COMPUTER NETWORKS - UNIT 1

INTRODUCTION

Data communications and networking is changing our lives and the way businesses are carried out today. Businesses today depend on computer networks and internetworks which help them to have access to accurate information and make decisions faster.

Technological advances in communications and networking have made it possible for communication links to carry more and faster signals. Hence services are evolving to make use of this. Example: conference calls, call waiting service, caller ID, voice mail etc.

The term telecommunication means communication at a distance. example: telephony, telegraphy, and television.

Data refers to information presented in whatever form is agreed upon by the parties creating and using the data.

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.

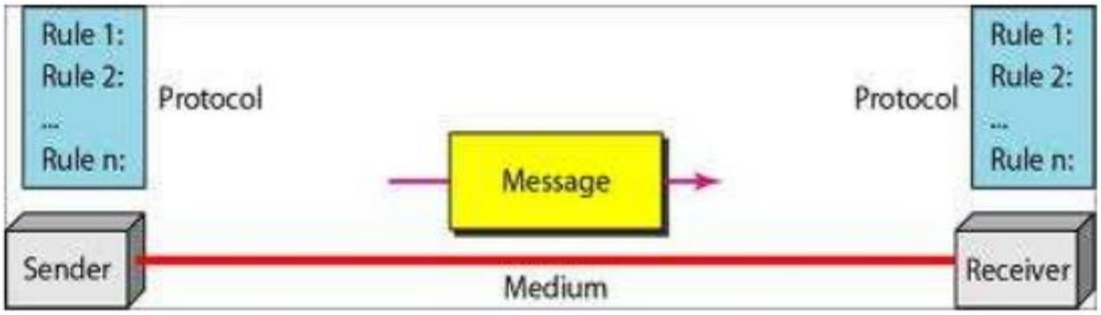
Data is represented in different forms like text, numbers, images, audio and video.

Both the devices are a part of this communication system which is made up of physical equipment (hardware) and programs (software).

4 fundamental characteristics for effective data communication:

1) **Delivery :** The data must be delivered to its correct destination/ user/ device.
2) **Accuracy** : The data must be delivered accurately without any alterations/ changes.
3) **Timeliness**: The system must deliver data in a timely manner. Late data is useless.
4) **Jitter** : There must be as less jitter as possible so that the quality of data is not reduced (jitter is the delay in packet arrival time).

Components of data communication system:



There are 5 components of data communication system:

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

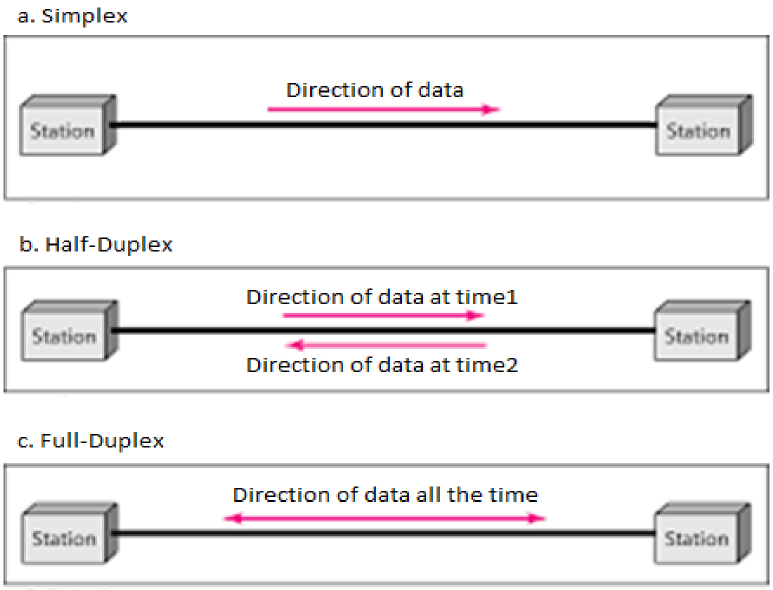
Data Flow:

Communication between devices can be simplex, half-duplex or full-duplex.

Simplex mode: The communication is unidirectional. Only one of the two devices on a link can transmit at any given time. The other can only receive. example: keyboards & monitors , television networks

Half-Duplex mode: In this mode, each station can both transmit and receive but not at the same time. When one station is sending, other is receiver and vice versa. example: Walkie-talkie , Citizen band (CB) radios

Full-Duplex mode: In this mode, both stations can transmit and receive simultaneously. example: telephone network.



NETWORKS:

A network is a set of devices (nodes) connected by communication links. A node can be computer, printer or any other device. Computer network means "A collection on autonomous computers interconnected by a single technology in order to share data, share resources, communication and increase productivity".

Network Applications

Computer systems and peripherals are connected to form a network. They provide numerous advantages:

1. **Business Application :** Resource sharing, and the goal is to make all programs, equipment, and especially data available to anyone on the network without regard to the physical location of the resource and the user. For smaller companies, all the computers are likely to be in a single office or single building, but for larger ones, the computers and employees may be scattered over number of offices and plants in many countries. A computer network can provide a powerful communication medium among employees through email, videoconferencing etc. Companies can do business electronically with other companies which is known as e-commerce.
2. **Home Application :** Some of the most popular uses of the Internet for home users are :
   - Access to remote information : Access to remote information comes in many forms. It can be surfing the www for information or for entertainment.
   - Person to person communication : Email is already used on daily basis by millions of people all over the world. Other forms of communication are videoconferencing, instant messaging, chat room, newsgroup, peer to peer communication etc.
   - Interactive entertainment : It is a huge growing industry. Television programs, movies, videos, audios, computer games etc, are different forms of entertainments.
   - Electronic commerce : Home shopping is already popular and enables users to inspect the online catalogs of thousands of companies. Many people's already pay their bills, manage their bank accounts and handle their investment electronically.
3. **Mobile Users :** Mobile computers, such as notebook computers and personal digital assistances are one of the fastest growing segments of the computer industry. It makes use of wireless network. As the computer used here are portable, people from any place can access to internet for work, business and entertainment.
4. **Some other general applications are :**
   - Education
   - Science and Engineering
   - Medical
   - Resource sharing such as printers and storage devices
   - Exchange of information by means of e-Mails and FTP
   - Information sharing by using Web or Internet
   - Interaction with other users using dynamic web pages
   - IP phones
   - Video conferences
   - Parallel computing
   - Instant messaging, etc.

