Computer Network BCA 5th Semester

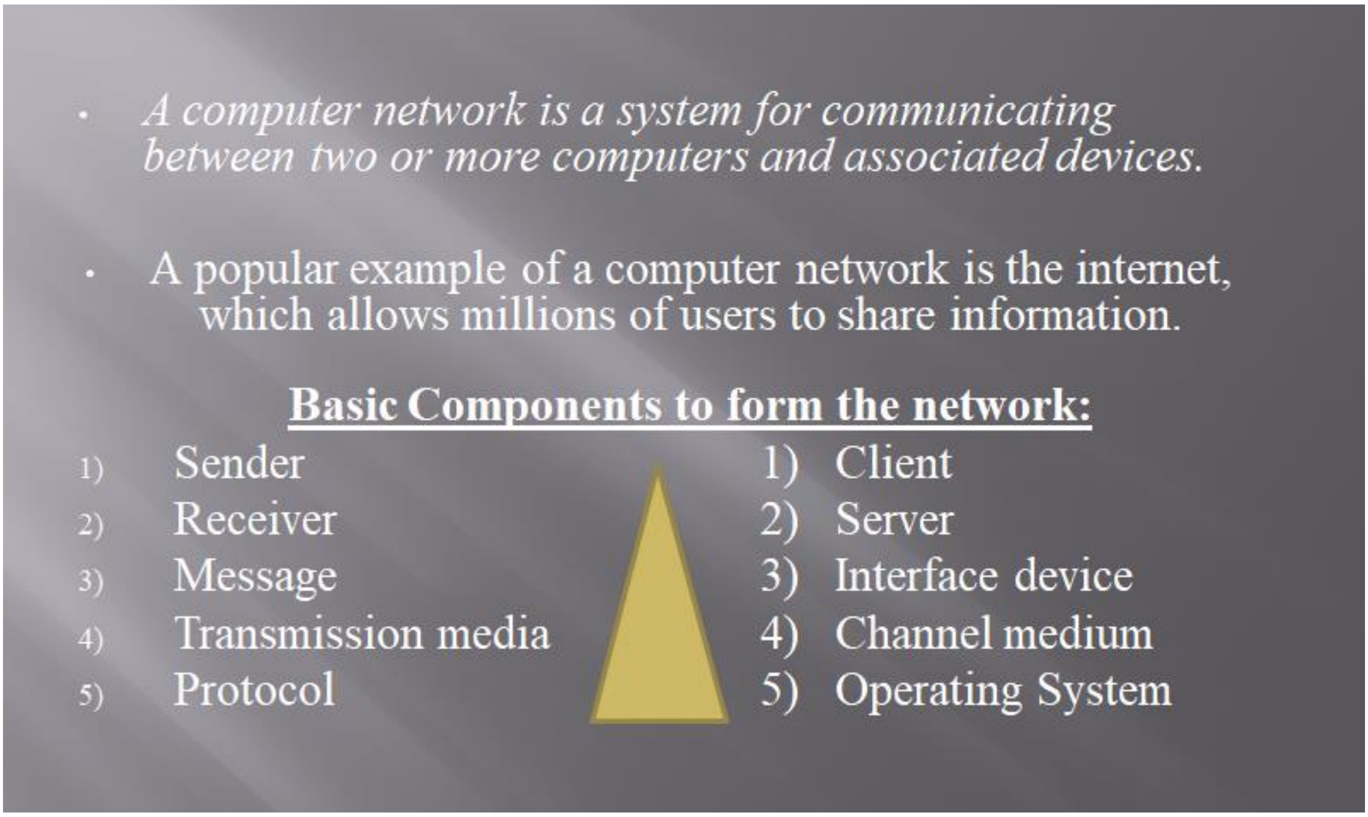
Chapter 1

NETWORK AS AN INFRASTRUCTURE FOR DATA COMMUNICATION:

Network infrastructure is the hardware and software resources of an entire network that enable network connectivity, communication, operations and management of an enterprise network.

It provides the communication path and services between users, processes, applications, services and external networks/the internet.

Network infrastructure is typically part of the IT infrastructure found in most enterprise IT environments. The entire network infrastructure is interconnected, and can be used for internal communications, external communications or both.



- *A computer network is a system for communicating between two or more computers and associated devices.*
- A popular example of a computer network is the internet, which allows millions of users to share information.

Basic Components to form the network:

1) Sender
2) Receiver
3) Message
4) Transmission media
5) Protocol

1) Client
2) Server
3) Interface device
4) Channel medium
5) Operating System

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

- **Receiver**. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on
- **Message**. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
- **Transmission medium**. The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fibre-optic cable, and radio waves.
- **Protocol**. A protocol is a set of rules that governs data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

Types of Network infrastructure

Networking Hardware components:

Routers

Switches

LAN cards

Wireless routers

Cable

Networking Software Components:

Network operations and management

Operating systems

Firewall

Network security applications

Network Transmission Services

Satellite

Wireless protocols

IP addressing

Effectiveness of data communication basically depends upon the certain elements:

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.

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

Timeliness: The system must deliver data in a timely manner.

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

Basic 3 things to be remembered for the direction of data flow

Simplex

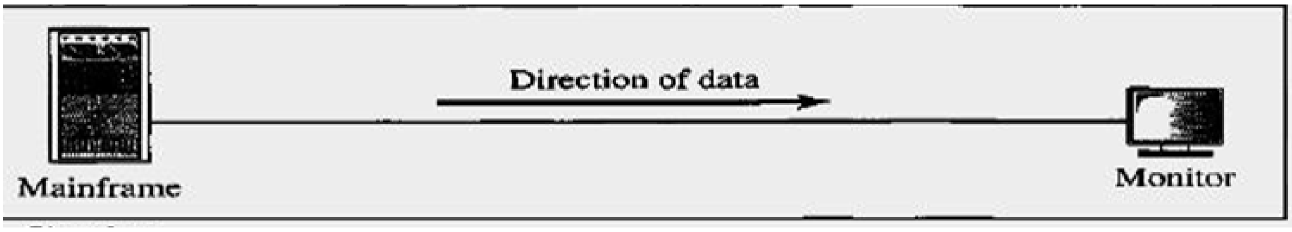
- In simplex mode, the communication is unidirectional, as on a one-way street.
- Only one of the two devices on a link can transmit; the other can only receive.
- Keyboards and traditional monitors are examples of simplex devices.
- The keyboard can only introduce input; the monitor can only accept output.
- The simplex mode can use the entire capacity of the channel to send data in one direction

Half-Duplex

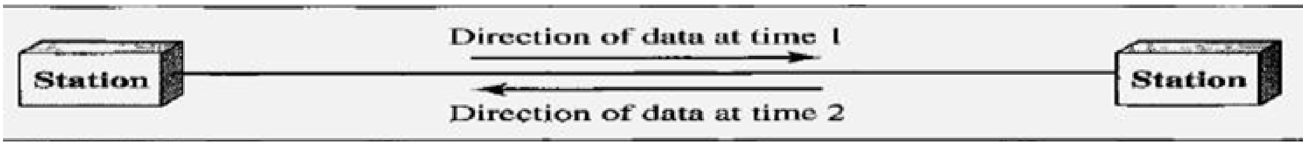
- In half-duplex mode, each station can both transmit and receive, but not at the same time.
- When one device is sending, the other can only receive, and vice versa.
- In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.
- Walkie-talkies and CB (citizens band) radios are both half-duplex systems.
- The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

Full Duplex

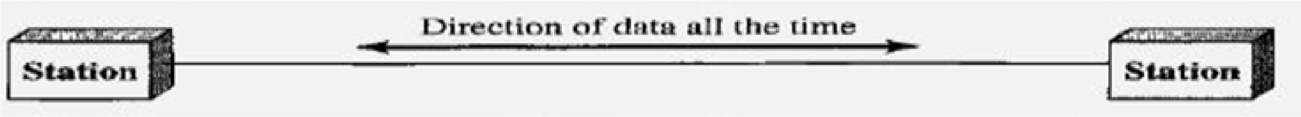
- In full-duplex made (also, called duplex), both stations can transmit and receive simultaneously.
- In full-duplex mode, signals going in one direction share the capacity of the link with signals going in the other direction.
- This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals travelling in both directions.
- One common example of full-duplex communication is the telephone network.



