Computer Networks

Syllabus

- OSI reference model , TCP/IP reference model
- Classification of networks
- Network topologies : Bus, Ring, Star, Mesh, Hybrid
- LAN components – Coaxial, twisted pair, optical fiber cables.
- connectors – repeaters, hubs, switches, NIC
- Ethernet, token bus, token ring, inter network packet exchange/sequenced packet exchange
- HTTP, FTP, SMTP, Telnet – TCP/IP addressing scheme – IP address classes - sub netting

DATA COMMUNICATIONS

The term telecommunication means communication at a distance. The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data.

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

Figure *Components of a data communication system*

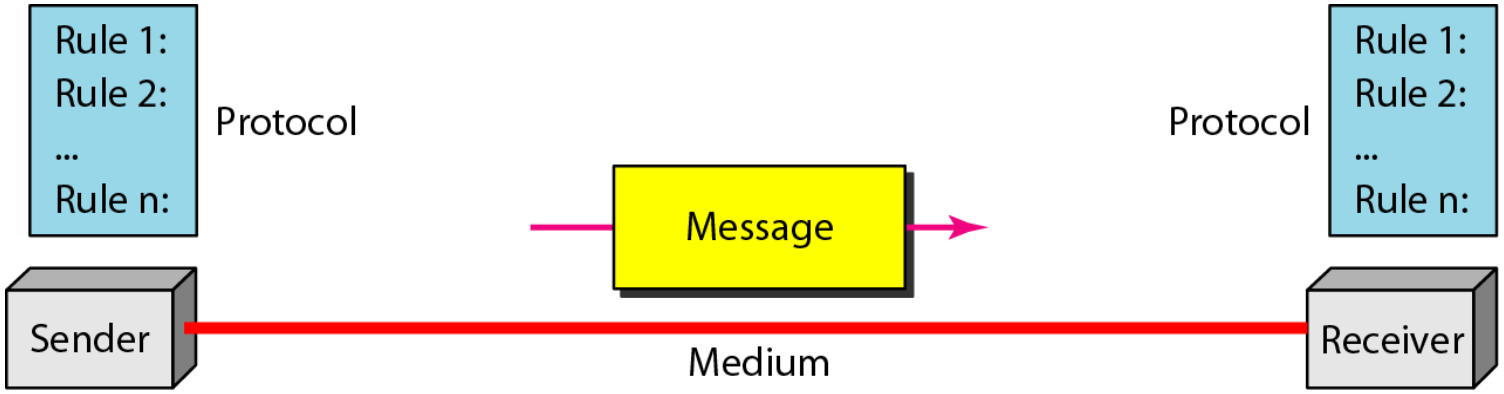
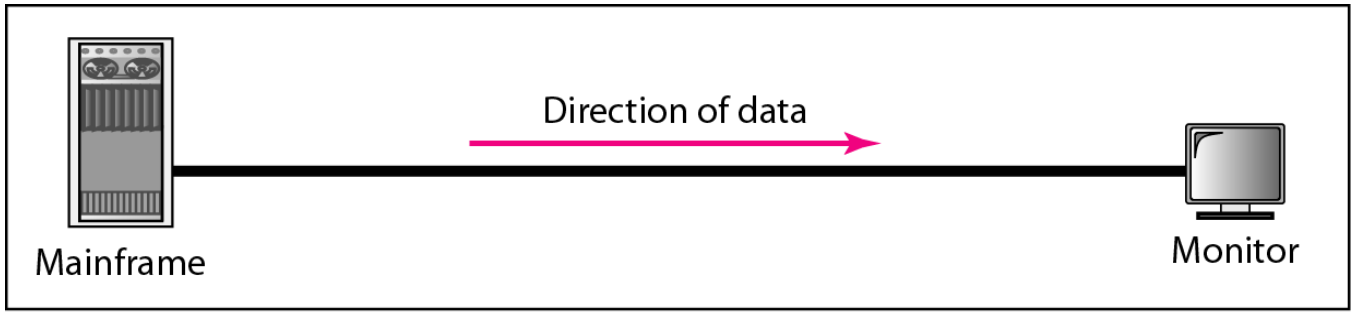
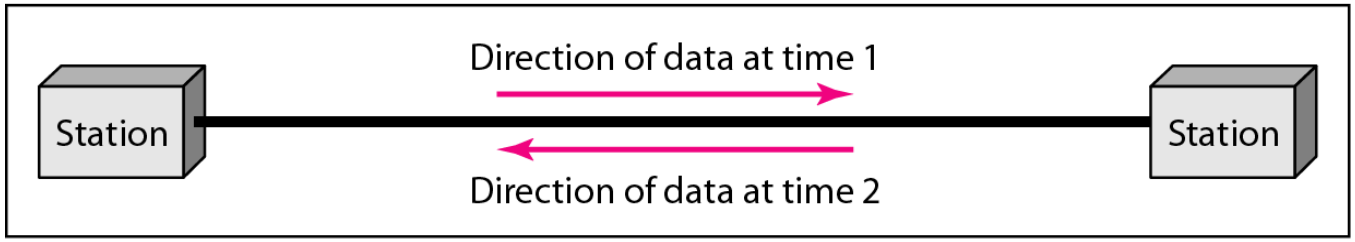


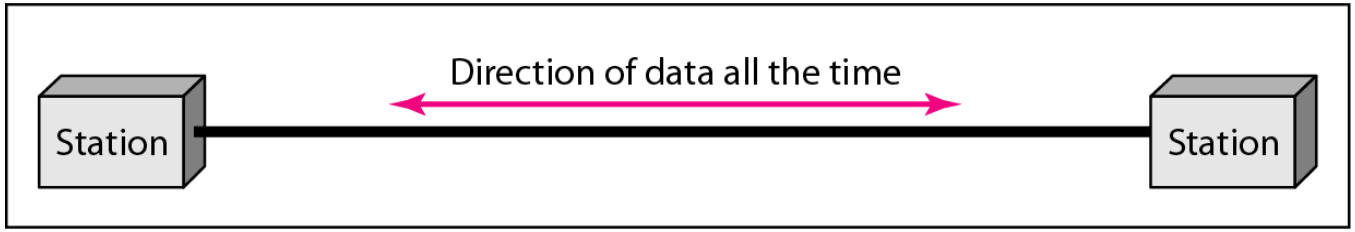
Figure *Data flow (simplex, half-duplex, and full-duplex)*



a. Simplex



b. Half-duplex



c. Full-duplex

NETWORKS

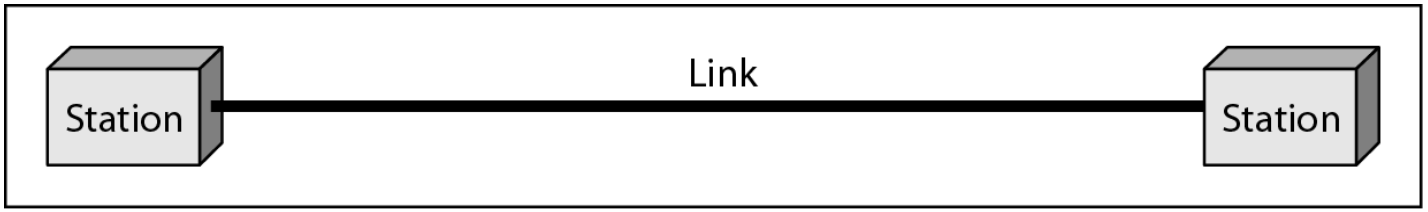
A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network. A link can be a cable, air, optical fiber, or any medium which can transport a signal carrying information.

A computer network is a group of two or more interconnected computer systems. You can establish a network connection using either cable or wireless media.

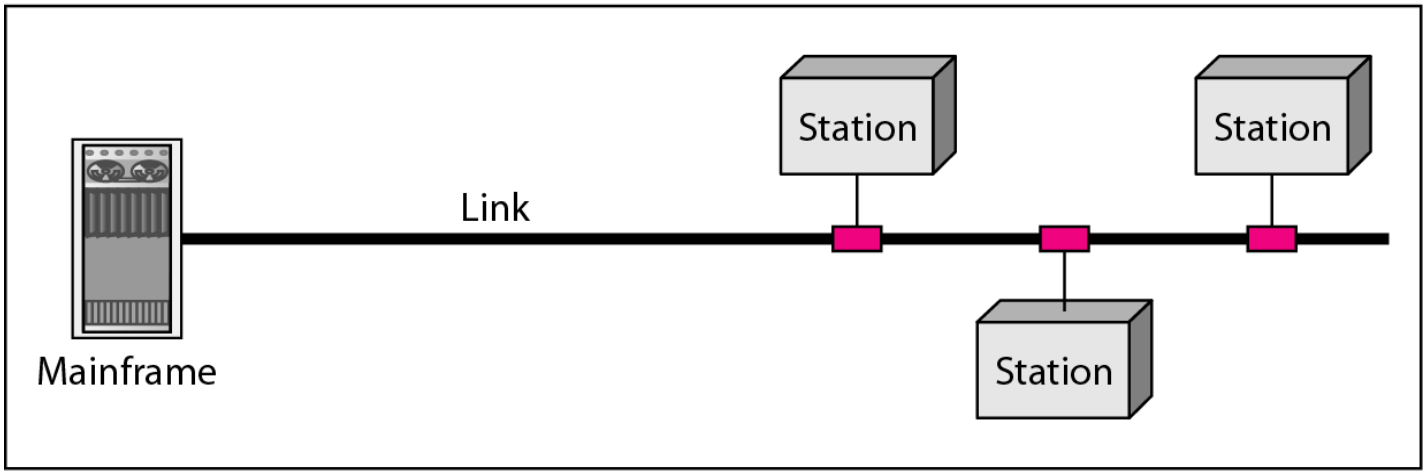
- **Performance**
  - **Depends on Network Elements**
  - **Measured in terms of Delay and Throughput**
- **Reliability**
  - **Failure rate of network components**
  - **Measured in terms of availability/robustness**
- **Security**
  - **Data protection against corruption/loss of data due to:**
    - **Errors**
    - **Malicious users**

- **Type of Connection**
  - **Point to Point - single transmitter and receiver**
  - **Multipoint - multiple recipients of single transmission**
- **Physical Topology**
  - **Connection of devices**
  - **Type of transmission - unicast, mulitcast, broadcast**