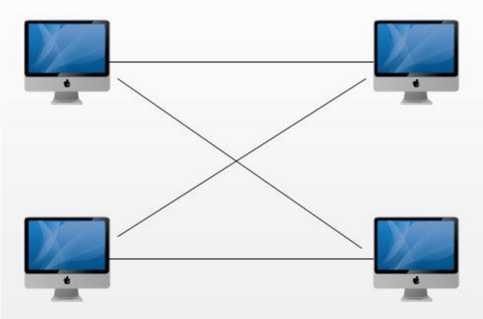
Network Architecture

Network architectures are sometimes classified into two broad categories:

1. peer-to-peer architectures.
2. client-server architectures,

1. Peer-to-Peer Architectures

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.



Peer to Peer Relationship

Advantages Of Peer-To-Peer Network:

- It is less costly as it does not contain any dedicated server.
- If one computer stops working but, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

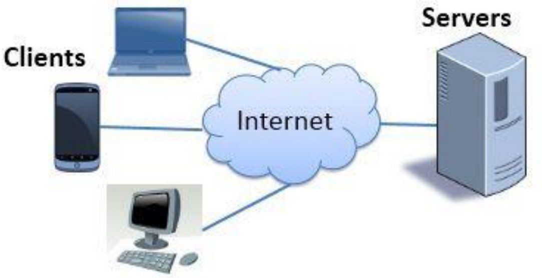
Disadvantages Of Peer-To-Peer Network:

- In the case of Peer-To-Peer network, it does not contain the centralized system . Therefore, it cannot back up the data as the data is different in different locations.
- It has a security issue as the device is managed itself.

2. client-server architectures :

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a server while all other computers in the network are called clients.
- A server performs all the major operations such as security and network management.

- A server is responsible for managing all the resources such as files, directories, printer, etc.
- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.



Client-Servers Network Model

Tiered Architectures

i) Two-tier architectures : The system architecture consists of a data server layer and an application client layer. Data access computation is associated with the data server layer, and the user interface is associated with the client application layer. If most of the application logic is associated with the client application logic, it is sometimes referred to as a “fat client.” If it is associated with the data access server, the application client layer is sometimes referred to as a “thin client.”

ii) Three-tier architecture : The system architecture consists of data server layer, an application server layer and a client application layer. The application server layer facilitates the separation of application logic from presentation, and promotes distributed processing.

iii) Multi-tier architecture : The system architecture is a superset of a three-tier architecture, and includes additional layers for data and/or application servers.

Types of Connections:

A communication link is a pathway that transfers data from one device to another.

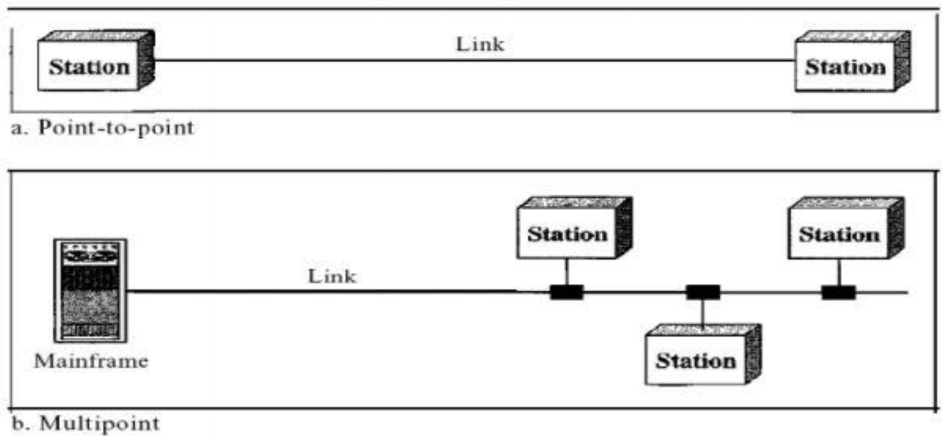
There are 2 types of connections:

1) Point – to – Point :

A point – to – point connection provides a dedicated link between two devices and uses the entire capacity of the link for transmission.
example: point to point link between remote control and television.

2) Multipoint (Multidrop) :

A multipoint connection is one in which more than two devices share a single link. The channel capacity is shared by several devices simultaneously (also called as spatially shared) or the devices take turns to share (called as timeshared).