SIMPLEX MODE

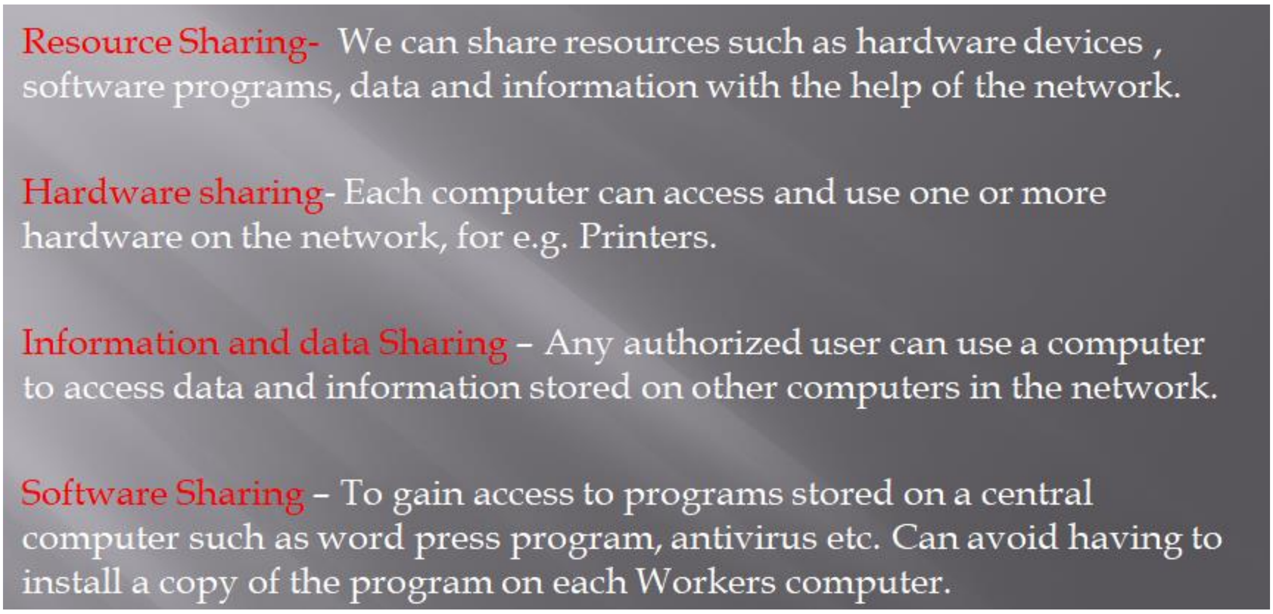


HALF-DUPLEX MODE



FULL DUPLEX MODE

Application of the Computer Network



Resource Sharing- We can share resources such as hardware devices , software programs, data and information with the help of the network.

Hardware sharing- Each computer can access and use one or more hardware on the network, for e.g. Printers.

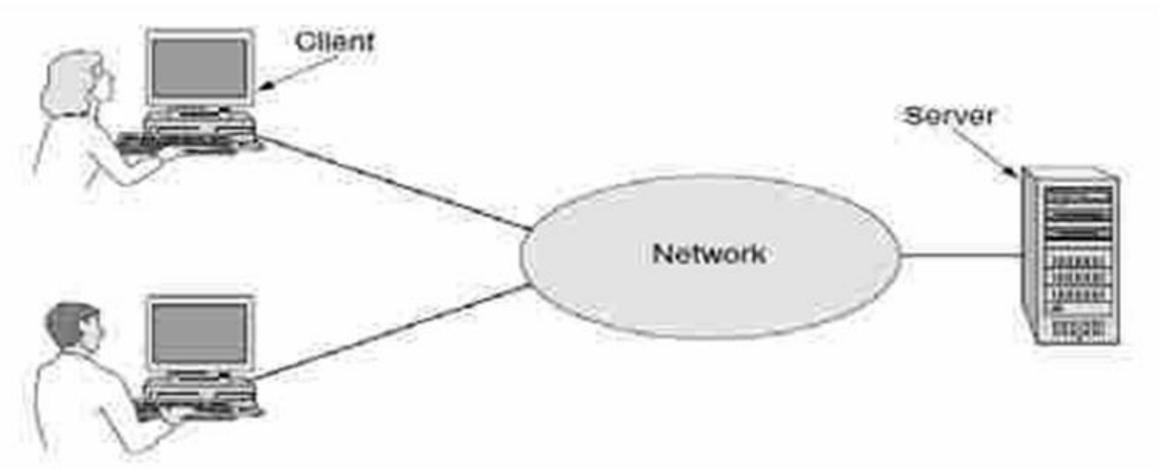
Information and data Sharing – Any authorized user can use a computer to access data and information stored on other computers in the network.

Software Sharing – To gain access to programs stored on a central computer such as word press program, antivirus etc. Can avoid having to install a copy of the program on each Workers computer.

Other Applications:

Business Application:

VPNs (Virtual Private Networks)
This whole arrangement is called the client-server model
Web application,
Communication medium
Email (electronic mail),
IP telephony
Voice over IP (VoIP)
Desktop sharing
E-commerce (electronic commerce)



Network Architecture

Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data.
Simply we can say that how computers are organized and how tasks are allocated to the computer.

Architecture also defines how the computers should get connected to get the maximum advantages of a computer network such as better response time, security, scalability etc.

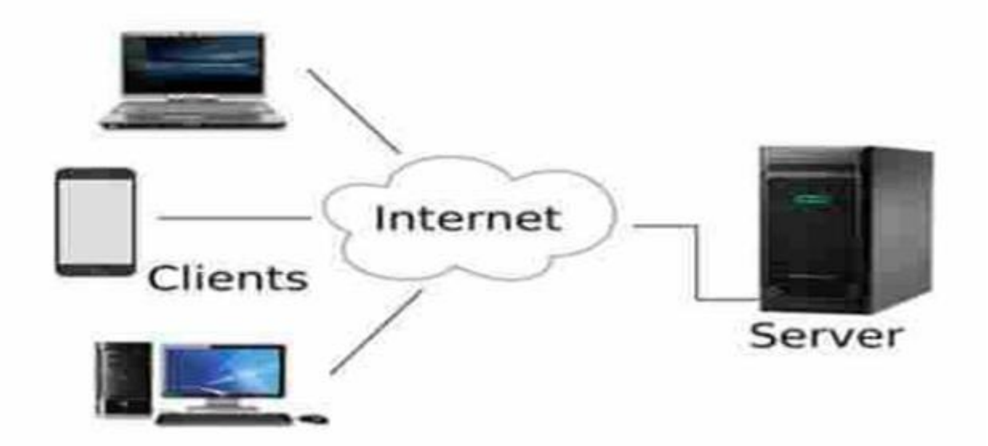
Types:

Computer network falls under two types

1) Client server network
2) P2P (peer-to-peer) network

- **Client Server Network**

Each client is assigned as account name and password that is verified by an authentication service. The authentication service guards access to the network. With the centralization of user accounts, security and access control, server based networks simplify the administration of large network.



The concentration of network resources such as files, printers and applications on servers also makes it easier to backup and maintain the data. Resource can be located on specialized dedicated servers for easier access.

Advantages

- Easier to administer when the network is large.
- All data can be backed up on one central location.

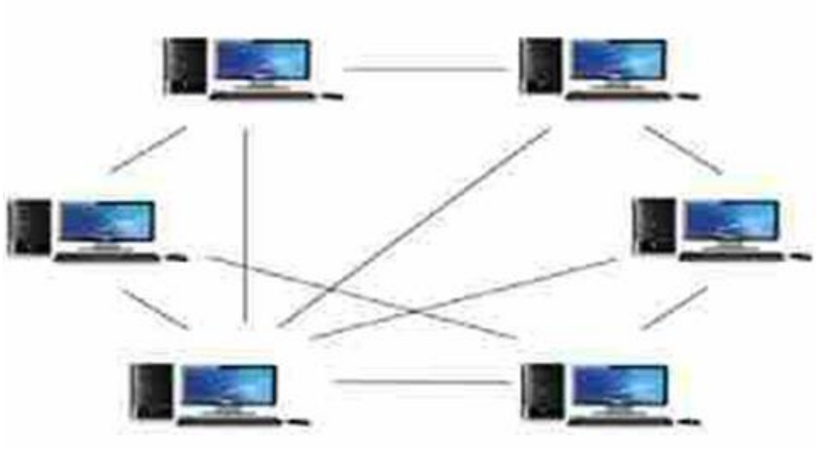
Disadvantages

- Requires expensive, more powerful hardware for the server machines.

- Has a single point of failure user data is unavailable when the server is down.
- Requires expensive specialized network administrative and operational software.
- Requires a professional administrator.

- **Peer-to-Peer Network**

Network computers act as equal partners, or peers. Each computer can take on the client function or the server function.



Suppose computer A may request for a file from computer B, which then sends file to computer A. In this case, computer A acts like the client and computer B as server.

At a later time, their role may be reserved; individual users control their own resources.

The users may decide to share certain files with other users. The users may also require passwords before they allow others to access their resources. Since individual users make these decisions, there is no central point of control or administration in the network.

When a computer acts as a server, the user of that machine may experience reduced performance as the machine server the requests made by other system.

Advantages

- Less expensive to implement.
- Doesn't require additional specialized network administration software.
- Doesn't require a dedicated network administrator.

Disadvantages

- Less secure.
- Doesn't scale well to large networks, and administration becomes unmanageable.
- Each must be trained to perform administrative tasks.
- All machines sharing resources negatively impact the performance.

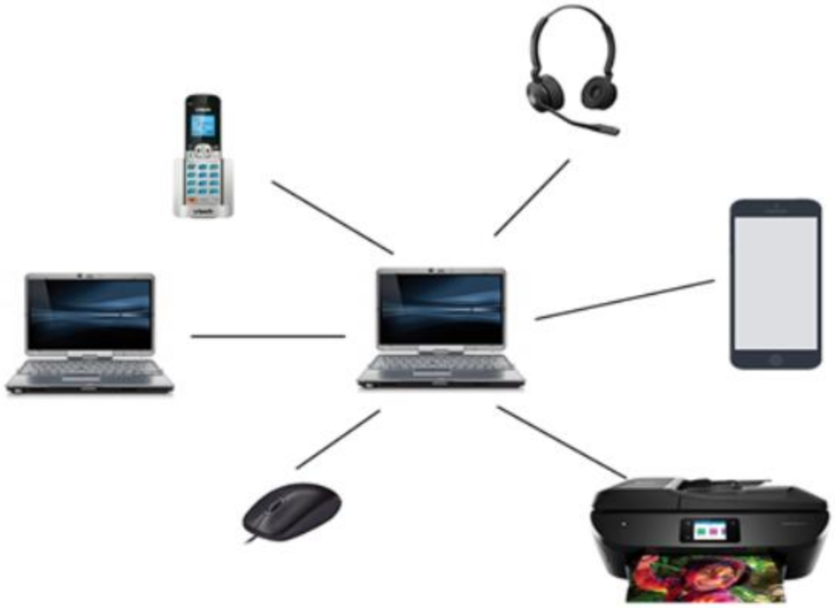
Types of Computer Network

A computer network can be categorized by their size. A **computer network** is mainly of **four types**:

- PAN(Personal Area Network)
- LAN(Local Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

Personal Area Network

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- Thomas Zimmerman was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of 30 feet.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.



