peripherals connected to a server within a small area such as an office or a commercial establishment.

Computers and other mobile devices use a LAN connection to share resources such as a printer or network storage. A LAN Network can cover an area of up to 1km, and hence is used within buildings and other close proximity networks.



A **MAN** or metropolitan area network is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN).

The term is applied to the interconnection of networks in a city into a single larger network (which may then also offer efficient connection to a wide area network). It is also used to mean the interconnection of several local area networks by bridging them with backbone lines. The latter usage is also sometimes referred to as a campus network. A MAN can cover areas within 10 km/s.



33. Compare MAN and WAN.

MAN (Metropolitan Area Network)	**WAN (Wide Area Network)**
1. MAN is privately owned and networks normally covers the area inside a town or a city.	1. Two types of WAN: switched WAN and point-to-point WAN.
2. MAN is a network with a size between a LAN and a WAN.	2. WAN size may comprise a country, a continent, or even the whole world.
3. It is designed for customers who need a high-speed connectivity.	3. WAN provides long distance transmission of data, image, audio, and video information.
4. Speeds of MAN ranges in terms of Mbps.	4. Speeds of WAN ranges from few kilo bits per second (Kbps) to megabits per second (Mbps).
5. Moderate	5. Low
6. It covers relatively large region such as cities, towns.	6. It spans large locality and connects countries together. Example Internet
7. Limited coverage, about up to 100 miles (or 200 km)	7. Unlimited (usually in 1000Km) range, uses repeater and other connectivity for range extension
8. Locally installed and based on common carrier e.g. twisted pair, fibre optic cable etc.	8. Locally installed and based on common carrier e.g. twisted pair wires, fibre, coaxial cable, wireless including wireless and cellular network based.
9. Example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer. Another example is the cable TV network in a city.	9. Example of a switched WAN is the asynchronous transfer mode (ATM) network. Point-to-point WAN is dial-up line that connects a home computer to the Internet

34. List and explain the role of internet today.

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.

Some of its major uses are:

- Access to remote information – pleasure surfing, picture viewing, financial or political research, etc.
- Person-to-person communication – instant messaging, online gaming, media sharing.
- Interactive entertainment – streaming, interactive films
- Electronic commerce. – amazon, flipkart, property sites, etc.

35. Explain the difference between port address, logical address and physical address.

Through logical address the system identifies a network (source to destination). after identifying the network physical address is used to identify the host on that network. The port address is used to identify the particular application running on the destination machine.

- **Logical Address:** An IP address of the system is called logical address. This address is the combination of Net ID and Host ID. This address is used by network layer to identify a particular network (source to destination) among the networks. This address can be changed by changing the host position on the network. So it is called logical address.
- **Physical address:** Each system having a NIC (Network Interface Card) through which two systems physically connected with each other with cables. The address of the NIC is called Physical address or mac address. This is specified by the manufacturer company of the card. This address is used by data link layer.
- **Port Address:** There are many applications running on the computer. Each application run with a port no.(logically) on the computer. This port no. for application is decided by the Kernel of the OS. This port no. is called port address.

Port Address	Logical Address	Physical Address
Attached at Transport Layer.	Attached at Network Layer.	Attached at Data Link Layer.
Address of Application or Process.	Address of a computer over a network.	Address of a node/ device.
16 bit.	32 bit.	48 bit.
Example: 753	Example: 192.168.225.179	Example: 07:01:02:01:2C:4B