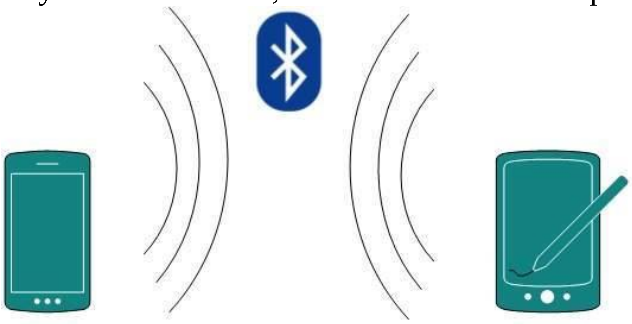


Classification of computer networks based on geographical area :

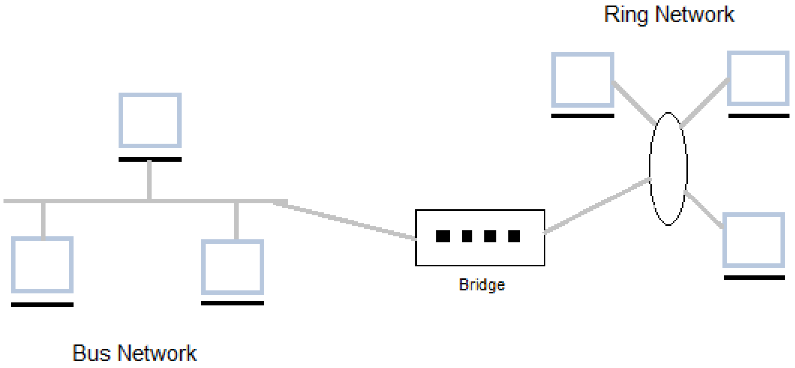
Classification based on geographical area :

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

Personal Area Network (PAN) - The interconnection of devices within the range of an individual person, typically within a range of 10 meters. For example, a wireless network connecting a computer with its keyboard, mouse or printer is a PAN. Also, a PDA that controls the user's hearing aid or pacemaker fits in this category. Typically, this kind of network could also be interconnected without wires to the Internet or other networks. A Personal Area Network (PAN) is smallest network which is very personal to a user. This may include Bluetooth enabled devices or infra-red enabled devices. PAN may include wireless computer keyboard and mouse, Bluetooth enabled headphones, wireless printers and TV remotes.



Local Area Network (LAN) - Privately-owned networks covering a small geographic area, like a home, office, building or group of buildings (e.g. campus). They are widely used to connect computers in company offices and factories to share resources (e.g., printers) and exchange information. LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance. Traditional LANs run at speeds of 10 Mbps to 100 Mbps, have low delay (microseconds or nanoseconds), and make very few errors. Newer LANs operate at up to 10 Gbps.

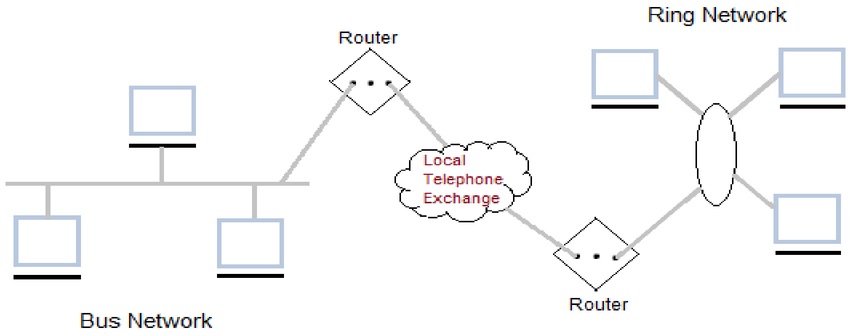


(Different Topologies interconnected in a Local Area Network)

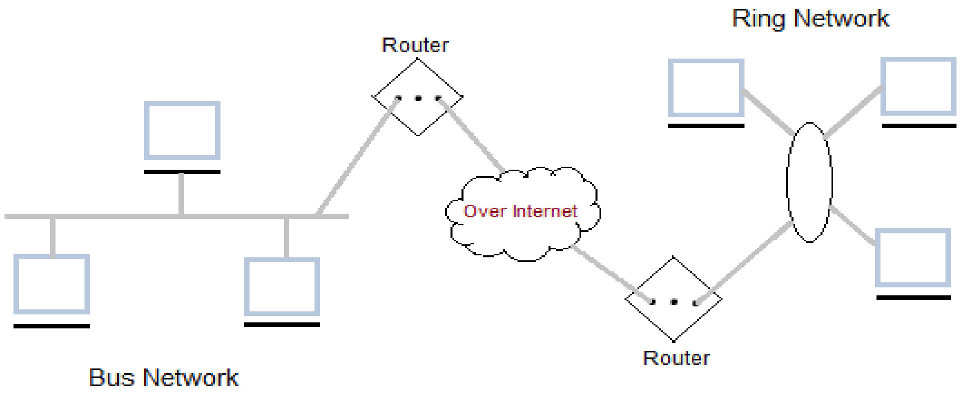
Applications of LAN

- One of the computer in a network can become a server serving all the remaining computers called clients. Software can be stored on the server and it can be used by the remaining clients.
- Connecting Locally all the workstations in a building to let them communicate with each other locally without any internet access.
- Sharing common resources like printers etc are some common applications of LAN.

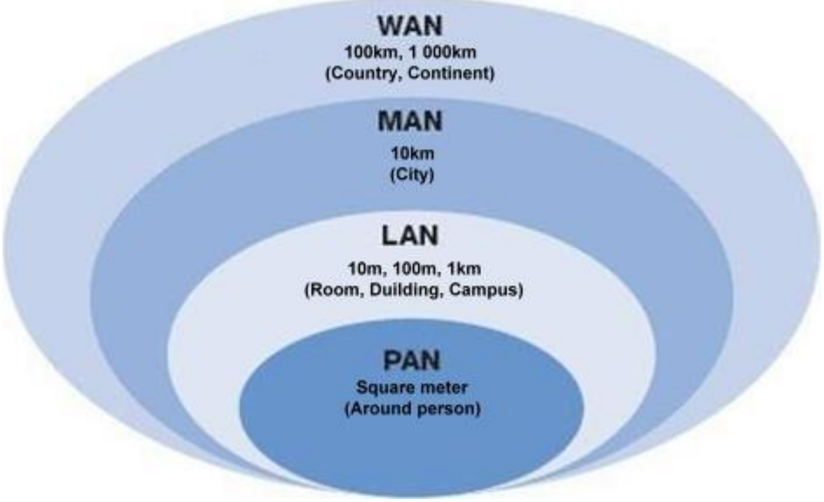
Metropolitan Area Network (MAN) - Covers a larger geographical area than is a LAN, ranging from several blocks of buildings to entire cities. A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations. They will often provide means for internetworking of LANs. Metropolitan Area Networks can span up to 50km, devices used are modem and wire/cable. It can be means to connecting a number of LANs into a larger network or it can be a single cable.