Types of connections: point-to-point and multipoint

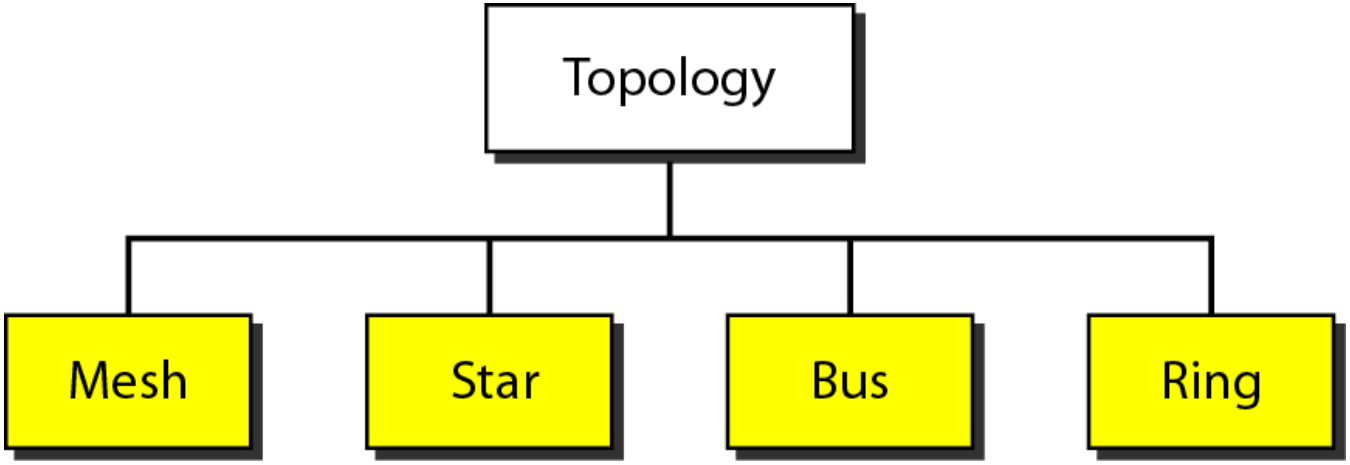


a. Point-to-point

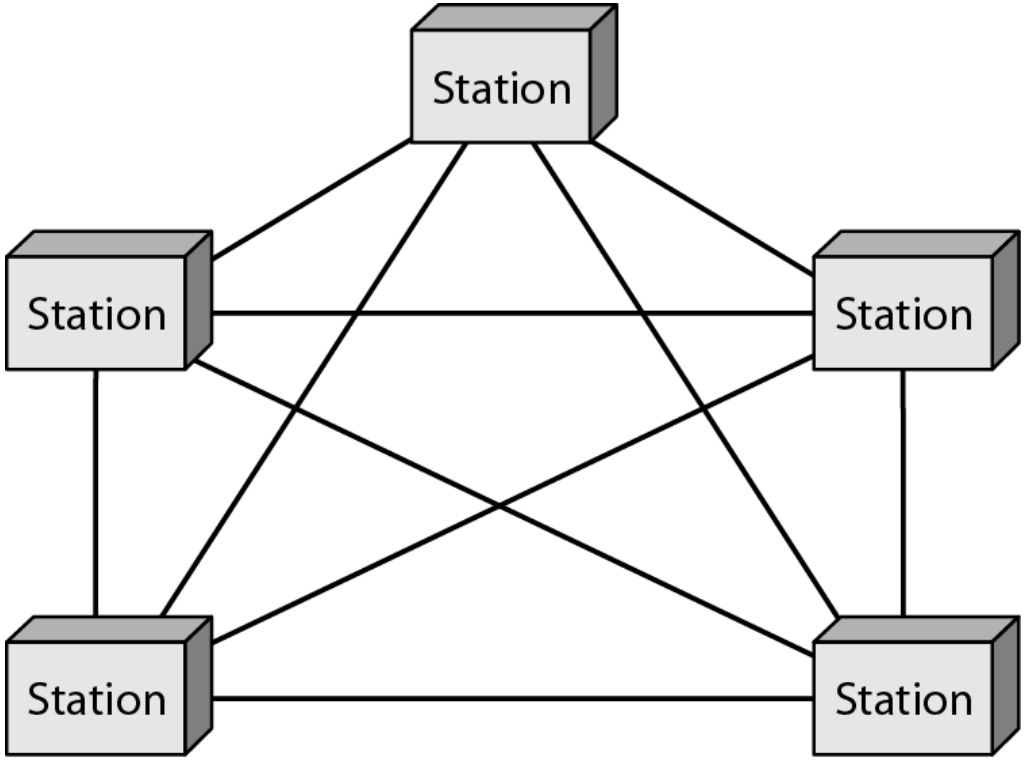


b. Multipoint

Categories of topology



A fully connected mesh topology (five devices)



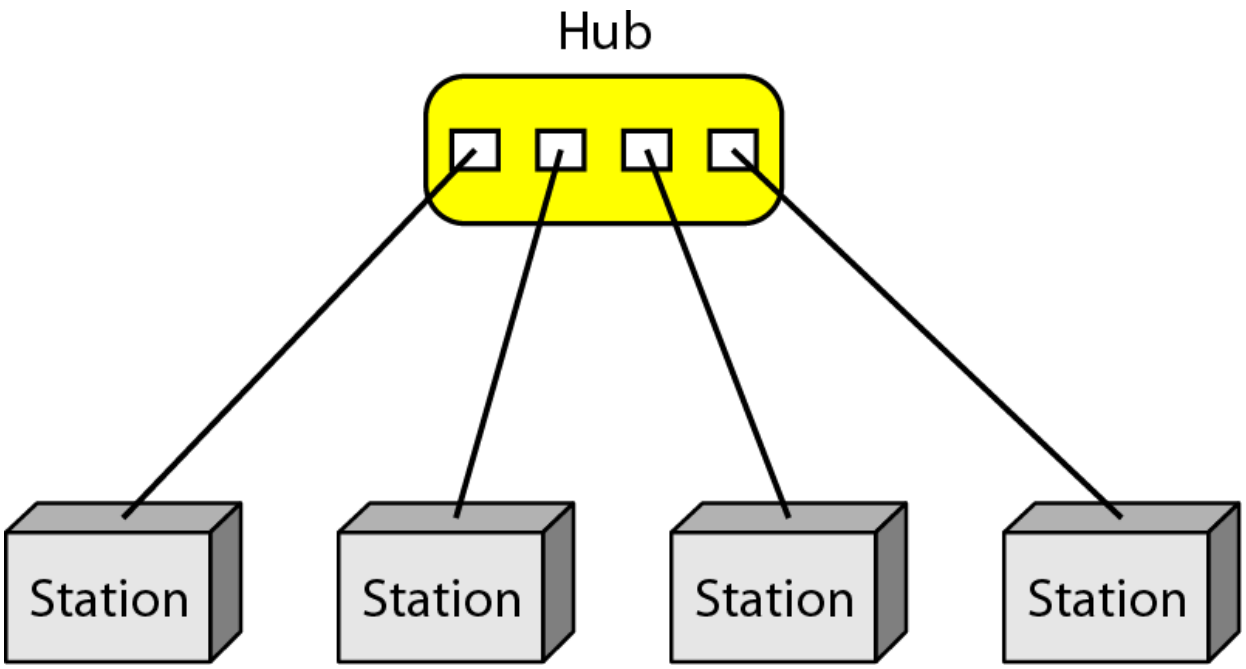
Advantages:

- The network can be expanded without disrupting current users.
- Need extra capable compared with other LAN topologies.
- No traffic problem as nodes has dedicated links.
- Dedicated links help you to eliminate the traffic problem.
- A mesh topology is robust.
- It has multiple links, so if any single route is blocked, then other routes should be used for data communication.
- P2P links make the fault identification isolation process easy.
- It helps you to avoid the chances of network failure by connecting all the systems to a central node.
- Every system has its privacy and security.

Disadvantages:

- Installation is complex because every node is connected to every node.
- It is expensive due to the use of more cables. No proper utilization of systems.
- Complicated implementation.
- It requires more space for dedicated links.
- Because of the amount of cabling and the number of input-outputs, it is expensive to implement.
- It requires a large space to run the cables.

Figure 1.6 *A star topology connecting four stations*



- In the star topology, all the computers connect with the help of a hub. This cable is called a central node, and all other nodes are connected using this central node. It is most popular on LAN networks as they are inexpensive and easy to install.

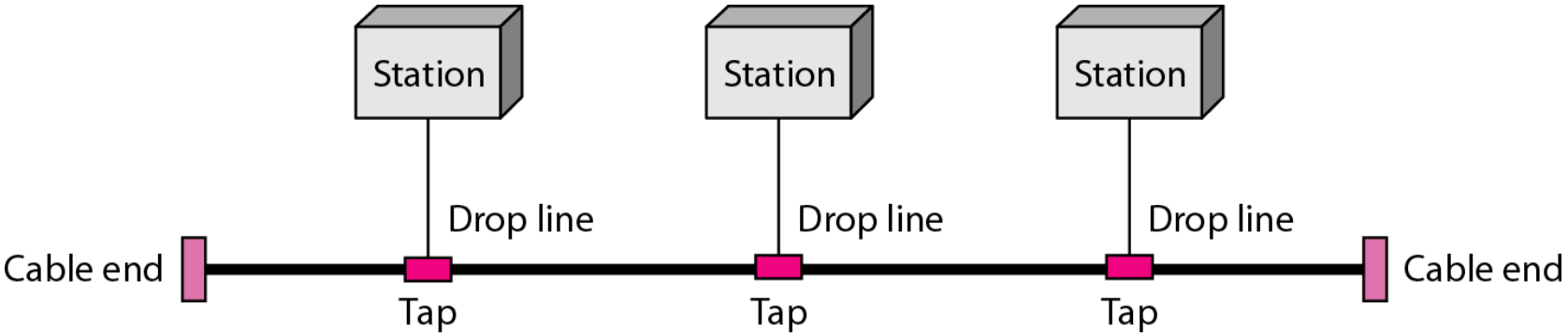
Advantages:

- Here are pros/benefits of start topology:
- Easy to troubleshoot, set up, and modify.
- Only those nodes are affected, that has failed. Other nodes still work.
- Fast performance with few nodes and very low network traffic.
- In Star topology, addition, deletion, and moving of the devices are easy.

Disadvantages:

- Here are cons/drawbacks of using Star:
- If the hub or concentrator fails, attached nodes are disabled.
- Cost of installation of star topology is costly.
- Heavy network traffic can sometimes slow the bus considerably.
- Performance depends on the hub's capacity
- A damaged cable or lack of proper termination may bring the network down.

Figure 1.7 *A bus topology connecting three stations*



- Bus topology uses a single cable which connects all the included nodes. The main cable acts as a spine for the entire network. One of the computers in the network acts as the computer server. When it has two endpoints, it is known as a linear bus topology.