➢ Local Area Network

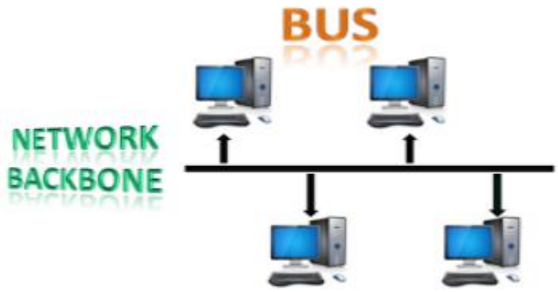
- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.
- Is very fast, with speed from 10mbps to 10GBps.

LAN's can either be made wired or wireless. Twisted pair coax or fiber optic cable can be used in wired LAN's

Nodes in a LAN are linked together with a certain *topology*. These topologies include:

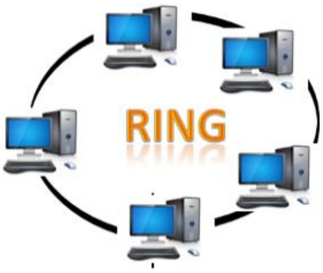
- Bus
- Ring
- Star
- Full mesh

Bus Topology:



- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
- The configuration of a bus topology is quite simpler as compared to other topologies.
- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

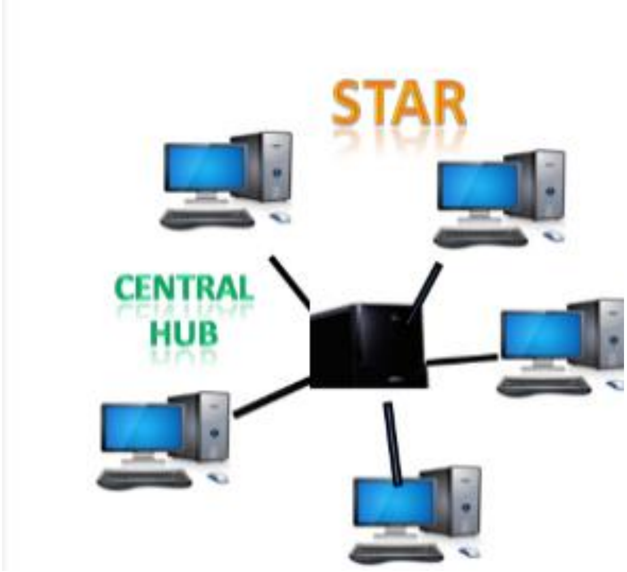
Ring Topology:



- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.

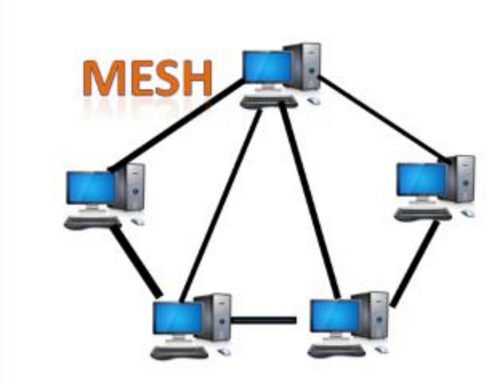
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is **token passing**.
- **Token passing:** It is a network access method in which token is passed from one node to another node.
- **Token:** It is a frame that circulates around the network.

Star Topology



- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
- Coaxial cable or RJ-45 cables are used to connect the computers.
- Hubs or Switches are mainly used as connection devices in a **physical star topology**.
- Star topology is the most popular topology in network implementation.

Full Mesh Topology



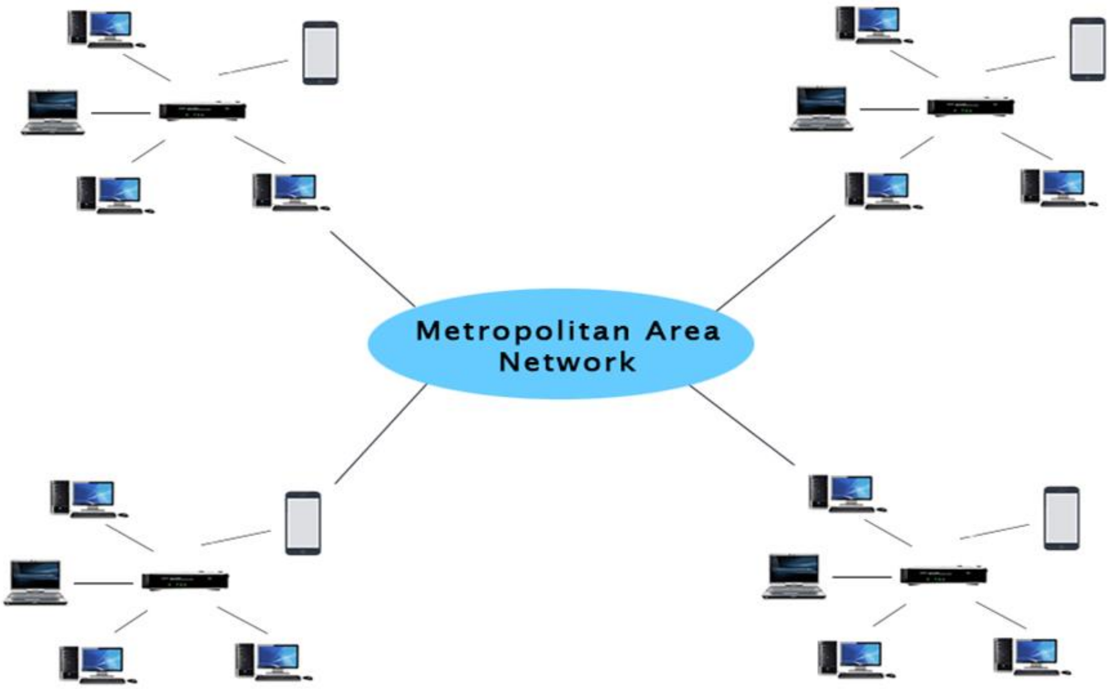
- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.
- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- Mesh topology is mainly used for wireless networks.

MAN (Metropolitan Area Network)

MAN network covers larger area by connections LANs to a larger network of computers.

In MAN various Local area networks are connected with each other through telephone lines.

The size of the Metropolitan area network is larger than LANs and smaller than WANs (wide area networks), a MANs covers the larger area of a city or town.



Uses :

MAN is used in communication between the banks in a city.

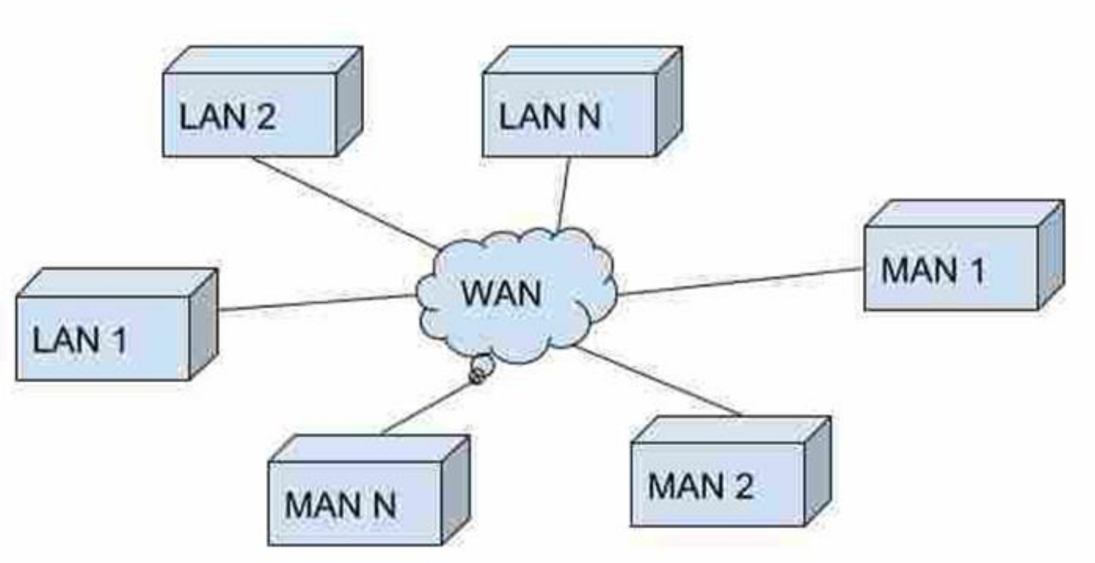
It can be used in an Airline Reservation.

It can be used in a college within a city.

It can also be used for communication in the military.

WAN(Wide Area Network):

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the MAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fiber optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.



Advantages of Wide area network (WAN)

Geographical area: A WAN provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN.

Centralized data: In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.

Get updated files: Software companies work on the live server. Therefore, the programmers get the updated files within seconds.

Exchange messages: In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype etc.

Sharing of software and resources: In WAN network, we can share the software and other resources like a hard drive, RAM.

Global Business: We can do the business over the internet globally.