Wide Area Networks (WAN) - Computer network that covers a large geographical area, often a country or continent. (any network whose communications links cross metropolitan, regional, or national boundaries). Less formally, a network that uses routers and public communications links. WAN can be private or it can be public leased network. It is not easy to design and maintain. Communication medium used by WAN are PSTN or Satellite links



Subnet : The collection of communication lines and router is called subnet.



Topology (Physical topology):

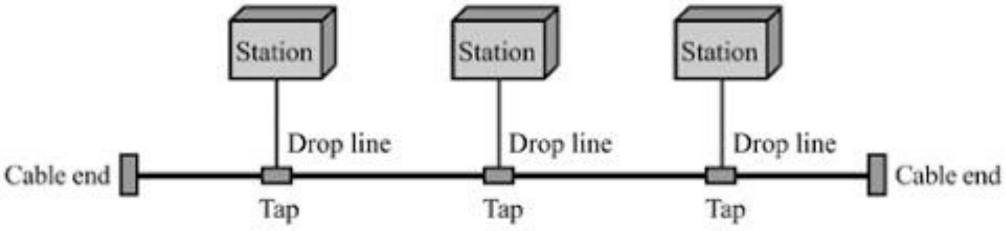
A topology is a way in which a network is arranged physically.

The topology of a network is a geometric representation of the relationship of all the links and linking devices(nodes) to one another.

There are 5 basic topologies :

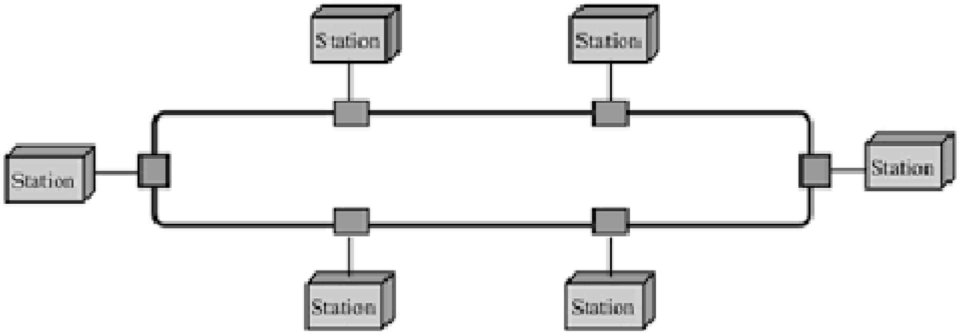
1) Bus 2) Ring 3) Star 4) Mesh 5)Hybrid

1) Bus Topology



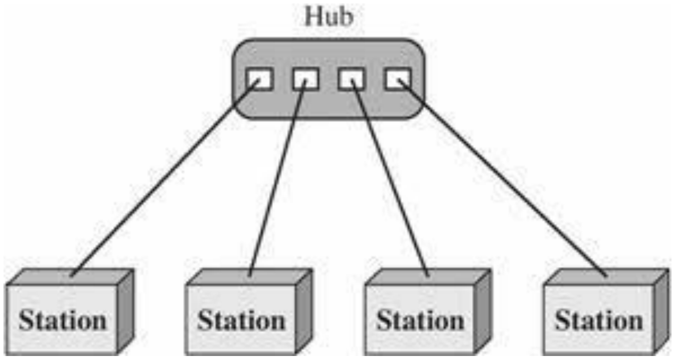
- Bus topology is multipoint connection.
- One long cable acts as backbone and links all the devices in the network.
- Each device is connected to the Bus cable using a drop line and tap.
  - A drop line is a connection between device and Bus cable.
  - A tap is a connector that splices or punctures the Bus cable to make the connection with the device.
- As the signal travels on the bus, it generates heat and becomes weaker. Hence there is a limitation on number of taps and distance between the taps.
- **Application:** Bus topology is used in early Ethernet LAN's
- **Advantages:**
  - Easy to install as only one single Bus cable is required to connect all devices. Hence less cabling is needed.
- **Dis-advantages:**
  - If the bus breaks or has a fault, then the entire data transmission is stopped.
  - Difficult to reconnect, detect fault and add new devices.
  - The signal quality degrades as it travels on the bus due to reflection at each tap.
  - The damaged part of the bus creates lot of noise.