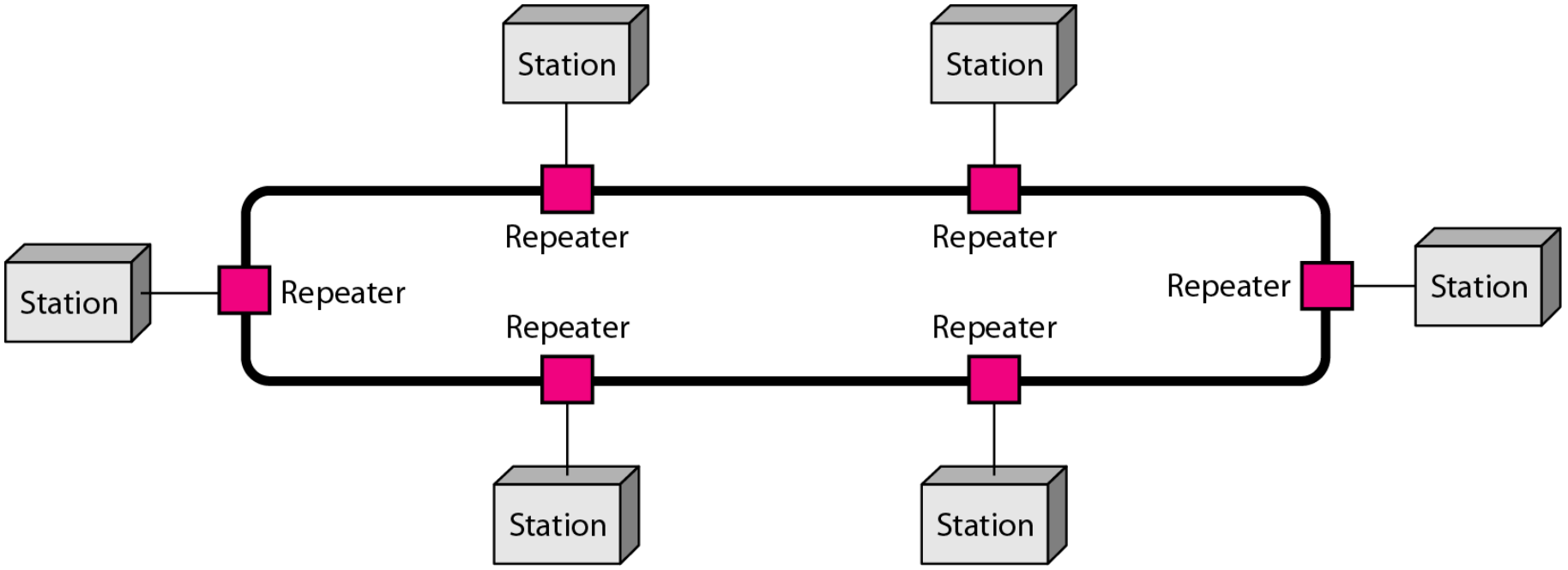
Advantages:

- Here are pros/benefits of using a bus topology:
- Cost of the cable is very less as compared to other topology, so it is widely used to build small networks.
- Famous for LAN network because they are inexpensive and easy to install.
- It is widely used when a network installation is small, simple, or temporary.
- It is one of the passive topologies. So computers on the bus only listen for data being sent, that are not responsible for moving the data from one computer to others.

Disadvantages:

- Here are the cons/drawbacks of bus topology:
- In case if the common cable fails, then the entire system will crash down.
- When network traffic is heavy, it develops collisions in the network.
- Whenever network traffic is heavy, or nodes are too many, the performance time of the network significantly decreases.
- Cables are always of a limited length.

Figure 1.8 *A ring topology connecting six stations*



- In a ring network, every device has exactly two neighboring devices for communication purpose. It is called a ring topology as its formation is like a ring. In this topology, every computer is connected to another computer. Here, the last node is combined with a first one.
- This topology uses token to pass the information from one computer to another. In this topology, all the messages travel through a ring in the same direction.

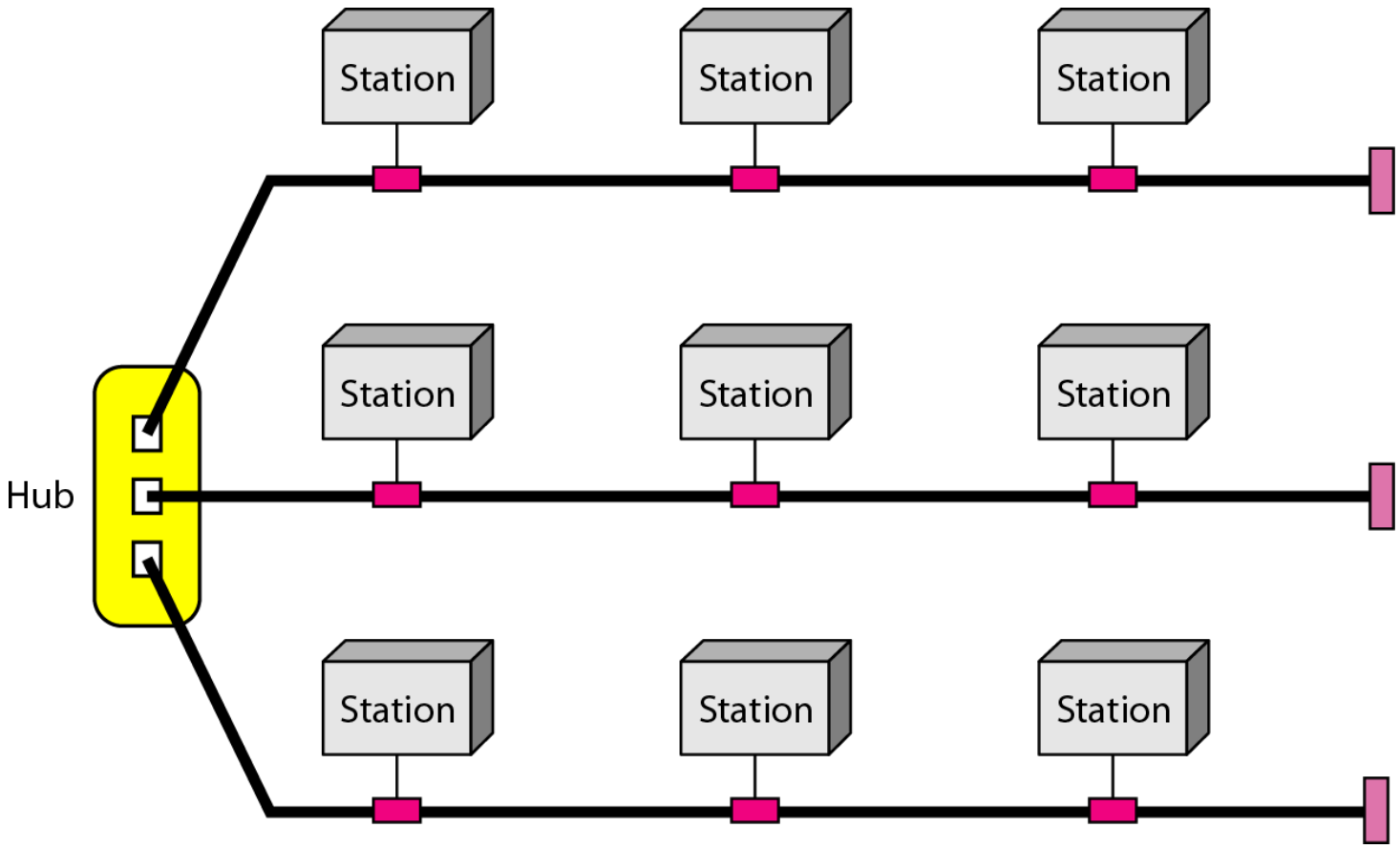
Advantages:

- Here are pros/benefits of ring topology:
- Easy to install and reconfigure.
- Adding or deleting a device in-ring topology needs you to move only two connections.
- The troubleshooting process is difficult in a ring topology.
- Failure of one computer can disturb the whole network.
- Offers equal access to all the computers of the networks
- Faster error checking and acknowledgment.

Disadvantages:

- Here are drawbacks/cons of ring topology:
- Unidirectional traffic.
- Break in a single ring can risk the breaking of the entire network
- Modern days high-speed LANs made this topology less popular.
- In the ring, topology signals are circulating at all times, which develops unwanted power consumption.
- It is very difficult to troubleshoot the ring network.
- Adding or removing the computers can disturb the network activity.

Figure 1.9 *A hybrid topology: a star backbone with three bus networks*



Advantages:

- Here, are advantages/pros using Hybrid topology:
- Offers the easiest method for error detecting and troubleshooting
- Highly effective and flexible networking topology
- It is scalable so you can increase your network size

Disadvantages:

- The design of hybrid topology is complex
- It is one of the costliest processes

Categories of networks

- A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.
- A computer network can be categorized by their size. A **computer network** is mainly of **four types**:
- LAN(Local Area Network)
- PAN(Personal Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

LAN(Local Area Network)

A **Local Area Network** (LAN) is a group of computer and peripheral devices which are connected in a limited area such as school, laboratory, home, and office building.
It is a widely useful network for sharing resources like files, printers, games, and other application.
The simplest type of LAN network is to connect computers and a printer in someone's home or office. In general, LAN will be used as one type of transmission medium.
It is a network which consists of less than 5000 interconnected devices across several buildings.

Characteristics of LAN

- Here are the important characteristics of a LAN network:
- It is a private network, so an outside regulatory body never controls it.
- LAN operates at a relatively higher speed compared to other WAN systems.
- There are various kinds of media access control methods like token ring and ethernet.

Advantages of LAN

- Here are the pros/benefits of LAN:
- Computer resources like hard-disks, DVD-ROM, and printers can share local area networks. This significantly reduces the cost of hardware purchases.
- You can use the same software over the network instead of purchasing the licensed software for each client in the network.
- Data of all network users can be stored on a single hard disk of the server computer.
- You can easily transfer data and messages over networked computers.
- It will be easy to manage data at only one place, which makes data more secure.
- Local Area Network offers the facility to share a single internet connection among all the LAN users.

Disadvantages of LAN

- Here are the cons/drawbacks of LAN:
- LAN will indeed save cost because of shared computer resources, but the initial cost of installing Local Area Networks is quite high.
- The LAN admin can check personal data files of every LAN user, so it does not offer good privacy.
- Unauthorized users can access critical data of an organization in case LAN admin is not able to secure centralized data repository.
- Local Area Network requires a constant LAN administration as there are issues related to software setup and hardware failures

PAN(Personal Area Network)

- **PAN** (Personal Area Network) is a computer network formed around a person.
- It generally consists of a computer, mobile, or personal digital assistant.
- PAN can be used for establishing communication among these personal devices for connecting to a digital network and the internet.

Characteristics of PAN

- Below are the main characteristics of PAN:
- It is mostly personal devices network equipped within a limited area.
- Allows you to handle the interconnection of IT devices at the surrounding of a single user.
- PAN includes mobile devices, tablet, and laptop.
- It can be wirelessly connected to the internet called WPAN.
- Appliances use for PAN: cordless mice, keyboards, and Bluetooth systems.