High bandwidth: The high bandwidth increases the data transfer rate which in turn increases the productivity.

Disadvantages of Wide area network (WAN)

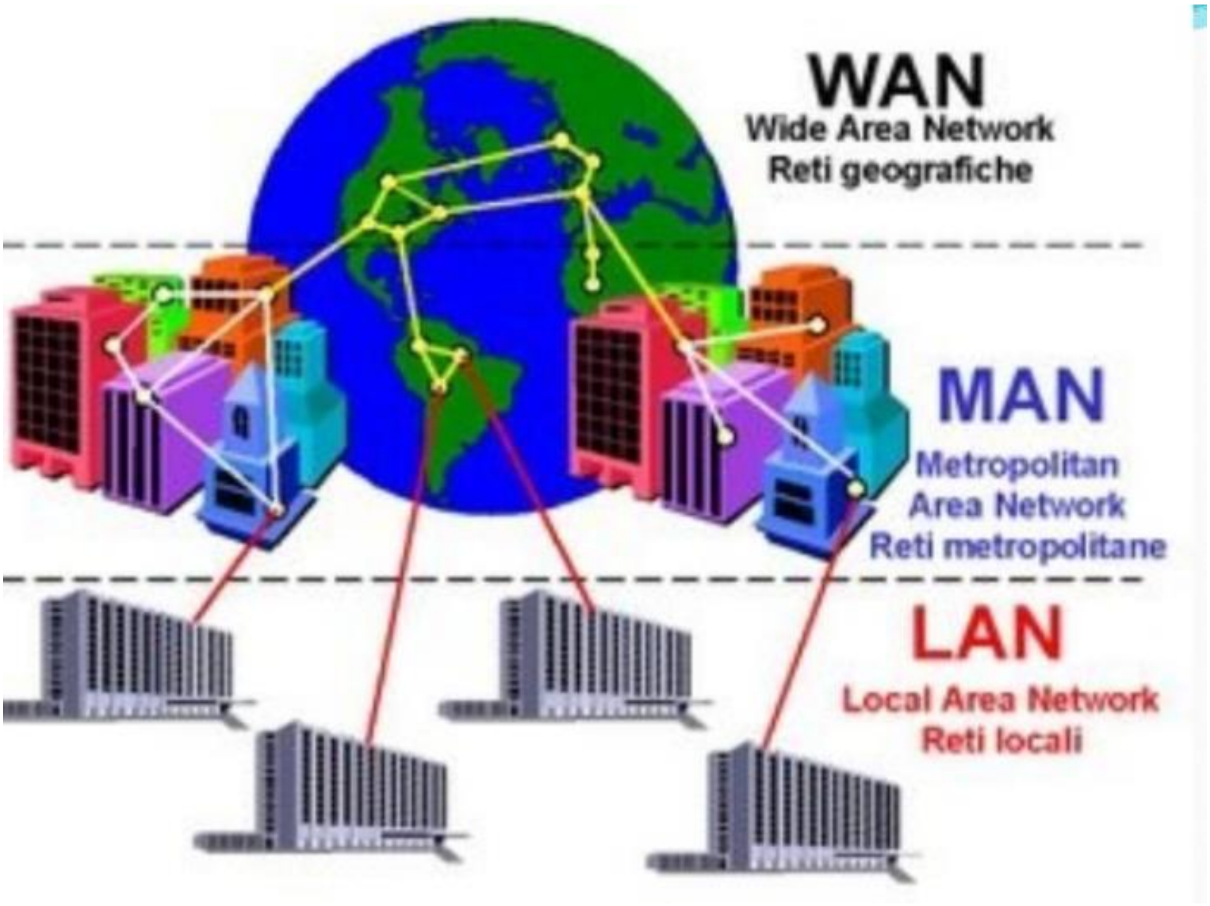
Security issue: A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.

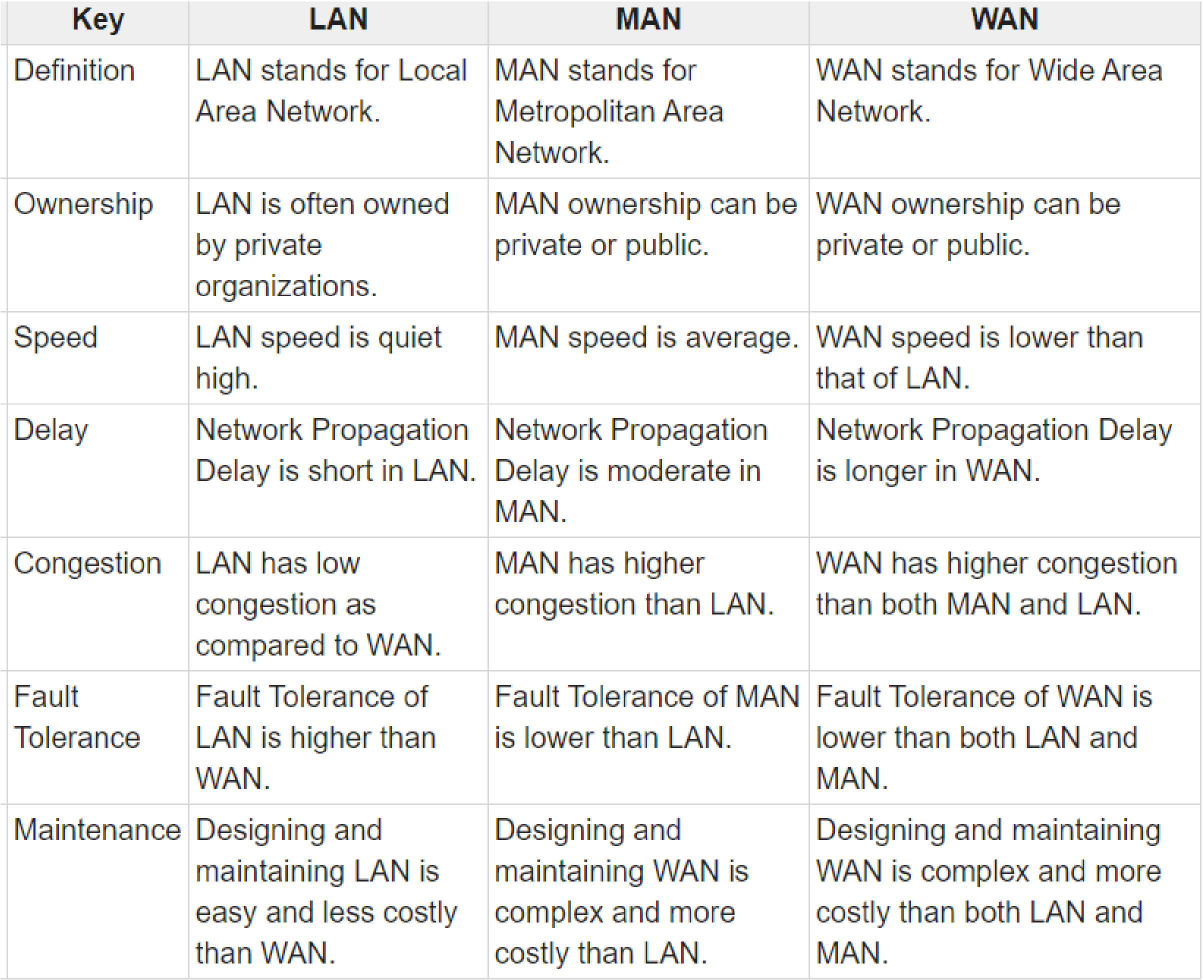
Needs Firewall & antivirus software: The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.

High Setup cost: An installation cost of the WAN network is high as it involves the purchasing of routers, switches.

Troubleshooting problems: It covers a large area so fixing the problem is difficult.

Geographically structured diagram of LAN, MAN and WAN





Key	LAN	MAN	WAN
Definition	LAN stands for Local Area Network.	MAN stands for Metropolitan Area Network.	WAN stands for Wide Area Network.
Ownership	LAN is often owned by private organizations.	MAN ownership can be private or public.	WAN ownership can be private or public.
Speed	LAN speed is quiet high.	MAN speed is average.	WAN speed is lower than that of LAN.
Delay	Network Propagation Delay is short in LAN.	Network Propagation Delay is moderate in MAN.	Network Propagation Delay is longer in WAN.
Congestion	LAN has low congestion as compared to WAN.	MAN has higher congestion than LAN.	WAN has higher congestion than both MAN and LAN.
Fault Tolerance	Fault Tolerance of LAN is higher than WAN.	Fault Tolerance of MAN is lower than LAN.	Fault Tolerance of WAN is lower than both LAN and MAN.
Maintenance	Designing and maintaining LAN is easy and less costly than WAN.	Designing and maintaining WAN is complex and more costly than LAN.	Designing and maintaining WAN is complex and more costly than both LAN and MAN.

Protocols and Standards

- A language that is used by system to communicate with one another.
- A protocol is a set of rules that governs(control) data communications.
- A protocol defines what is communicated, how is communicated, and when it is communicated.

KEY Elements of PROTOCOLS:

Syntax

- Structure or format of the data.
- Indicates how to read the bits - field delineation (border or boundary).
- Syntax should be same in sender and receiver for to communicate.

Semantics

- Interprets the meaning of the bits
- Knows which fields define what action
- Interpretation of the syntax should be same

Timing

- When data should be sent and what
- Speed at which data should be sent or speed at which it is being received

Major Protocols

- **NetBEUI**(NetBios Extended End User Interface)
    - Developed by IBM for Windows and DOS.
    - Nonroutable protocol that sends data but unable to cross the router to reach the network.
    - NetBIOS – session mode- Connection oriented, reliable, error detection, retransmission of data if miss.