2) Ring Topology:



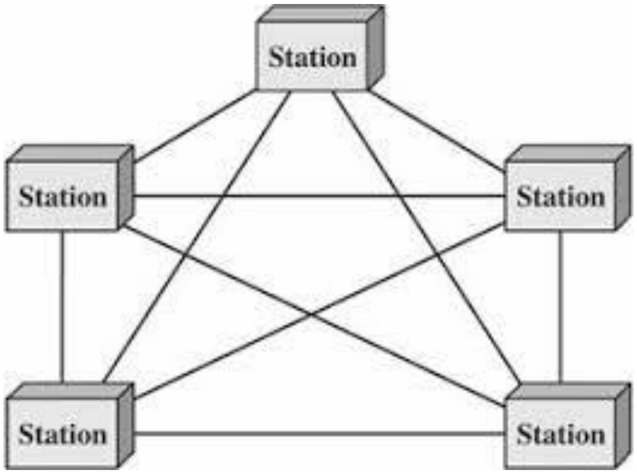
- In a ring topology, each device has a dedicated point-to-point connection with only the two devices on its either side.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination.
- **Application:** used in LAN's
- **Advantages:**
  - Easy to install and reconfigure
  - Adding or deleting a devices needs to change only two neighbouring connections.
- **Dis-advanatges:**
  - A break in the ring can disable the entire network.

3) Star Topology:



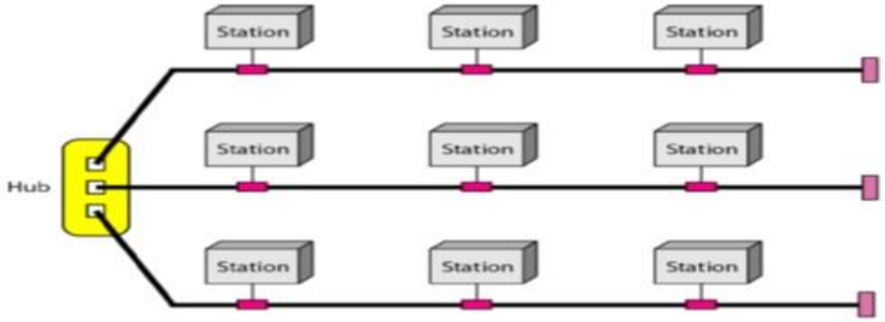
- In star topology, each device has a dedicated point to point link **only to a central controller** called as **Hub**.
- The devices are **not directly linked** to each other.
- The **hub** acts as an **exchange of data traffic** between the devices. It relays the data from one device to another.
- **Application:** It is used in LAN
- **Advantages:**
  - Less expensive than mesh
  - Number of I/O ports required is less (one I/O port for each device).
  - easy to install and reconfigure
  - Robust
  - Easy fault detection and isolation.
- **Dis-advantages:**
  - If hub fails, the entire network becomes dead.
  - compared to ring and bus , more cabling is needed

4) Mesh topology:



- In mesh topology **every device has a dedicated point to point link** with every other device.
- In a mesh with n nodes (devices) , the number of links required is given by **n (n-1) / 2**
- Hence every device must have (n-1) Input – output ports to connect to all other (n-1) devices.
- **Application :** mesh is used as a backbone n/w to connect one regional telephone office to another.
- **Advantages :**
  - Less traffic in the network
  - Robust.
  - private and secure
  - Fault detection and isolation is easy.
- **Dis-advantages :**
  - Lot of cabling and I/O ports are required
  - Installation and reconnection is difficult.
  - Network hardware can be expensive.

5) Hybrid : We have two different topologies in a single network. example star as a backbone and three buses as branches together.



PROTOCOLS

- **Protocol is a set of rules that govern the data communication**. It defines what is communicated, how and when it is communicated.
- The key elements of a protocol are:
    - **Syntax**: It is the structure (format) and order of data in which it is presented.
    - **Semantics**: It defines how a bit pattern is interpreted and what action is to be taken based on it.
    - **Timing:** It defines when the data has to be sent and how fast it has to be sent.

STANDARDS

- Standards are necessary to **create and maintain** an **open and competitive market** for equipment manufacturers.
- Standards allow national and international data and telecommunications **technology and processes to interoperate**.
- Standards **provide guidelines** to manufacturers, vendors, government agencies, and other service providers **about the kind of interconnectivity that is required in today's marketplace** and in international communications.
- There are 2 types of data communication standards
  a) De Jure : standards which are legislated by an officially recognized body.
  b) De Facto : Standards which are defined by manufacturers to define the functionality of their new product or technology.
- Standards are created by standard creation committees, forums and government regulatory agencies.
- **Standard creation committees** are procedural bodies. examples include ISO (International Organization for Standardization), ANSI(American National Standards Institute) , ITU-T (International Telecommunication Union – Telecommunication), IEEE (Institute of Electrical and Electronics Engineers) and EIA (Electronic Industries Association).
- **Forums** are made up of representatives from interested corporations who work with universities and users to test, evaluate, and standardize new technologies and present their conclusions to the standards bodies.
- **Regulatory Agencies:** They protect the public interest by regulating radio, television, and wire/cable communications.
- **Internet Standards:** It is a strict formal regulation that is followed by all those who work with the internet. It starts as an Internet Draft for 6 months and then it is published to attain an RFC (request for comment).

NETWORK MODELS

A network is a combination of hardware and software that sends data from one location to another. The hardware consists of physical equipment that carries signals and software consists of instruction sets that make possible the network services.

An open system is a set of protocols that allows any two different systems to communicate despite of their underlying architecture.

THE OSI (Open System Interconnection) MODEL

The OSI model was developed by **ISO** (International Standards Organization) which covered all the aspects of network communication.

The purpose of OSI model is to facilitate communication between different systems without changing the logic of the underlying hardware and software.