Advantages of PAN

- Here are the important pros/benefits of PAN network:
- PAN networks are relatively secure and safe
- It offers only short-range solution up to ten meters
- Strictly restricted to a small area

Disadvantages of PAN

- Here are the cons/drawbacks of using PAN network:
- It may establish a bad connection to other networks at the same radio bands.
- Distance limits.

There are two types of Personal Area Network:

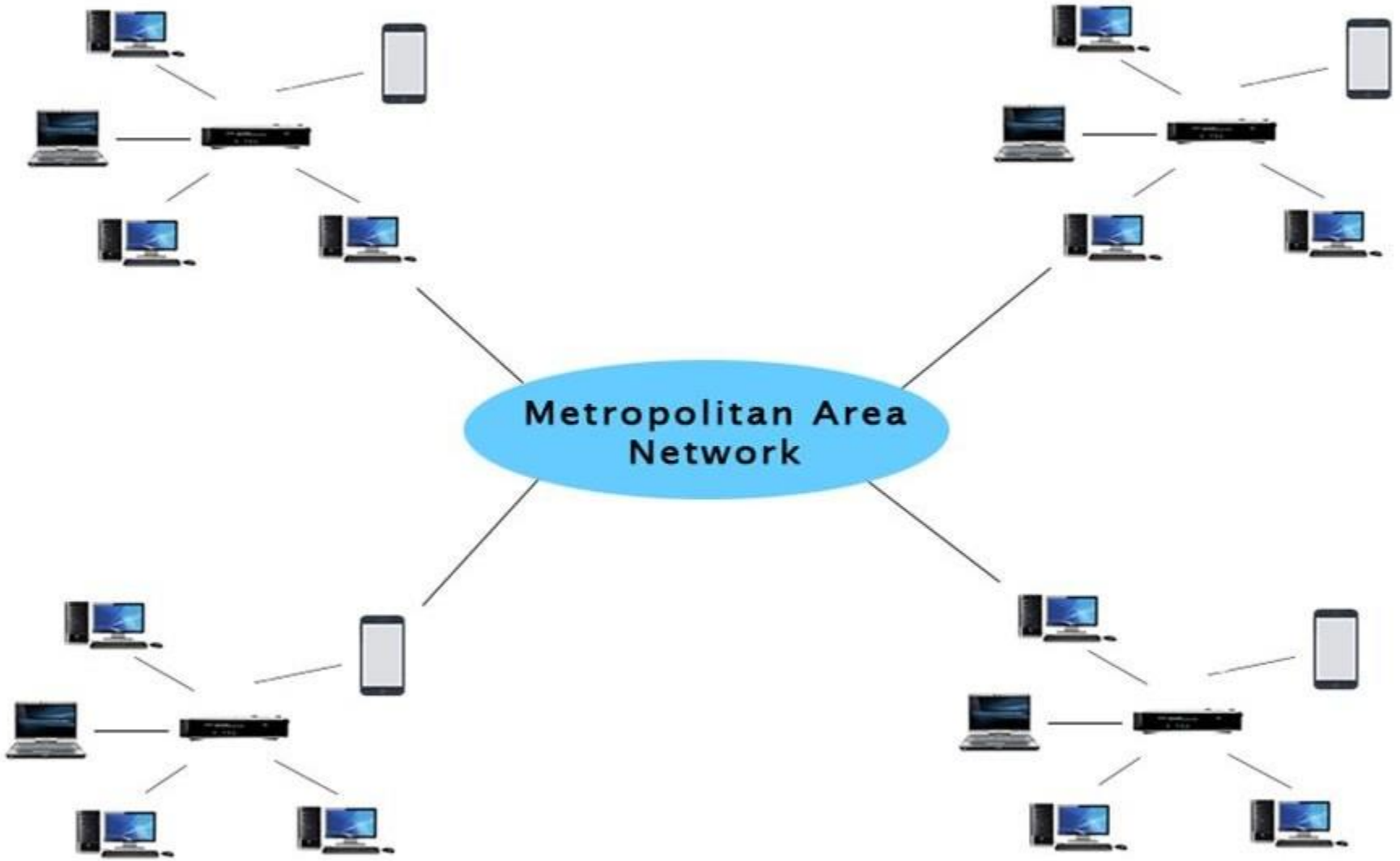
- Wired Personal Area Network
- Wireless Personal Area Network
- **Wireless Personal Area Network:** Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.
- **Wired Personal Area Network:** Wired Personal Area Network is created by using the USB.

Examples Of Personal Area Network:

- **Body Area Network:** Body Area Network is a network that moves with a person. **For example**, a mobile network moves with a person. Suppose a person establishes a network connection and then creates a connection with another device to share the information.
- **Offline Network:** An offline network can be created inside the home, so it is also known as a **home network**. A home network is designed to integrate the devices such as printers, computer, television but they are not connected to the internet.
- **Small Home Office:** It is used to connect a variety of devices to the internet and to a corporate network using a VPN

MAN(Metropolitan Area Network)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- It has a higher range than Local Area Network(LAN).


Metropolitan Area
Network

Uses Of Metropolitan Area Network

- 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.

Characteristics of MAN

- Here are important characteristics of the MAN network:
- It mostly covers towns and cities in a maximum 50 km range
- Mostly used medium is optical fibers, cables
- Data rates adequate for distributed computing applications.

Advantages of MAN

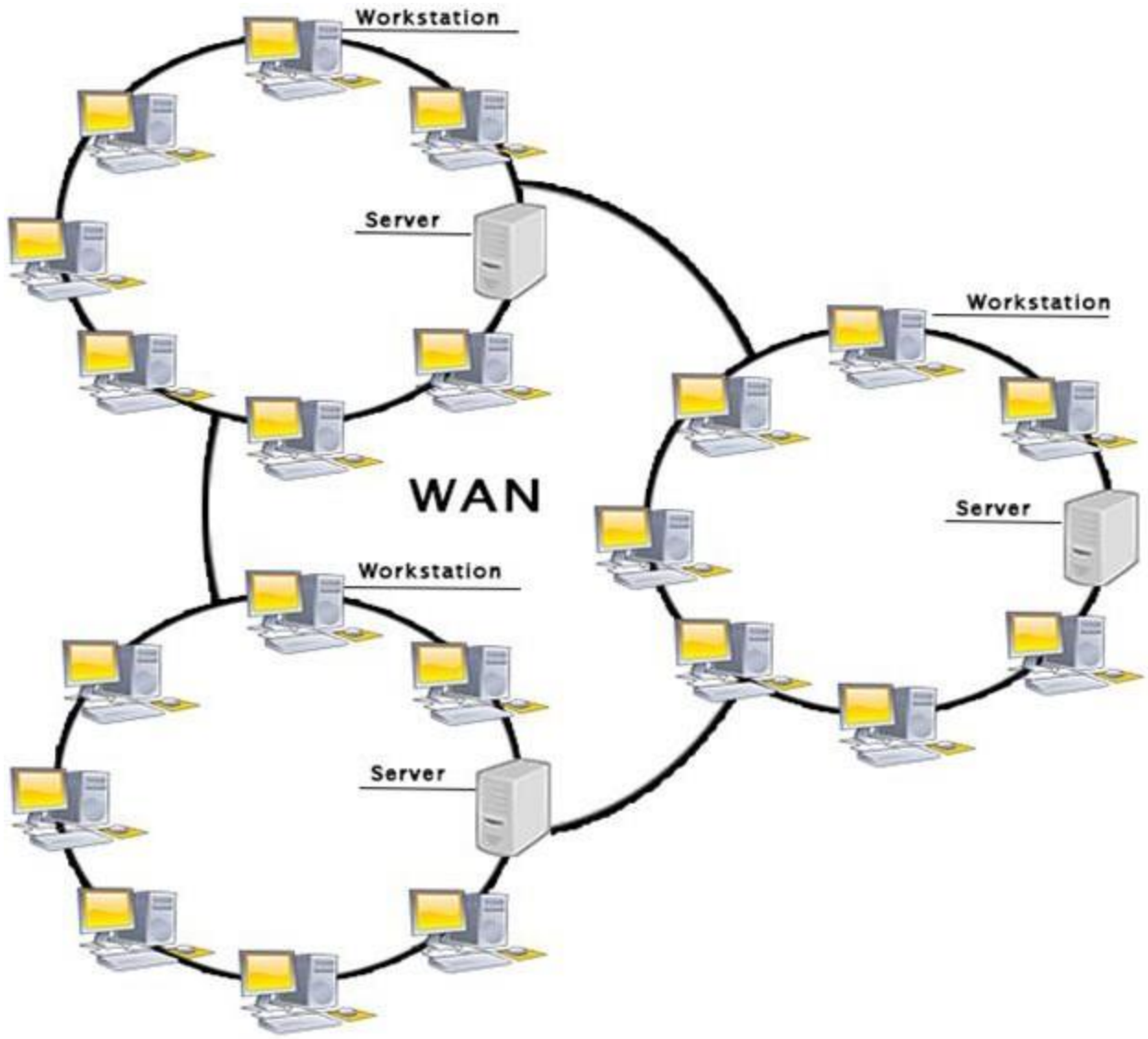
- Here are the pros/benefits of MAN network:
- It offers fast communication using high-speed carriers, like fiber optic cables.
- It provides excellent support for an extensive size network and greater access to WANs.
- The dual bus in MAN network provides support to transmit data in both directions concurrently.
- A MAN network mostly includes some areas of a city or an entire city.

Disadvantages of MAN

- Here are drawbacks/cons of using the MAN network:
- You need more cable to establish MAN connection from one place to another.
- In MAN network it is tough to make the system secure from hackers

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 LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre 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.


Workstation
Server
Workstation
WAN
Server
Workstation
Server

Examples Of Wide Area Network

- **Mobile Broadband:** A 4G network is widely used across a region or country.
- **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
- **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

Characteristics of WAN

- Below are the characteristics of WAN:
- The software files will be shared among all the users; therefore, all can access to the latest files.
- Any organization can form its global integrated network using WAN.

Advantages of WAN

- Here are the benefits/pros of WAN:
- WAN helps you to cover a larger geographical area. Therefore business offices situated at longer distances can easily communicate.
- Contains devices like mobile phones, laptop, tablet, computers, gaming consoles, etc.
- WLAN connections work using radio transmitters and receivers built into client devices.

Disadvantages of WAN

- Here are the drawbacks/cons of WAN network:
- The initial setup cost of investment is very high.
- It is difficult to maintain the WAN network. You need skilled technicians and network administrators.
- There are more errors and issues because of the wide coverage and the use of different technologies.
- It requires more time to resolve issues because of the involvement of multiple wired and wireless technologies.
- Offers lower security compared to other types of network in computer.