    - datagram mode – Connectionless , full of error, but speed, non-reliable
- **IPX/SPX** (Internetwork packet exchange/Sequenced Packet Exchange)
    - IPX – Routing protocol, connectionless, unreliable transport
    - SPX - reliable delivery, connection oriented, errorless data /packets to the destined point.
- **Apple Talk** - Basically use for connecting multiple systems together in Macintosh. Environment.
- **TCP/IP** (Transmission control Protocol/ Internet Protocol)
    - Routable protocols, Reroute Packets, Connect heterogeneous (dissimilar) networks

Demerits:

Complexity in the configuration- regarding IP address, subnet mask and default gateway

Security – open design, unsecure protocol, if need to more secure then additional features need to be done to secure the network traffic, we can use SSL(secure socket layer) for this.

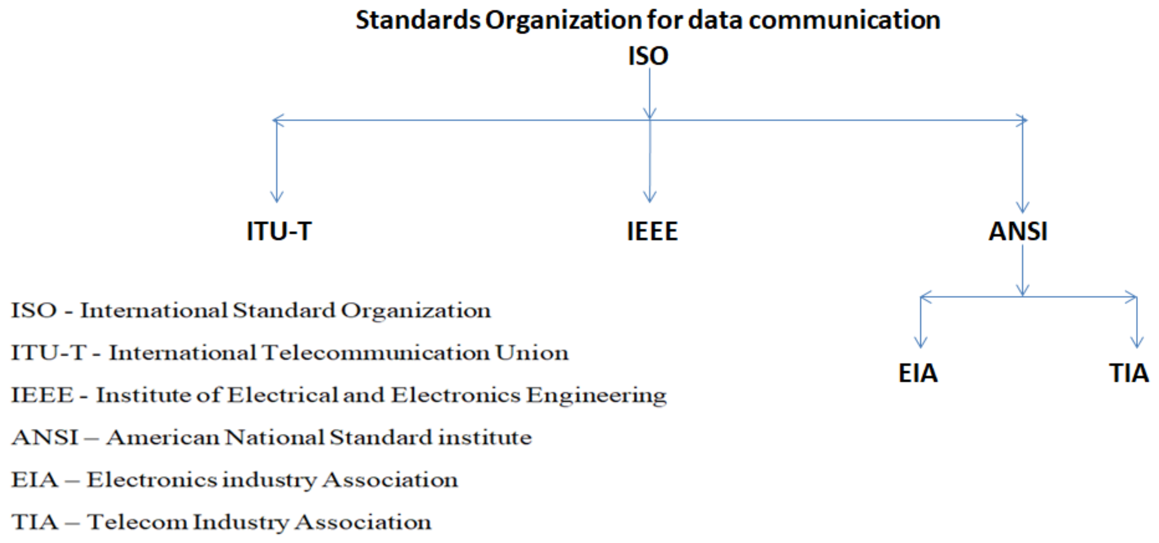
Standards:

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

Two Categories of Standards

De facto: 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.

De jure: Those standards by law or by regulation. These are the standards recognized officially by an Organization.



ISO - International Standard Organization

ITU-T - International Telecommunication Union

IEEE - Institute of Electrical and Electronics Engineering

ANSI – American National Standard institute

EIA – Electronics industry Association

TIA – Telecom Industry Association

OSI Reference Model

- OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.

Principles of OSI Reference Model

The OSI reference model has 7 layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

1. A layer should be created where a different abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.

4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that architecture does not become unwieldy.

Feature of OSI Model

1. Big picture of communication over network is understandable through this OSI model.
2. We see how hardware and software work together.
3. We can understand new technologies as they are developed.
4. Troubleshooting is easier by separate networks.
5. Can be used to compare basic functional relationships on different networks.

Merits:

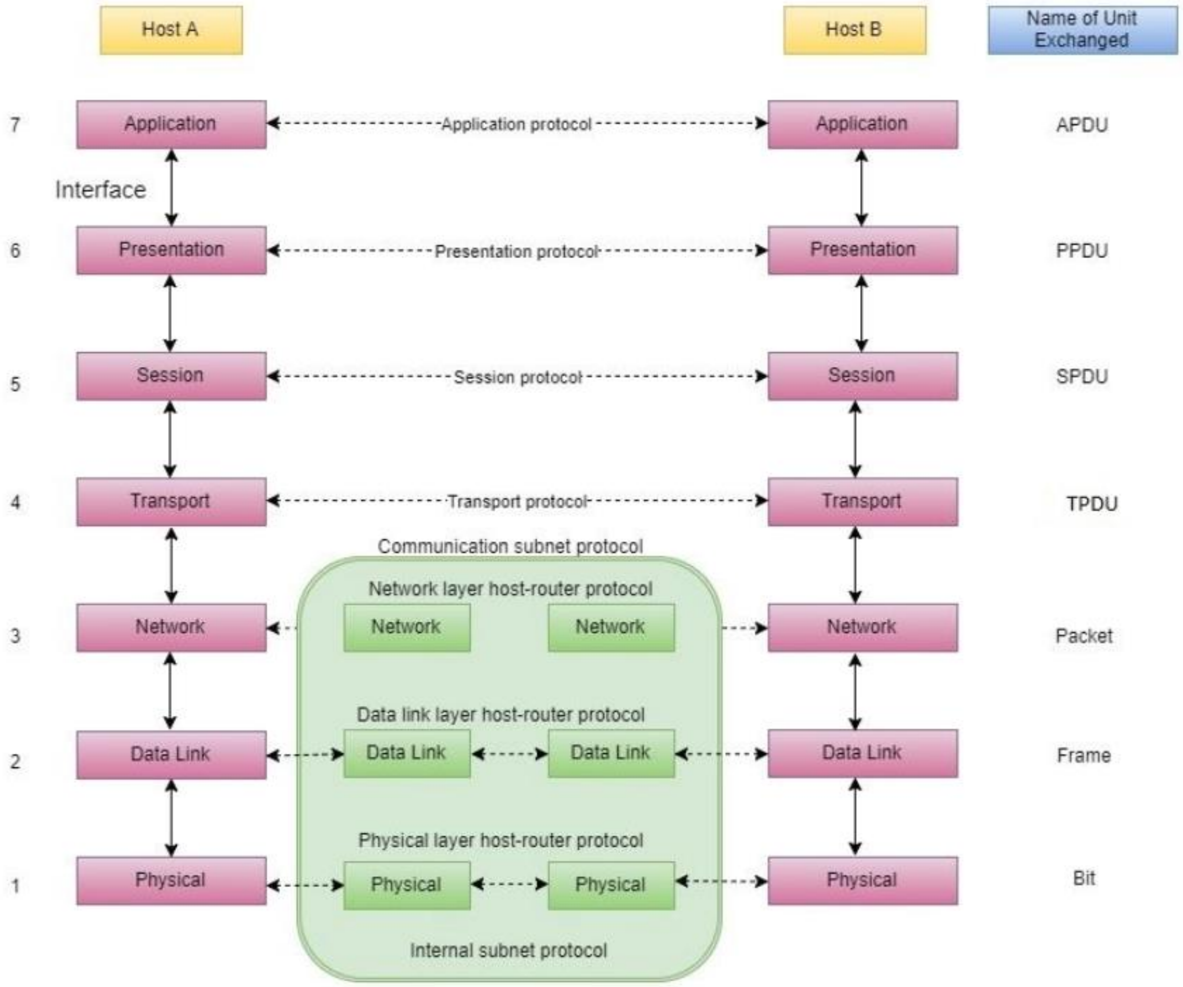
1. OSI model distinguishes well between the services, interfaces and protocols.
2. Protocols of OSI model are very well hidden.
3. Protocols can be replaced by new protocols as technology changes.
4. Supports connection oriented services as well as connectionless service.

Demerits:

1. Model was devised before the invention of protocols.
2. Fitting of protocols is tedious task.
3. It is just used as a reference model.

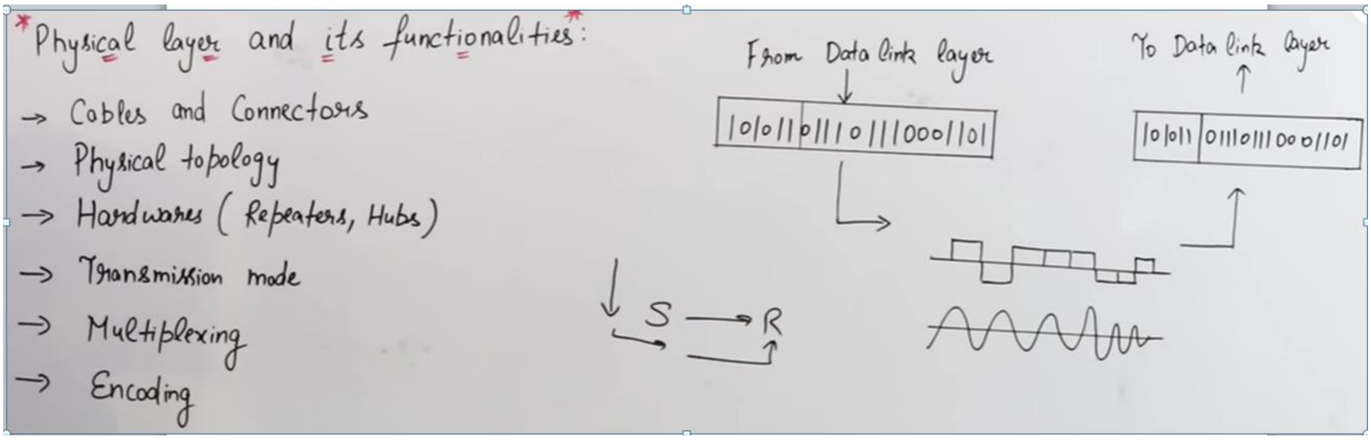
The ISO-OSI model is seven layer architecture. It defines seven layers or levels in a complete communication system. They are:

1. Application Layer
2. Presentation Layer
3. Session Layer
4. Transport Layer
5. Network Layer
6. Data link Layer
7. Physical Layer



Physical Layer

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

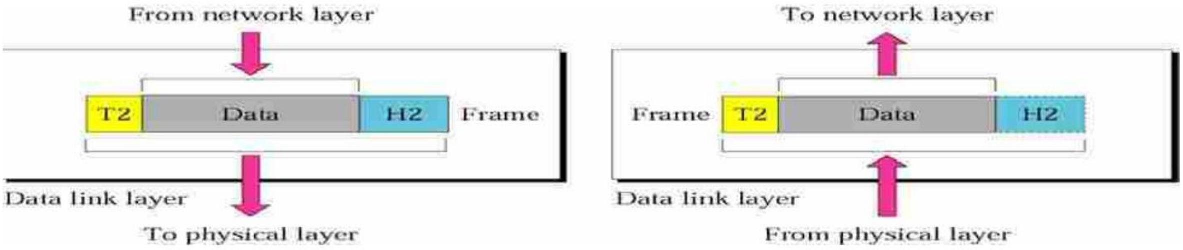


*Physical layer and its functionalities:

- → Cables and Connectors
- → Physical topology
- → Hardwares (Repeaters, Hubs)
- → Transmission mode
- → Multiplexing
- → Encoding

Data Link Layer

- ➢ Data link layer synchronizes the information which is to be transmitted over the physical layer.
- ➢ The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
- ➢ Transmitting and receiving data frames sequentially is managed by this layer.
- ➢ This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.
- ➢ This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.



Network Layer

- ➢ Network Layer routes the signal through different channels from one node to other.
- ➢ It acts as a network controller. It manages the Subnet traffic.
- ➢ It decides by which route data should take.
- ➢ It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.

Other responsibilities of the network layer include the following:

- **Logical addressing.**
    - ➢ The physical addressing implemented by the data link layer handles the addressing problem locally.
    - ➢ If a packet passes the network boundary, we need another addressing system to help the source and destination systems.
    - ➢ The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.
- **Routing**
    - ➢ When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination.
    - ➢ One of the functions of the network layer is to provide this mechanism.
- **Path determination:**
    - ➢ Route taken by packets from source to destination (Routing Algorithm). OSPF, BGP, IS-IS

Transport Layer

- ➢ Transport Layer decides if data transmission should be on parallel path or single path.
- ➢ Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer
- ➢ It receives messages from the Session layer above it, converts the message into smaller units and passes it on to the Network layer.
- ➢ Transport layer can be very complex, depending upon the network requirements.

Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

Session Layer

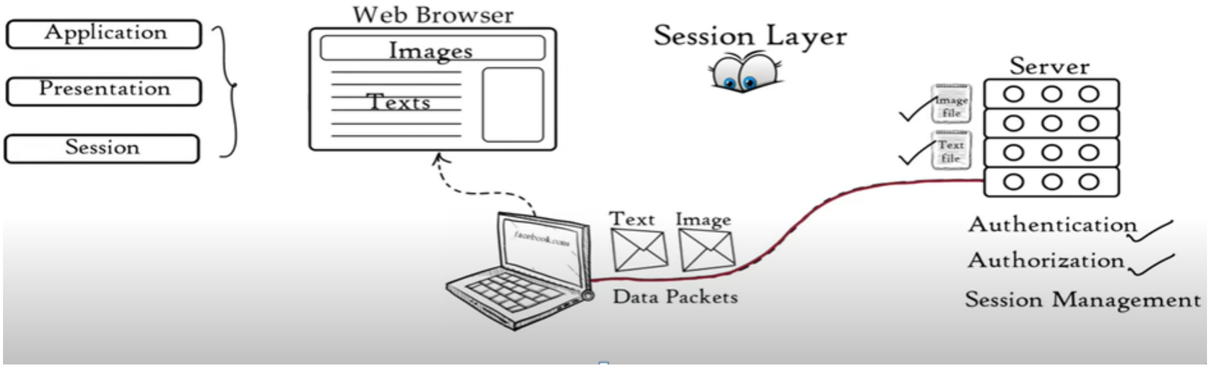
- ➢ Session Layer manages and synchronize the conversation between two different applications.
- ➢ Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

Basically, Session has 3 major roles.

Authentication: Who you are?? Is this the right person to access??

Authorization: Sufficient permission has or not to access

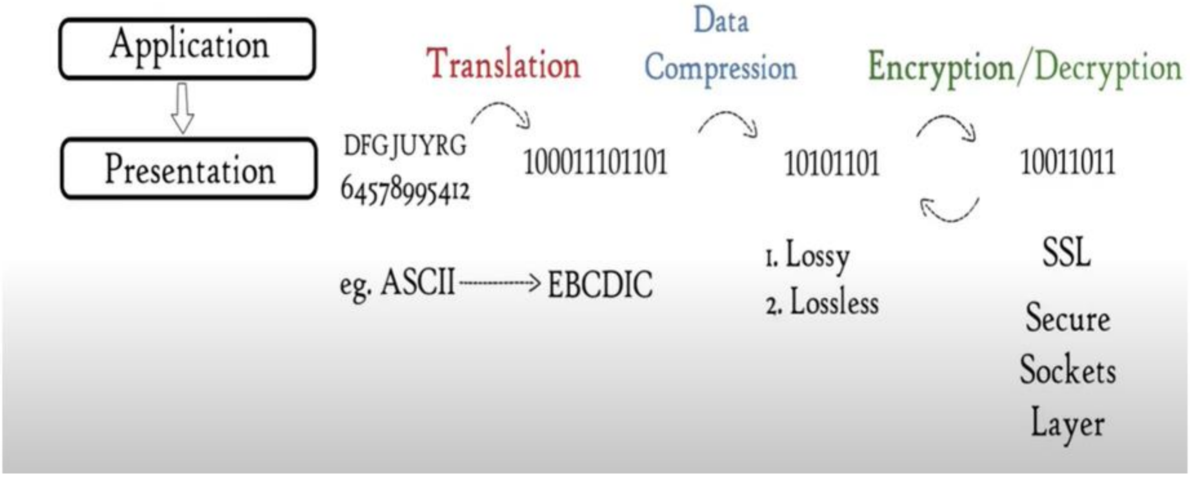
Session management: Between Server and client, it creates session to send and receive the data in a separate session. For e.g. We can check the figure.



Presentation layer:

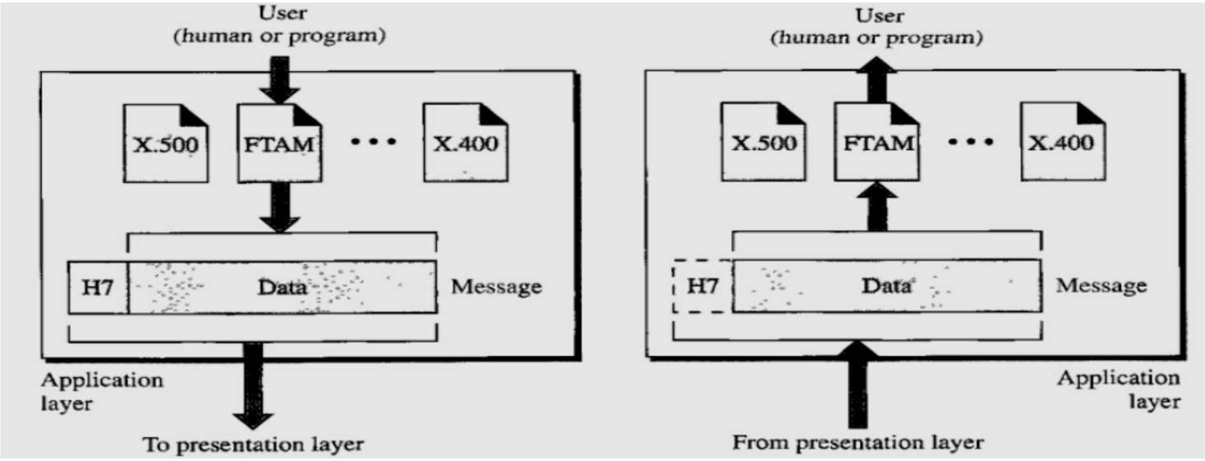
Presentation Layer Specific responsibilities of the presentation layer include the following:

- **Translation.**
- The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on.
- The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods.
- The presentation layer at the sender changes the information from its sender-dependent format into a common format.
- The presentation layer at the receiving machine changes the common format into its receiver-dependent format.
- Encryption.
- To carry sensitive information, a system must be able to ensure privacy.
- Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network.
- Decryption reverses the original process to transform the message back to its original form.
- Compression.
- Data compression reduces the number of bits contained in the information.
- Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.