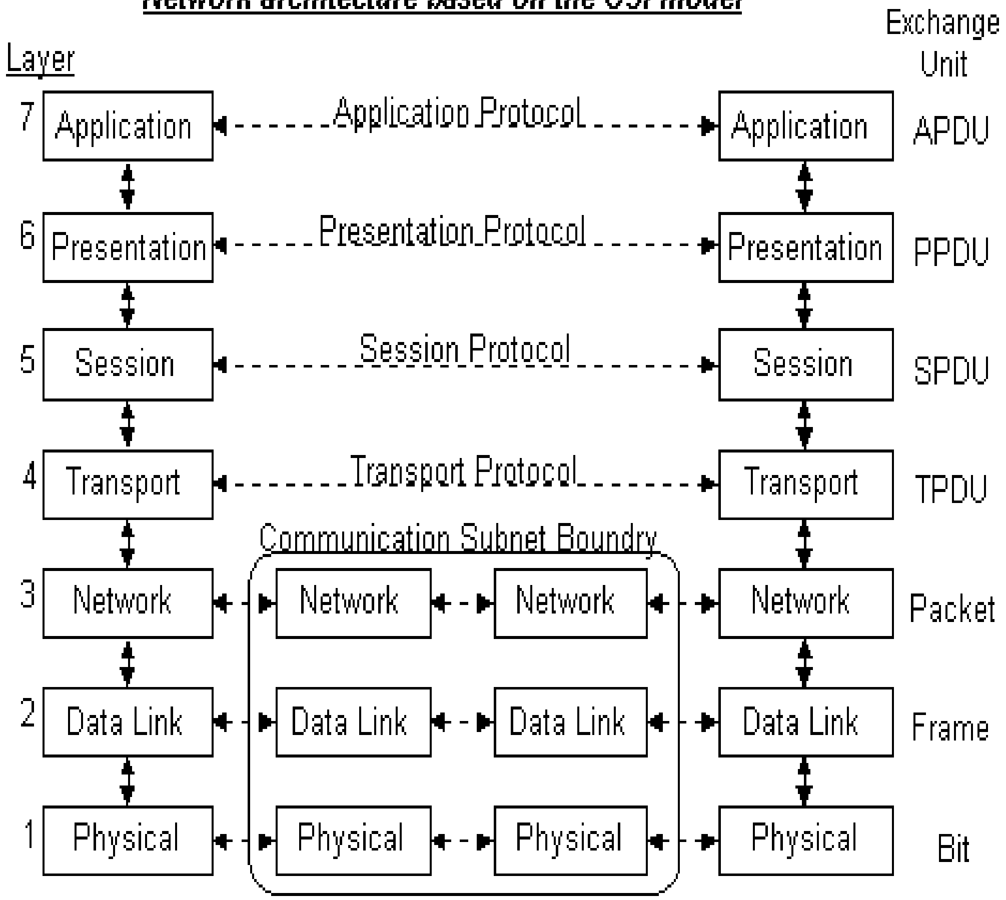
OSI model is used to design a network architecture that is comprehensive, flexible, robust and interoperable.

OSI is a **seven layered framework** where in each layer defines a part of the process of moving information across the network. Each layer provides services to the layer above it and uses the services of the layer below it.

Communication between machines is carried out by **peer-to-peer processes** using the protocols appropriate to a given layer.

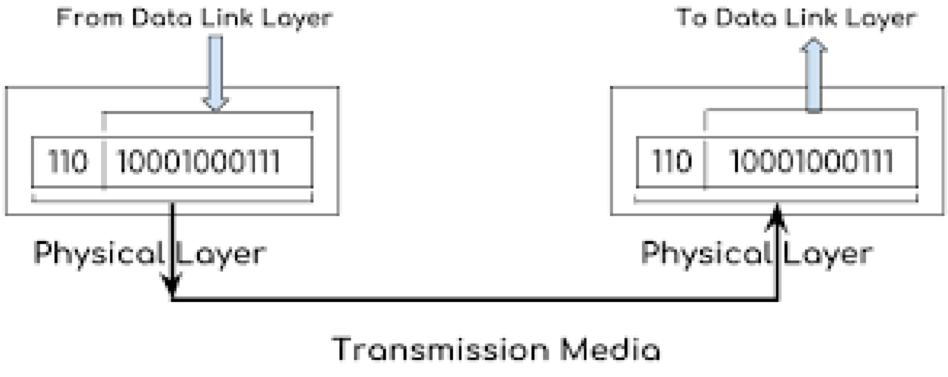
Interfaces between the adjacent pair of layers are used to pass the data and network information down and up the layers. Interfaces and layers provide modularity to a network.

Network architecture based on the OSI model



LAYERS IN OSI MODEL

1) PHYSICAL LAYER:

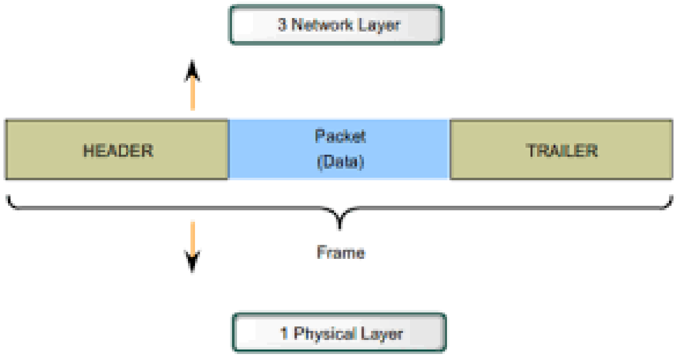


The physical layer is responsible for movements of individual bits from one hop (node) to the next.

- The physical layer is **responsible for movement of data bits from one hop (node / device) to another.**
- It **defines and co-ordinates the functions of physical devices** to carry the bit stream (data bits) over the physical medium.
- It deals with the **mechanical and electrical specifications** of the interface and transmission medium.
- **The main functions of physical layer are:**
  - Define the **physical characteristics of interfaces** between devices. Also define characteristics and type of transmission medium.
  - Representation of bits:-defines the **type of signal encoding** of bits.
  - Defines the **data Rate** of the bits
  - Specifies the **clock synchronization** of sender and receiver.
  - It specifies whether the **line configuration of the devices** is point-topoint or multipoint.
  - It specifies the **physical topology** of the devices to form the network.
  - Example: mesh, star, bus, ring, hybrid.
  - It defines the direction of transmission (**transmission mode**) between two devices. Example: simplex, half duplex , full duplex.