DISTINGUISH BETWEEN LAN,WAN,MAN

PARAMETERS	LAN	WAN	MAN
Ownership of network	Private	Private or public	Private or public
Geographical area covered	Small	Very large	Moderate
Design and maintenance	Easy	Not easy	Not easy
Communication medium	Coaxial cable	PSTN or satellite links	Coaxial cables, PSTN, optical fibre, cables, wireless
Bandwidth	Low	High	moderate
Data rates(speed)	High	Low	moderate

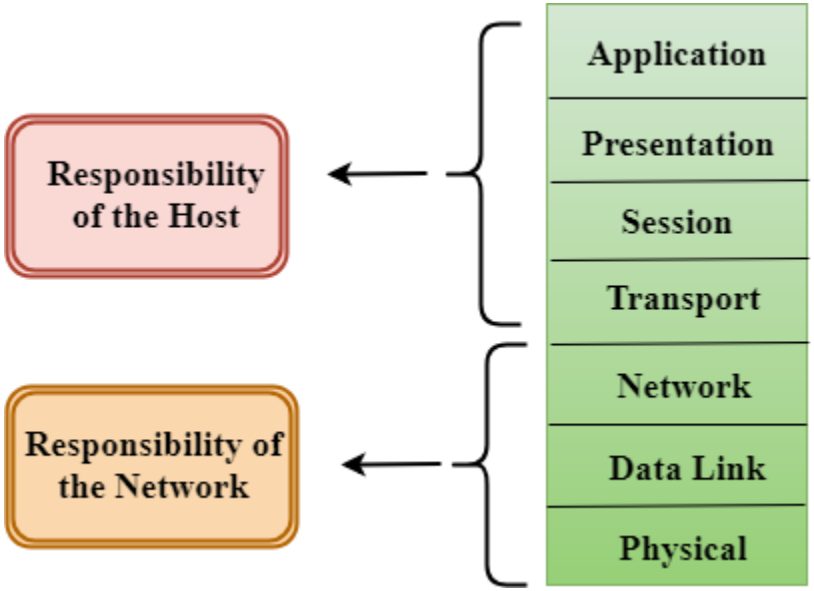
OSI Model

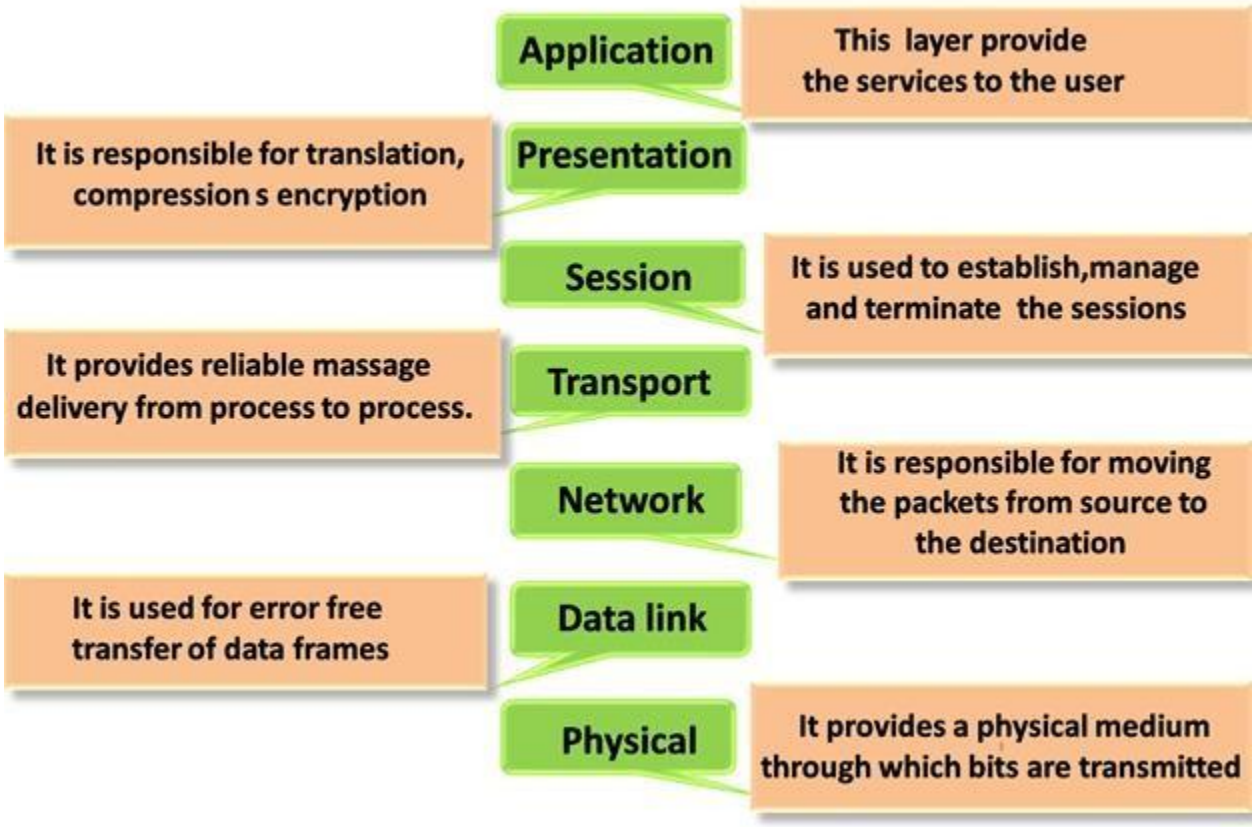
What is OSI?

- 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.

Characteristics of OSI Model:

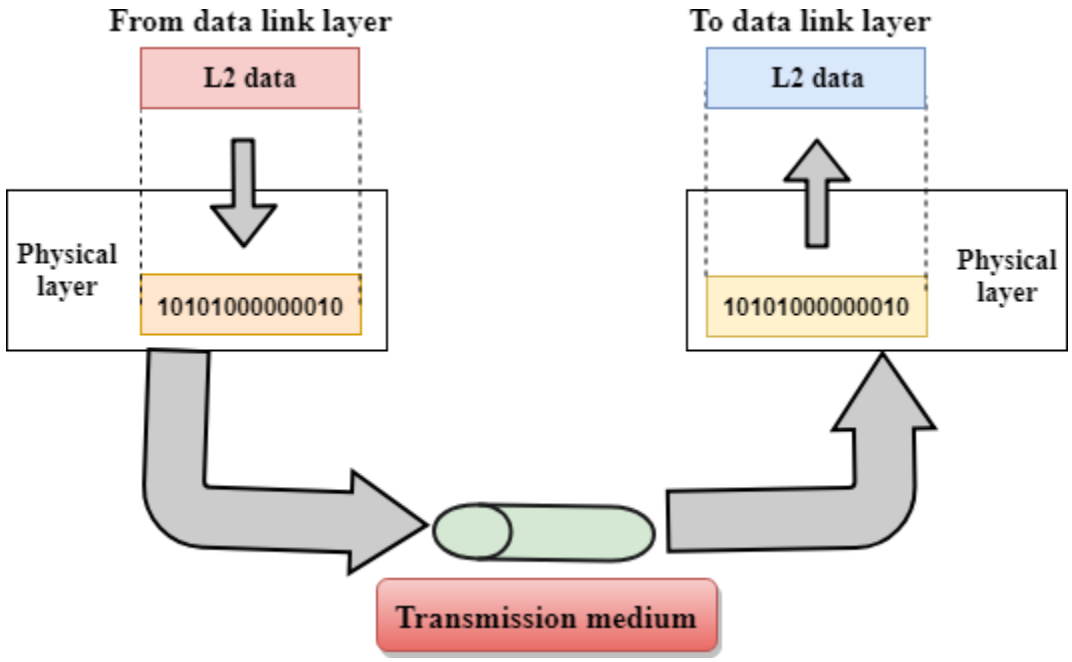
- The OSI model is divided into two layers: upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications.
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.




Application
This layer provide the services to the user
It is responsible for translation, compression s encryption
Presentation
Session
It is used to establish,manage and terminate the sessions
It provides reliable massage delivery from process to process.
Transport
Network
It is responsible for moving the packets from source to the destination
It is used for error free transfer of data frames
Data link
Physical
It provides a physical medium through which bits are transmitted

Physical layer

•The main functionality of the physical layer is to transmit the individual bits from one node to another node.
•It is the lowest layer of the OSI model.
•It establishes, maintains and deactivates the physical connection.
•It specifies the mechanical, electrical and procedural network interface specifications.



Functions of a Physical layer

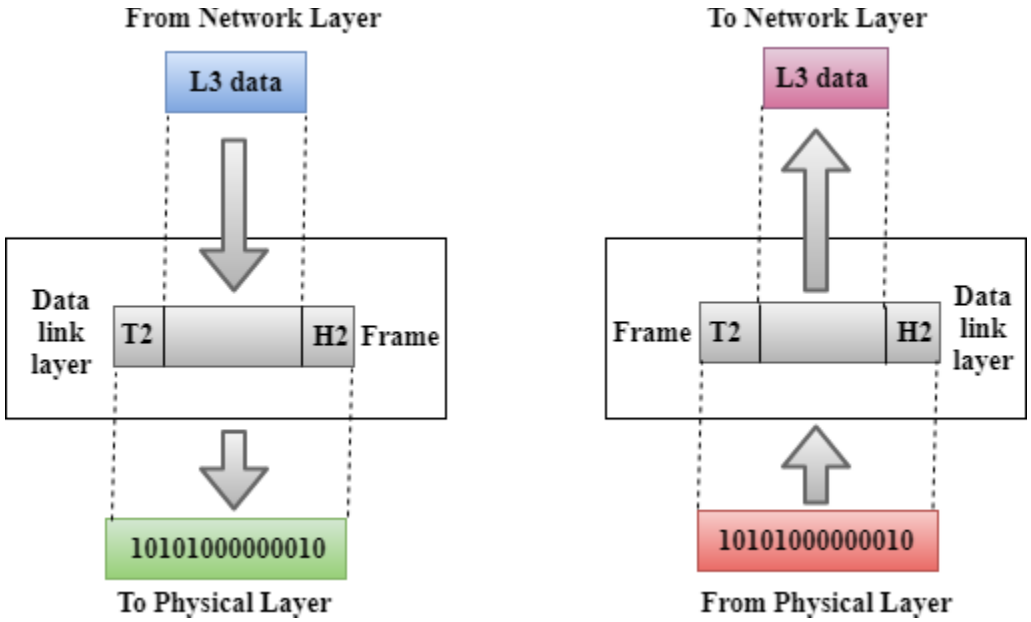
- **Line Configuration:** It defines the way how two or more devices can be connected physically.
- **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- **Topology:** It defines the way how network devices are arranged.
- **Signals:** It determines the type of the signal used for transmitting the information.

Data link Layer

- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub-layers:
  - **Logical Link Control Layer**
    - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
    - It identifies the address of the network layer protocol from the header.
    - It also provides flow control.

Contd..

- **Media Access Control Layer**
  - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
  - It is used for transferring the packets over the network.