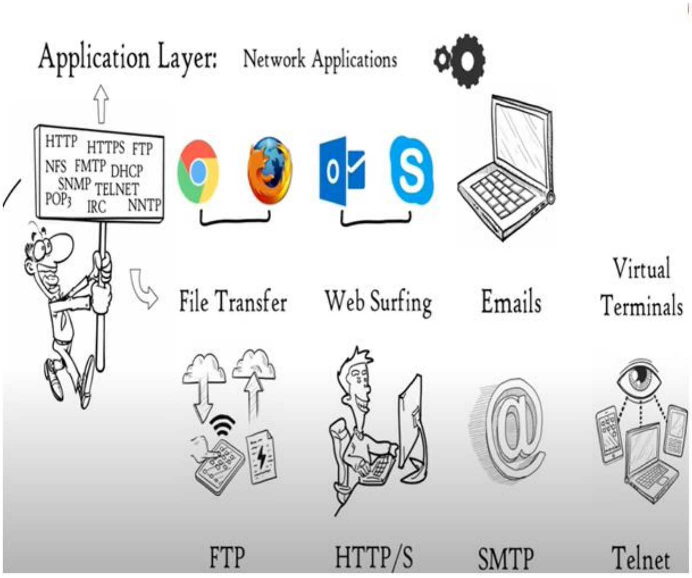
Application Layer

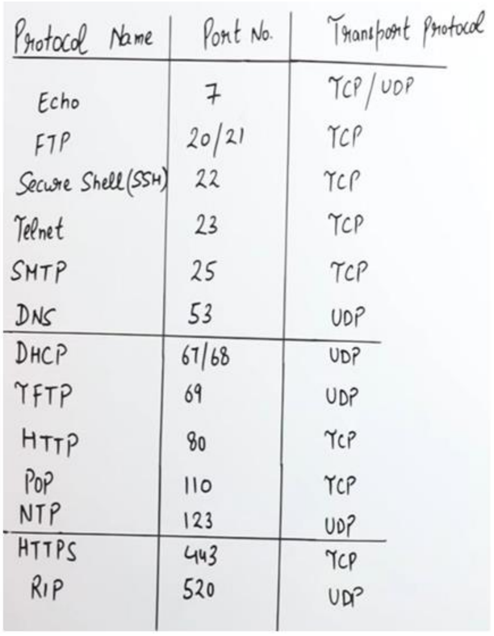
- The application layer enables the user, whether human or software, to access the network.
- It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.
- The figure shows the relationship of the application layer to the user and the presentation layer.



Specific services provided by the application layer include the following:

- **Network virtual terminal**
- A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.
- To do so, the application creates a software emulation of a terminal at the remote host.
- The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa.
- The remote host believes it is communicating with one of its own terminals and allows the user to log on.
- **File transfer, access, and management**
- This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- **Mail services**
- This application provides the basis for e-mail forwarding and storage.
- **Directory services**
- This application provides distributed database sources and access for global information about various objects and services.





Protocol Name	Port No.	Transport Protocol
Echo	7	TCP/UDP
FTP	20/21	TCP
Secure Shell (SSH)	22	TCP
Telnet	23	TCP
SMTP	25	TCP
DNS	53	UDP
DHCP	67/68	UDP
TFTP	69	UDP
HTTP	80	TCP
POP	110	TCP
NTP	123	UDP
HTTPS	443	TCP
RIP	520	UDP

Merits of OSI reference model

- OSI model distinguishes well between the services, interfaces and protocols.
- Protocols of OSI model are very well hidden.
- Protocols can be replaced by new protocols as technology changes.
- Supports connection oriented services as well as connectionless service.

Demerits of OSI reference model

- Model was devised before the invention of protocols.
- Fitting of protocols is tedious task.
- It is just used as a reference model.

TCP/IP Protocol Suite

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Protocols that are used in TCP/IP suite

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)
- virtual terminal (TELNET)
- file transfer(FTP), and electronic mail (SMTP)
- Domain Name System (DNS)
- HTTP (Hyper Text Transfer Protocol)
- Stream Control Transmission Protocol (SCTP)
- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP)
- Internet Group Message Protocol (IGMP)
- ICMP (Internet Control Message Protocol)

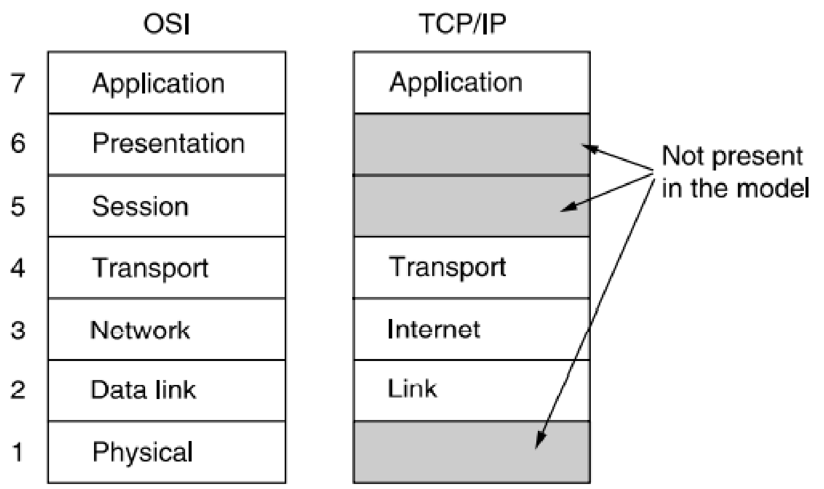


Figure 1-21. The TCP/IP reference model.

TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality; however, the modules are not necessarily interdependent whereas the OSI model specifies which functions belong to each of its layers, the layers of the TCP/IP protocol suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system.

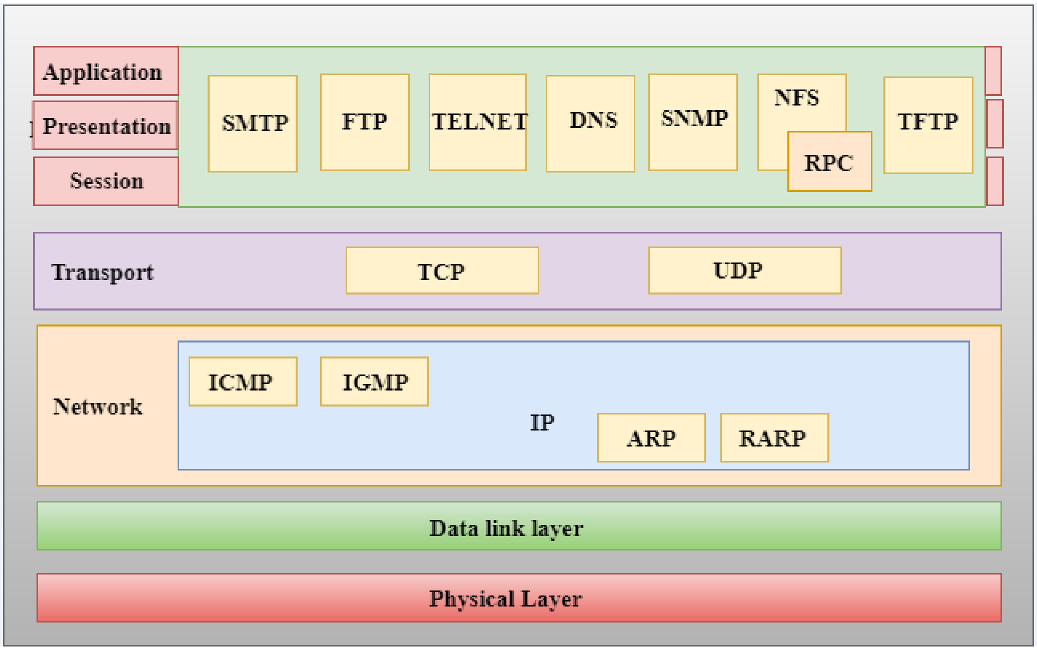


Figure: TCP/IP PROTOCOL SUITE (TCP/IP and OSI model)

Functional layer of TCP/IP Protocol

Network Access Layer

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Following are the protocols used in Network layer are:

- **IP Protocol:** IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.

- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

- **ARP Protocol**

  - ARP stands for **Address Resolution Protocol**.
  - ARP is a network layer protocol which is used to find the physical address from the IP address.
  - **The two terms are mainly associated with the ARP Protocol:**
    - **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
    - **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

- **ICMP Protocol**

  - **ICMP** stands for Internet Control Message Protocol.
  - It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
  - A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
  - An ICMP protocol mainly uses two terms:
    - **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.

- **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.

- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

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

Transport Layer:

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

User Datagram Protocol:

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

UDP consists of the following fields:

Source port address: The source port address is the address of the application program that has created the message.

Destination port address: The destination port address is the address of the application program that receives the message.

Total length: It defines the total number of bytes of the user datagram in bytes.

Checksum: The checksum is a 16-bit field used in error detection.

- **Transmission Control Protocol**:
  - The TCP provides full transport-layer services to applications.
  - TCP is a reliable stream transport protocol.
  - The term stream, in this context, means connection-oriented:
  - A connection must be established between both ends of a transmission before either can transmit data.
  - At the sending end of each transmission, TCP divides a stream of data into smaller units called segments.
  - Each segment includes a sequence number for reordering after receipt, together with an acknowledgment number for the segments received.
  - Segments are carried across the internet inside of IP datagram.
  - At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.
- **Stream Control Transmission Protocol**:
  - The SCTP provides support for newer applications such as voice over the Internet.
  - It is a transport layer protocol that combines the best features of UDP and TCP.

Application Layer:

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using HTTP protocol to interact with the network where HTTP protocol is an application layer protocol.

Following are the main protocols used in the application layer:

- **HTTP:**

- HTTP stands for Hypertext transfer protocol.
- This protocol allows us to access the data over the world wide web.
- It transfers the data in the form of plain text, audio, video.