2) DATA LINK LAYER:

- **Framing** : The data link layer divides the stream of bits received from the network layer into data units called frames.



- **Physical addressing :** The data link layer adds a header to the frame to define the sender and receiver of the frame. If the receiver system is outside the sender's network, the receiver address is the address of the device that connects the network to the next one.
- **Flow control** : The data link layer imposes a flow control mechanism to avoid overwhelming the receiver during data transmission.

- **Error control** : The data link layer consist of mechanism to detect and retransmit damaged or lost frames. It also recognizes duplicate frames. Error control is achieved by adding a trailer to end of the frame.
- **Access control** : The data link layer protocols determine which device has control over the link at any given time in a multipoint connection.

3) NETWORK LAYER :

- The network layer is responsible for the delivery of individual packets from the source host to the destination host usually across multiple networks (links).
- Other responsibilities of the network layer include the following:
  - **Logical addressing** : the network layer provides an addressing system to help distinguish the source and destination when a packet is to be transmitted from one network to another. It adds the logical address of sender and receiver to the header of the packet coming from the upper layer.
  - **Routing** : the network layer provides a mechanism where in the connecting devices (called *routers* or *switches)* route or switch the packets to their final destination.

4) TRANSPORT LAYER :

- The transport layer is responsible for the end to end delivery of the entire message.
- It ensures that the message arrives intact and in-order.
- Other responsibilities of the transport layer include the following:
  - **Service-point addressing** : The transport layer header includes the *service-point address* (or port address). The transport layer gets the entire message to the correct process running on the destination computer.
  - **Segmentation and reassembly** :The transport layer divides a message into transmittable segments, wherein each segment contains a sequence number. These numbers are used to reassemble the message correctly at destination and to identify and replace packets if they are lost in transmission.
  - **Connection control** : The transport layer is either connectionless or connection oriented.
    - ✓ A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine.
    - ✓ A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.
  - **Flow control** :The transport layer is responsible for end to end flow control.
  - **Error control** : the transport layer is responsible for process-to process error control. The sending transport layer makes sure that the entire message reaches

the receiving transport layer without error (damage, loss, or duplication). Further the Error correction is achieved through retransmission.

5) SESSION LAYER:

- The session layer is responsible for dialog control and synchronization.
- It establishes, maintains and synchronizes the interaction between devices that communicate.
- Other specific responsibilities of session layer are:
  - **Dialog control** : The session layer allows two devices to communicate either in a half or full duplex mode.
  - **Synchronization** : Checkpoints or synchronization points are added to a stream of data to ensure that every data unit is received and acknowledged independently. Therefore in case the network crashes, only the data units after the checkpoint need to be resent.

6) PRESENTATION LAYER:

- The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.
- Other specific tasks are:
  - **Translation** : The presentation layer allows systems with different encoding methods to interoperate. 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 ensure privacy the sensitive information is encrypted and resulting message is sent out over the network. At the receiver, the message is decrypted back to its original form.
  - **Compression** : Data compression is performed to reduce the number of bits contained in the information. This is done specifically for multimedia such as text, audio, and video.

7) APPLICATION LAYER :

- 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.
- Specific services provided by application layer are:
  - **Network virtual terminal** : A network virtual terminal allows a user to log on to a remote host by creating 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, retrieve files and to manage or control files in a remote computer locally.
- **Mail services** : It provides the basis for e-mail forwarding and storage.
- **Directory services** : It provides distributed databases and access for global information about various objects and services.

Transmission Control Protocol/Internet Protocol (TCP/IP) Reference Model

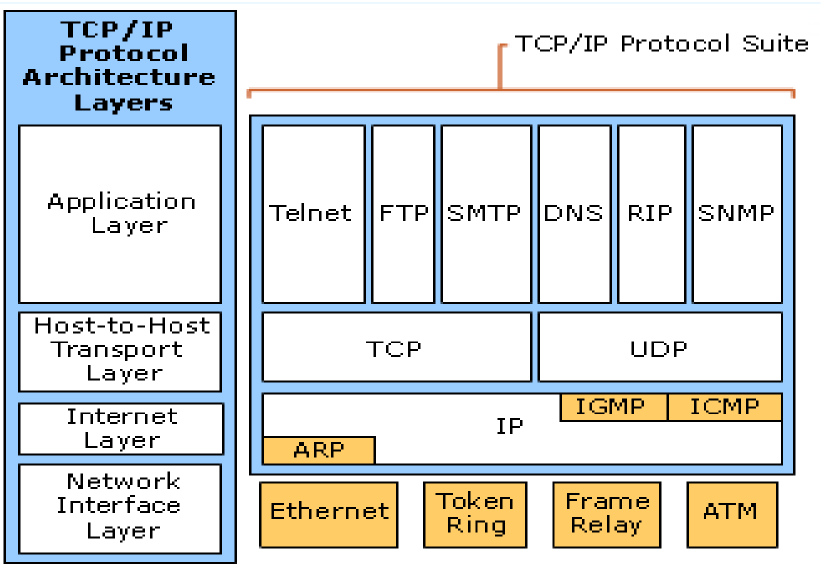
This protocol suite is the engine for the Internet and networks worldwide. Its simplicity and power has led to its becoming the single network protocol of choice in the world today. TCP/IP is a set of protocols developed to allow cooperating computers to share resources across the network. TCP/IP model has the ability to interconnect multiple networks of different architecture.