From Network Layer
L3 data
Data link layer
T2
H2
Frame
10101000000010
To Physical Layer
To Network Layer
L3 data
Frame
T2
H2
Data link layer
10101000000010
From Physical Layer

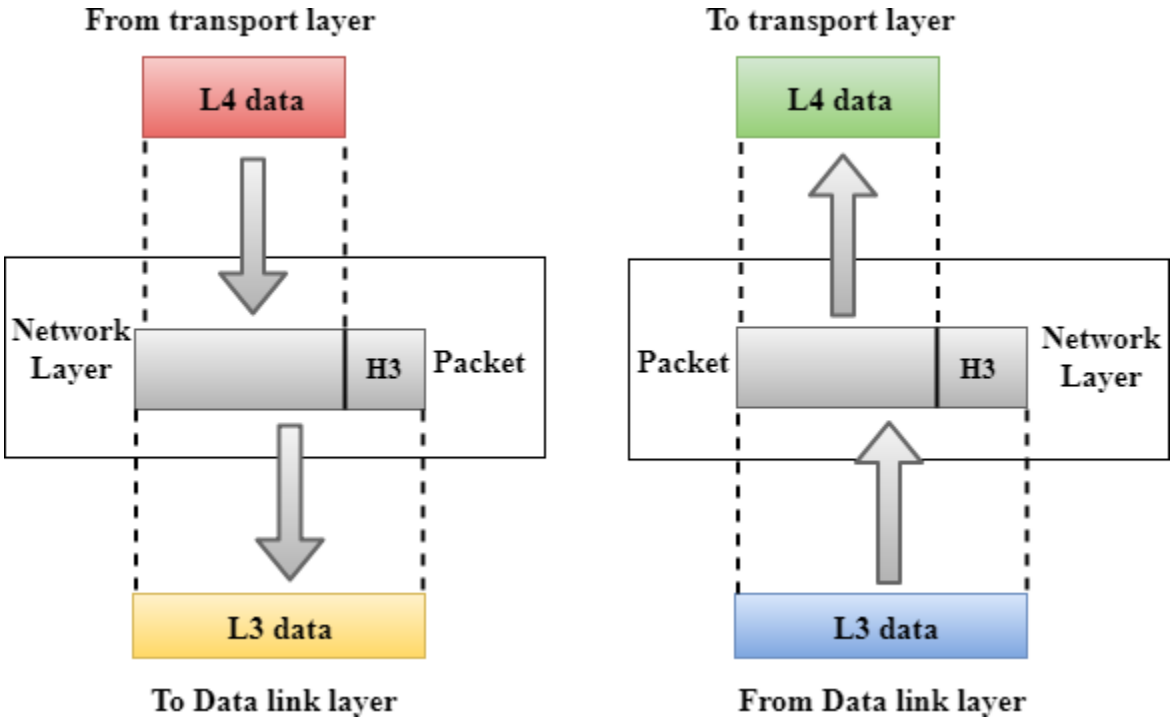
Functions of the Data-link layer

- **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.

Header	Packet	Trailer

- **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 occur, 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



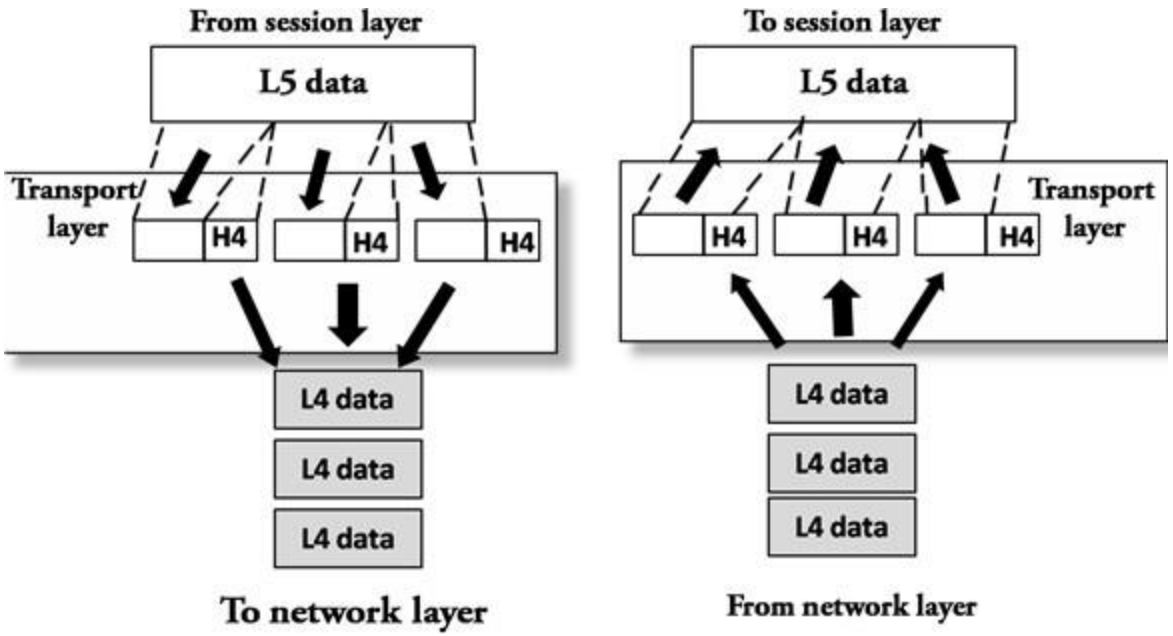
Contd..

- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The n/w link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IPv4(32 bits) and Ipv6(128 bits).

Functions of 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



- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

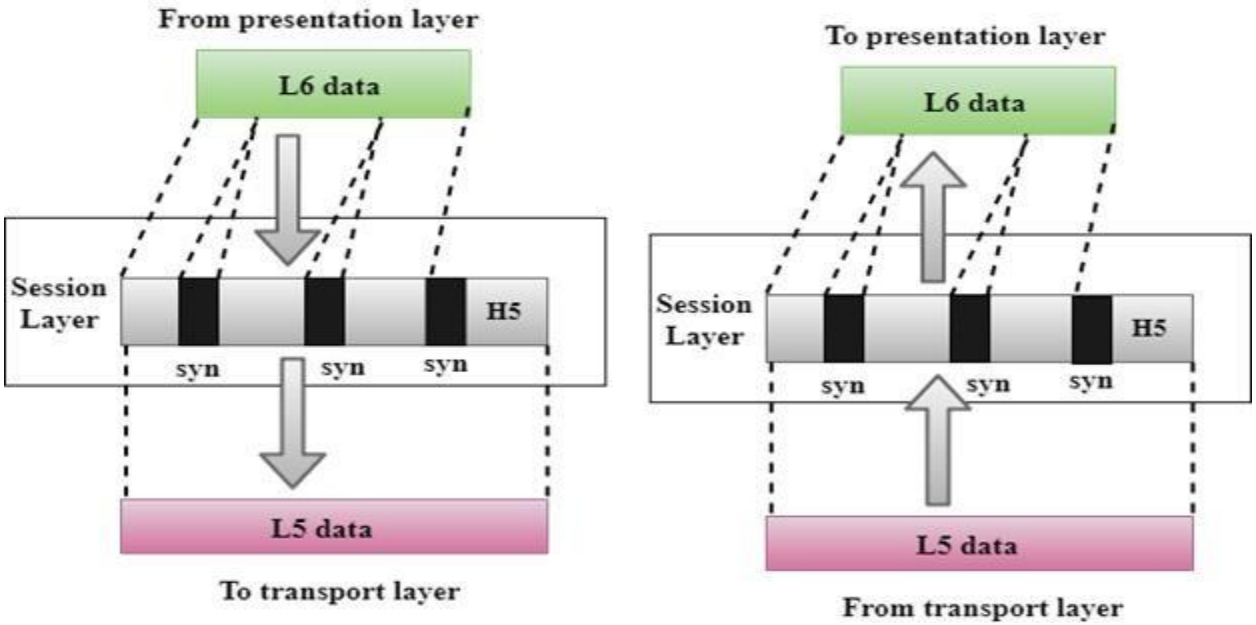
Contd..

- **The two protocols used in this layer are:**
- **Transmission Control Protocol**
  - It is a standard protocol that allows the systems to communicate over the internet.
  - It establishes and maintains a connection between hosts.
  - When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.
- **User Datagram Protocol**
  - User Datagram Protocol is a transport layer protocol.
  - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Functions of 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.

Session Layer



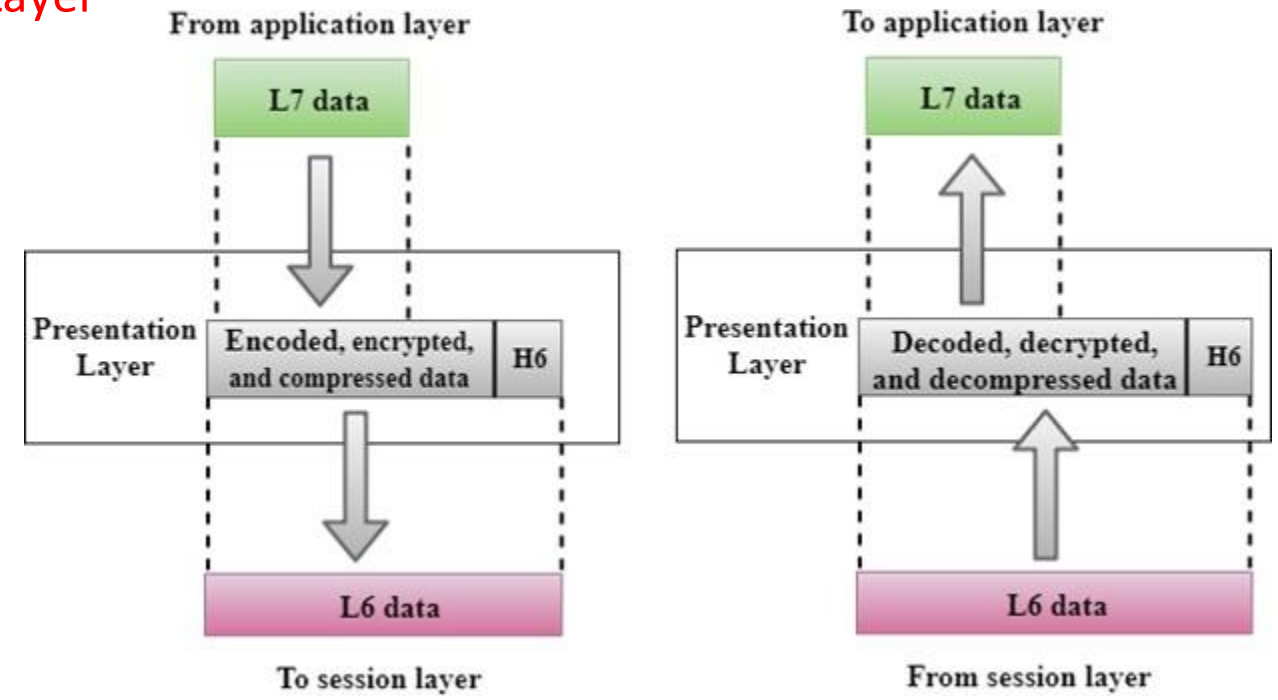
The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

Dialog control: Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.