- It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.

- **SNMP**:
  - SNMP stands for Simple Network Management Protocol.
  - It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
- **SMTP**:
  - SMTP stands for Simple mail transfer protocol.
  - The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol.
  - This protocol is used to send the data to another e-mail address.
- **DNS**:
  - DNS stands for Domain Name System.
  - An IP address is used to identify the connection of a host to the internet uniquely.
  - But, people prefer to use the names instead of addresses.
  - Therefore, the system that maps the name to the address is known as Domain Name System.
- **TELNET**:
  - It is an abbreviation for Terminal Network.
  - It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- **FTP**:
  - FTP stands for File Transfer Protocol.
  - FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

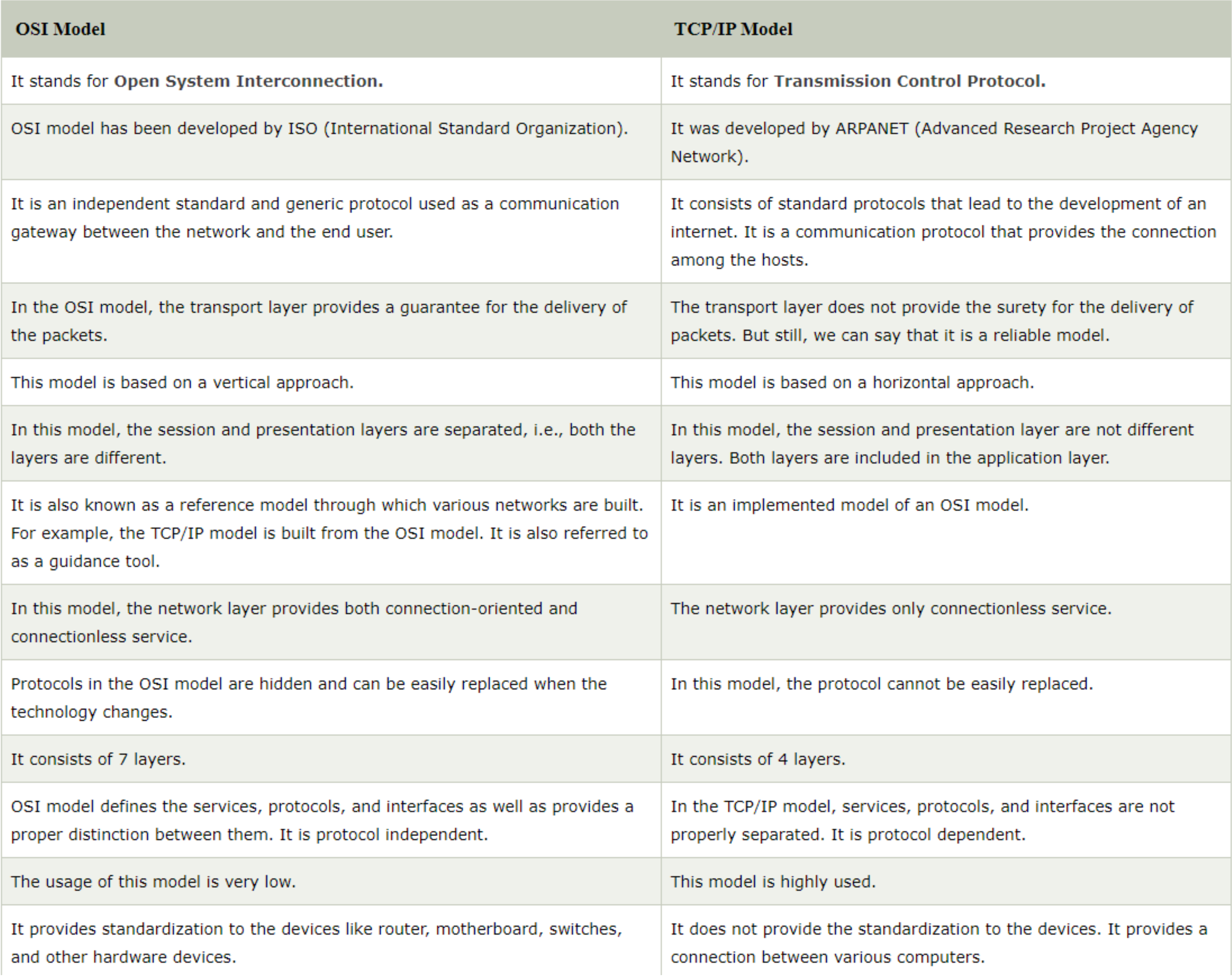
Merits of TCP/IP model

- It operated independently.
- It is scalable.
- Client/server architecture.
- Supports a number of routing protocols.
- Can be used to establish a connection between two computers.

Demerits of TCP/IP

- In this, the transport layer does not guarantee delivery of packets.
- The model cannot be used in any other application.
- Replacing protocol is not easy.
- It has not clearly separated its services, interfaces and protocols.

Comparison between OSI and TCP/IP Reference model



OSI Model	TCP/IP Model
It stands for **Open System Interconnection.**	It stands for **Transmission Control Protocol.**
OSI model has been developed by ISO (International Standard Organization).	It was developed by ARPANET (Advanced Research Project Agency Network).
It is an independent standard and generic protocol used as a communication gateway between the network and the end user.	It consists of standard protocols that lead to the development of an internet. It is a communication protocol that provides the connection among the hosts.
In the OSI model, the transport layer provides a guarantee for the delivery of the packets.	The transport layer does not provide the surety for the delivery of packets. But still, we can say that it is a reliable model.
This model is based on a vertical approach.	This model is based on a horizontal approach.
In this model, the session and presentation layers are separated, i.e., both the layers are different.	In this model, the session and presentation layer are not different layers. Both layers are included in the application layer.
It is also known as a reference model through which various networks are built. For example, the TCP/IP model is built from the OSI model. It is also referred to as a guidance tool.	It is an implemented model of an OSI model.
In this model, the network layer provides both connection-oriented and connectionless service.	The network layer provides only connectionless service.
Protocols in the OSI model are hidden and can be easily replaced when the technology changes.	In this model, the protocol cannot be easily replaced.
It consists of 7 layers.	It consists of 4 layers.
OSI model defines the services, protocols, and interfaces as well as provides a proper distinction between them. It is protocol independent.	In the TCP/IP model, services, protocols, and interfaces are not properly separated. It is protocol dependent.
The usage of this model is very low.	This model is highly used.
It provides standardization to the devices like router, motherboard, switches, and other hardware devices.	It does not provide the standardization to the devices. It provides a connection between various computers.

Critiques of OSI and TCP/IP Reference model

Neither the OSI model and its protocols nor the TCP/IP model and its protocols are perfect. The criticism of the OSI model and its protocols can be summarized as:

1. Bad timing.
2. Bad technology.
3. Bad implementations.
4. Bad politics.

Bad timing

The competing TCP/IP protocols were already in widespread use by research universities by the time the OSI protocols appeared. While the billion-dollar wave of investment had not yet hit, the academic market was large enough that many vendors had begun cautiously offering TCP/IP products. When OSI came around, they did not want to support a second protocol stack until they were forced to, so there were no initial offerings. With every company waiting for every other company to go first, no company went first and OSI never happened.

Bad Technology

The second reason that OSI never caught on is that both the model and the protocols are flawed. The choice of seven layers was more political than technical, and two of the layers (session and presentation) are nearly empty, whereas two other ones (data link and network) are overfull.

The OSI model, along with its associated service definitions and protocols, is extraordinarily complex. They are also difficult to implement and inefficient in operation.

In addition to being incomprehensible, another problem with OSI is that some functions, such as addressing, flow control, and error control, reappear again and again in each layer.

Bad Implementations

Given the enormous complexity of the model and the protocols, it will come as no surprise that the initial implementations were huge, unwieldy, and slow. It did not take long for people to associate "OSI" with "poor quality". Although the products improved in the course of time, the image stuck.

In contrast, one of the first implementations of TCP/IP was part of Berkeley UNIX and was quite good. People began using it quickly, which led to a large user community, which led to improvements, which led to an even larger community. Here the spiral was upward instead of downward.

Bad Politics

On account of the initial implementation, many people, especially in academia, thought of TCP/IP as part of UNIX, and UNIX in the 1980s in academia was not unlike parenthood and apple pie.

Critiques of TCP/IP

- First, the model does not clearly distinguish the concepts of services, interfaces, and protocols. Good software engineering practice requires differentiating between the specification and the implementation, something that OSI does very carefully, but TCP/IP does not. Consequently, the TCP/IP model is not much of a guide for designing new networks using new technologies.
- Second, the TCP/IP model is not at all general and is poorly suited to describing any protocol stack other than TCP/IP. Trying to use the TCP/IP model to describe Bluetooth, for example, is completely impossible.
- Third, the link layer is not really a layer at all in the normal sense of the term as used in the context of layered protocols. It is an interface (between the network and data link layers). The distinction between an interface and layer is crucial and one should not be sloppy about it.
- Fourth, the TCP/IP model does not distinguish between the physical and data link layers. These are completely different. The physical layer has to do with the transmission characteristics of copper wire, fiber optics, and wireless communication. The data link layer's job is to delimit the start and end of frames and get them from one side to the other with the desired degree of reliability. A proper model should include both as separate layers. The TCP/IP model does not do this.

- In Short for TCP/IP Critiques, we can arrange as
  - Service, interface, and protocol not very successful
  - Not a general model
  - Host-to-network “layer” not really a layer
  - No mention of physical and data link layers
  - Minor protocols deeply establish, hard to replace