This model was initially developed& used by ARPANET (Advanced Research Project Agency Network). ARPANET was a community of researchers sponsored by the U.S. department of defense. It connects many universities and government installations using leased telephone lines . Certainly the ARPANET is the best- known TCP/IP network.

The most accurate name for the set of protocols is the "Internet protocol suite". TCP and IP are two of the protocols in this suite. The Internet is a collection of networks. Term "Internet" applies to this entire set of networks. Like most networking software, TCP/IP is modeled in layers.

TCP / IP PROTOCOL SUITE

- The TCP/IP protocol suite is made of four layers:
  1) Network interface layer
  2) Internet layer
  3) Transport layer
  4) Application layer
- TCP/IP is a hierarchical protocol made up of interactive modules, wherein each module provides a specific functionality.



1) NETWORK INTERFACE LAYER (physical and data link layer) :

- At these Layers TCP/IP does not define any specific protocol and supports all standard and propriety protocols.
- The network access layer, also known as the data link layer, **handles the physical infrastructure** that lets computers communicate with one another over the internet. This covers ethernet cables, wireless networks, network interface cards, device drivers in your computer, and so on.

2) INTERNET LAYER:

- The internet layer, also known as the network layer, **controls the flow and routing of traffic** to ensure data is sent speedily and accurately. This layer is also responsible for reassembling the data packet at its destination.
- The network layer supports the Internetworking protocol (IP) which in turn makes use of 4 other protocols called ARP, RARP, ICMP and IGMP.
- **IP protocol :**
  - ➢ It is a transmission mechanism used by TCP/IP
  - ➢ It is unreliable and connectionless because it does not perform error tracking and checking. Hence it is also called as Best-effort delivery service as it only concentrates on delivering the messages to its destination.
  - ➢ IP transports data in packets called datagrams on separate routes but does not take care of out of order (sequence) packets and duplicate packets.
- **ARP (Address Resolution Protocol):**
  - ➢ ARP is used to associate or find the physical (station) address of a device when its logical address is known.
  - ➢ The physical address of a device is the one imprinted on its NIC card.

- **RARP(Reverse Address Resolution Protocol):**
  - It is used to discover the logical(internet) address of a host (device) when its physical address is known.
  - RARP is used when a computer is connected to a network for the first time or when a diskless computer is booted.
- **ICMP (Internet Control message protocol):**
  - It is a mechanism used by host computers and gateways to send notifications back to the sender about the datagram problems.
  - It sends query and error reporting messages.
- **IGMP (Internet Group Message Protocol):**
  - It is used for transmission of a message simultaneously to a group of recipients.

3) TRANSPORT LAYER:

- Transport layer is responsible for end to end delivery of data packets.
- Transport layer is represented by two protocols: TCP and UDP which help in process to process delivery of messages.
- **UDP (User Datagram Protocol):**
  - It is a process-to-process protocol that adds source and destination port addresses, error control checksum and length information to the data from the upper layer. The self-contained data frame is known as **datagram**.
  - UDP is unreliable connectionless transport protocol.
- **TCP (transmission Control Protocol):**
  - TCP is a reliable connection oriented transport protocol.
  - A connection is established between the sender and receiver before transmitting data.
  - At sender side, the stream of data is divided into smaller units called segments. Each segment has a sequence number for reordering and an acknowledgement number.
  - These segments are transmitted inside the IP datagrams.
  - At receiver side, the TCP collects these datagrams as they come in and then reorders them based on their sequence numbers.

4) APPLICATION LAYER:

- Various application layer protocols are SMTP, FTP, Telnet, HTTP, DNS, SNMP etc. and these protocols mainly work on client server model.
- This layer allows the user to interact with the application.
- **SMTP (Simple Mail transfer Protocol) :**
  - It provides electronic mail service between users on the internet.
  - It provides mail exchange using email addresses.

- SMTP connections are secured with SSL (Secure Socket Layer).

- **FTP(File Transfer Protocol):**
  - It is used to copy a file from one host to another in a network.
  - FTP establishes 2 types of connections between hosts namely data connection and control connection.
  - Data connection transfers data by using port 20 and control connection transfers commands & responses using port 21.
- **HTTP(HyperText Transfer Protocol):**
  - It is mainly used to access data on the worldwide web.
  - It can transfer text, hypertext, audio, video etc.
- **Telnet :**
  - It provides a bi-directional text oriented communication service by using **virtual terminal connection (remote login).**
  - It is based on a reliable connection- oriented transport.
- **DNS (Domain Name System):**
  - DNS is a hierarchical system that uses a hierarchy of name servers to resolve internet host names (domain names) to their corresponding IP addresses.
- **SNMP (Simple Network Management Protocol):**
  - SNMP allows monitoring and management of network devices such as servers, workstations, printers, routers, bridges, and hubs, as well as services such as **Dynamic Host Configuration Protocol** (**DHCP**) or **Windows Internet Name Service** (WINS).
- **DHCP(Dynamic Host Configuration Protocol**):
  - It is used for dynamically assigning IP addresses to computers in a network.
  - Every time a computer connects to a network it will have a different IP address.

Comparison of OSI Reference Model and TCP/IP Reference Model

Following are some major differences between OSI Reference Model and TCP/IP Reference Model, with diagrammatic comparison below.

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	2. In TCP/IP model the transport layer does not

guarantees the delivery of packets.	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. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	5. TCP/IP model is, in a way implementation of the OSI model.
6. Network layer of OSI model provides both connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.
7. OSI model has a problem of fitting the protocols into the model.	7. TCP/IP model does not fit any protocol
8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.
9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	9. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
10. It has 7 layers	10. It has 4 layers