Synchronization: Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

Presentation Layer

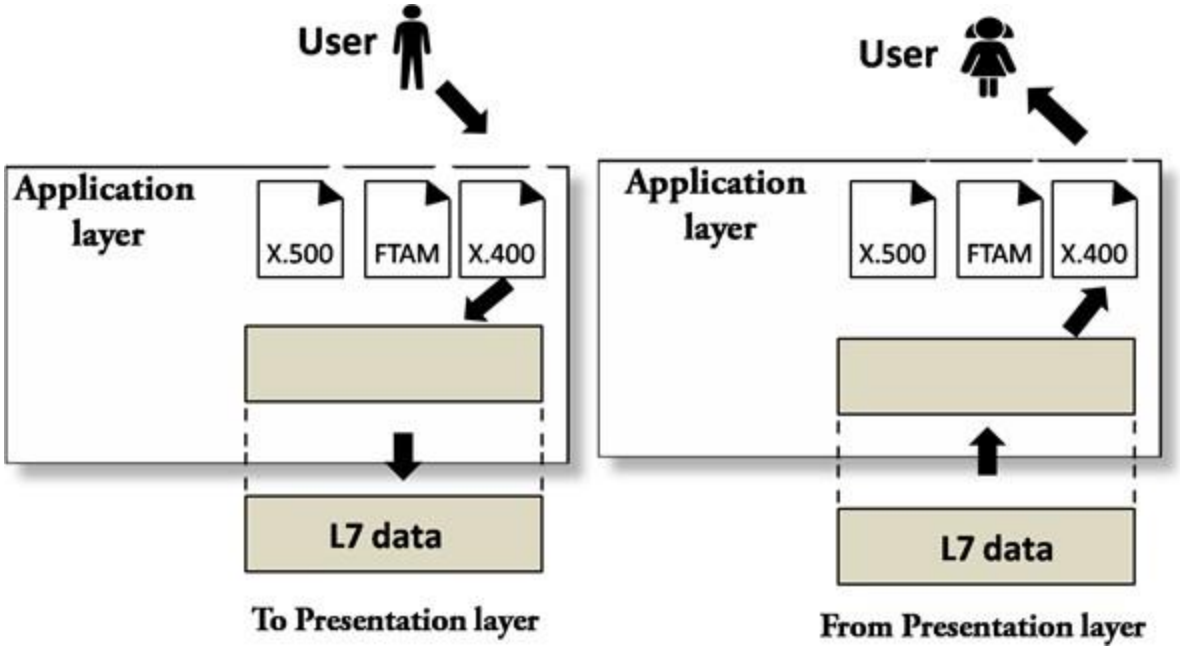


A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
It acts as a data translator for a network.
This layer is a part of the operating system that converts the data from one presentation format to another format.
The Presentation layer is also known as the syntax layer.

Functions of 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.

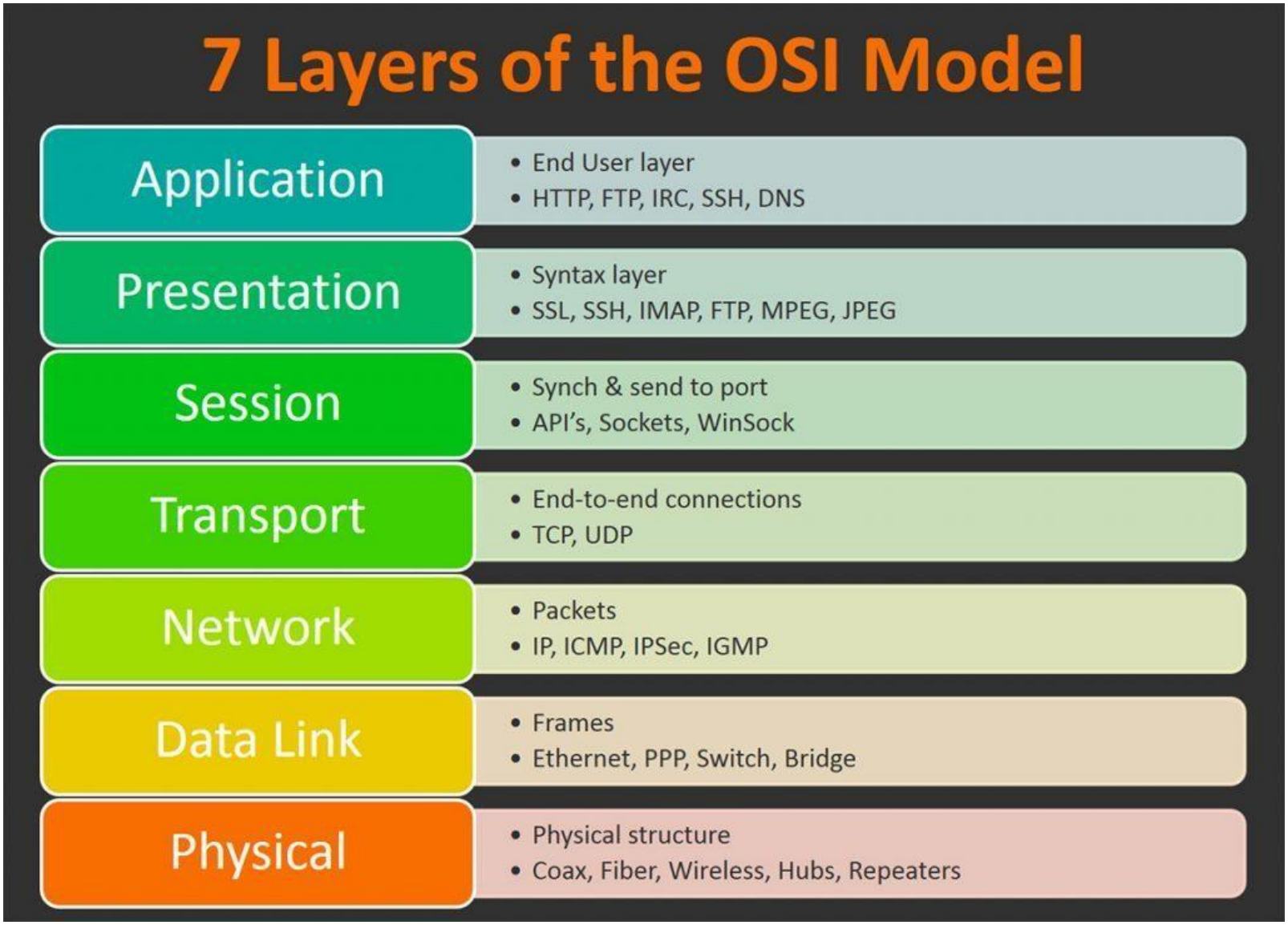
Application Layer

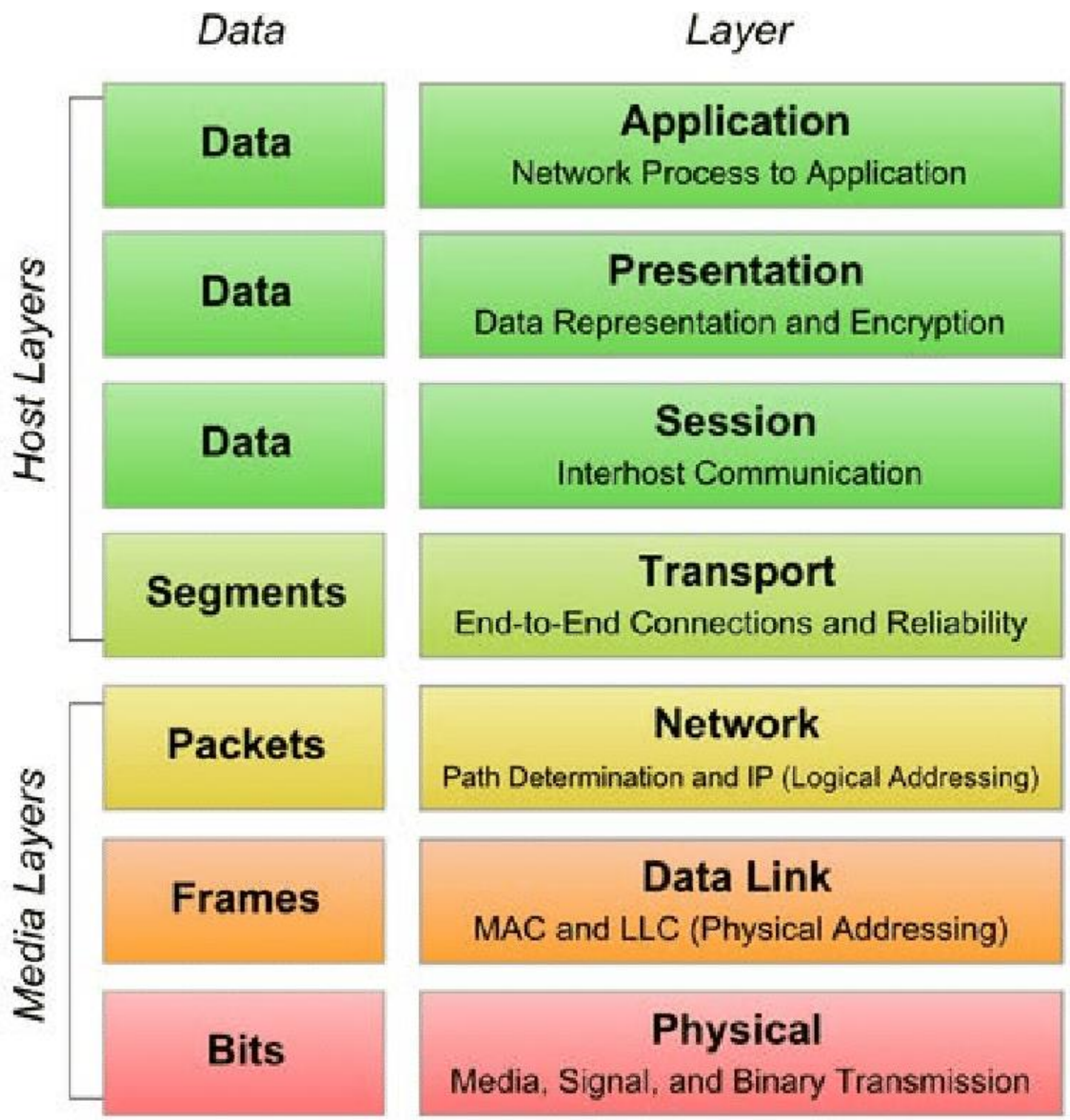


An application layer serves as a window for users and application processes to access network service.
It handles issues such as network transparency, resource allocation, etc.
An application layer is not an application, but it performs the application layer functions.
This layer provides the network services to the end-users.

Functions of 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.


7 Layers of the OSI Model
Application
• End User layer
• HTTP, FTP, IRC, SSH, DNS
Presentation
• Syntax layer
• SSL, SSH, IMAP, FTP, MPEG, JPEG
Session
• Synch & send to port
• API's, Sockets, WinSock
Transport
• End-to-end connections
• TCP, UDP
Network
• Packets
• IP, ICMP, IPSec, IGMP
Data Link
• Frames
• Ethernet, PPP, Switch, Bridge
Physical
• Physical structure
• Coax, Fiber, Wireless, Hubs, Repeaters


Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Physical Addressing)
Bits
Physical
Media, Signal, and Binary Transmission

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	**GATEWAY** Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP		Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		

TCP/IP

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model
- It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components.
- But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols.
- It stands for Transmission Control Protocol/Internet Protocol.
  The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer

OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

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.

Protocols used in Internet layer

- **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.

Transport Layer

- The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.
- The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.
- **User Datagram Protocol (UDP)**
  - It provides connectionless service and end-to-end delivery of transmission.
  - It is an unreliable protocol as it discovers the errors but not specify the error.
  - User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
  - **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.
  - UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.

- **Transmission Control Protocol (TCP)**
  - It provides a full transport layer services to applications.
  - It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
  - TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
  - At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
  - At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

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.

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.

TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable	OSI is less reliable
TCP/IP does not have very strict boundaries.	OSI has strict boundaries
TCP/IP follow a horizontal approach.	OSI follows a vertical approach.
TCP/IP uses both session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP developed protocols then model.	OSI developed model then protocol.
Transport layer in TCP/IP does not provide assurance delivery of packets.	In OSI model, transport layer provides assurance delivery of packets.
TCP/IP model network layer only provides connection less services.	Connection less and connection oriented both services are provided by network layer in OSI model.
Protocols cannot be replaced easily in TCP/IP model.	While in OSI model, Protocols are better covered and is easy to replace with the change in technology.

LAN Components

What is Transmission media?

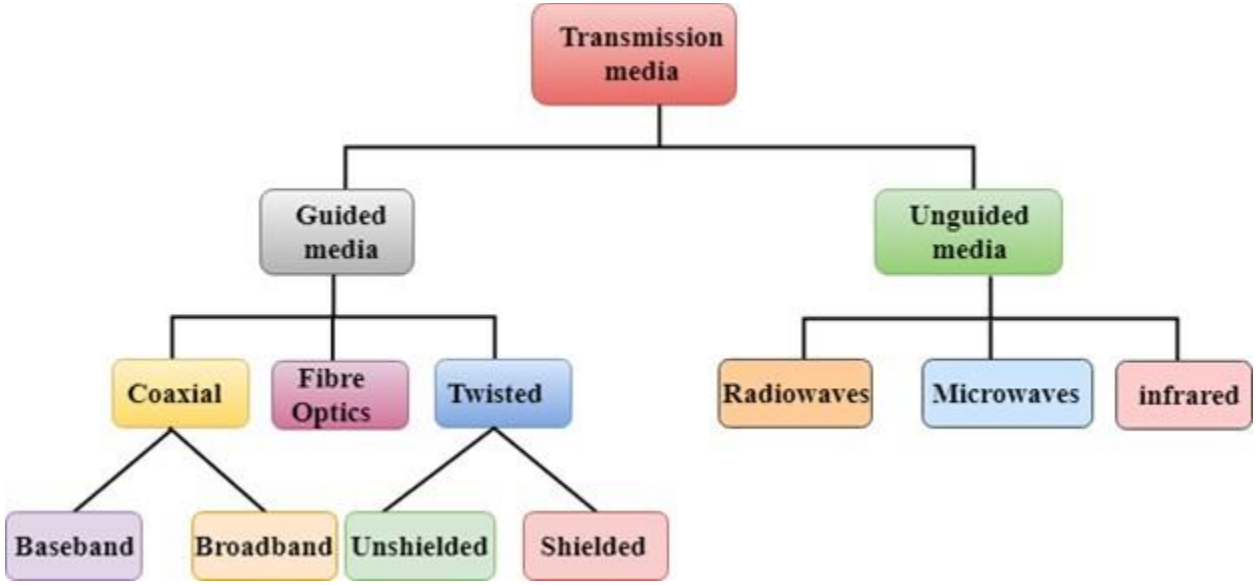
- Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.
- The main functionality of the transmission media is to carry the information in the form of bits through **LAN**(Local Area Network).
- It is a physical path between transmitter and receiver in data communication.
- In a copper-based network, the bits in the form of electrical signals.
- In a fibre based network, the bits in the form of light pulses.
- In **OSI**(Open System Interconnection) phase, transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 component.
- The electrical signals can be sent through the copper wire, fibre optics, atmosphere, water, and vacuum.
- The characteristics and quality of data transmission are determined by the characteristics of medium and signal.
- Transmission media is of two types are wired media and wireless media. In wired media, medium characteristics are more important whereas, in wireless media, signal characteristics are more important.
- Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.
- The transmission media is available in the lowest layer of the OSI reference model, i.e., **Physical layer**.

Factors need to be considered for designing the transmission media

- **Bandwidth:** All the factors are remaining constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal.
- **Transmission impairment:** When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.
- **Interference:** An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.

Causes Of Transmission Impairment

- **Attenuation:** Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.
- **Distortion:** Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delay distortion.
- **Noise:** When data is travelled over a transmission medium, some unwanted signal is added to it which creates the noise.



Guided Media:

It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

Features:

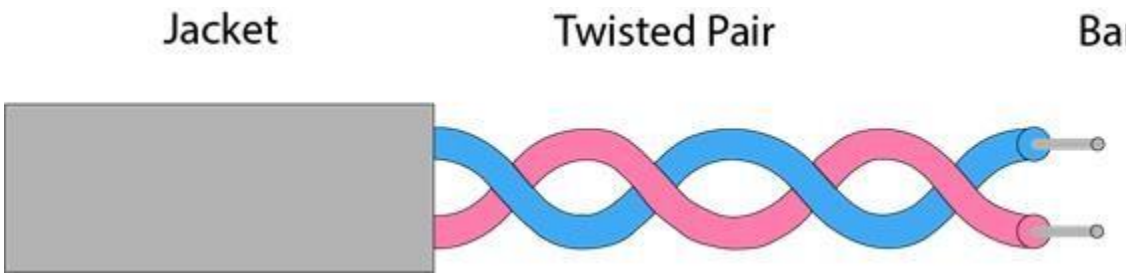
High Speed

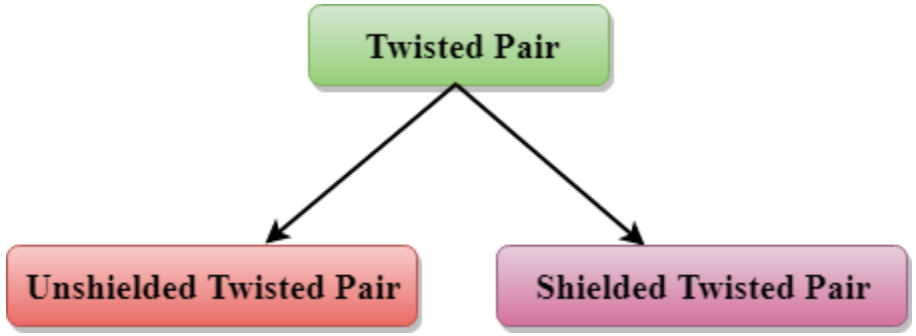
Secure

Used for comparatively shorter distances

(i) Twisted Pair Cable

- It consists of 2 separately insulated conductor wires wound about each other.
- Generally, several such pairs are bundled together in a protective sheath.
- They are the most widely used Transmission Media
- A twisted pair cable is cheap as compared to other transmission media.
- Installation of the twisted pair cable is easy, and it is a lightweight cable.
- The frequency range for twisted pair cable is from 0 to 3.5KHz.


Jacket
Twisted Pair
Bare Wire


Twisted Pair
Unshielded Twisted Pair
Shielded Twisted Pair

Unshielded Twisted Pair (UTP):

- This type of cable has the ability to block interference and does not depend on a physical shield for this purpose.
- It is used for telephonic applications.

Following are the categories of the unshielded twisted pair cable:

- **Category 1:** Category 1 is used for telephone lines that have low-speed data.
- **Category 2:** It can support upto 4Mbps.
- **Category 3:** It can support upto 16Mbps.
- **Category 4:** It can support upto 20Mbps. Therefore, it can be used for long-distance communication.
- **Category 5:** It can support upto 200Mbps.

Advantages Of Unshielded Twisted Pair:

- It is cheap.
- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.

Disadvantage:

- This cable can only be used for shorter distances because of attenuation.

Shielded Twisted Pair

- A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

Characteristics Of Shielded Twisted Pair:

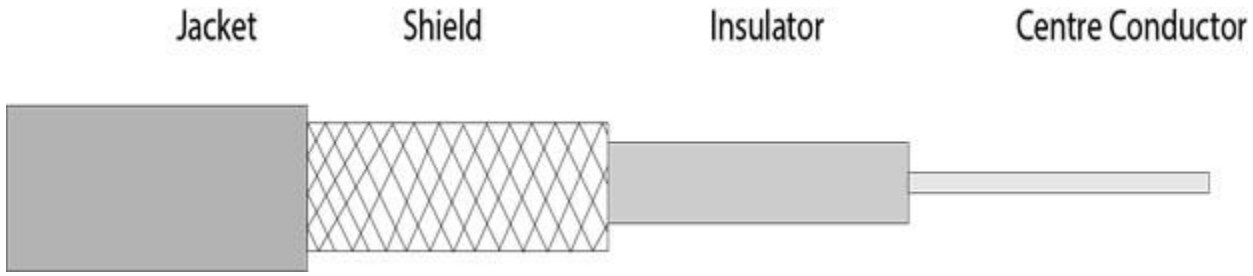
- The cost of the shielded twisted pair cable is not very high and not very low.
- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.

Disadvantages

- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate.

Coaxial Cable

- Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
- The name of the cable is coaxial as it contains two conductors parallel to each other.
- It has a higher frequency as compared to Twisted pair cable.
- The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh. The middle core is made up of non-conductive cover that separates the inner conductor from the outer conductor.
- The middle core is responsible for the data transferring whereas the copper mesh prevents from the **EMI**(Electromagnetic interference).



Coaxial cable is of two types:

Baseband transmission: It is defined as the process of transmitting a single signal at high speed.

Broadband transmission: It is defined as the process of transmitting multiple signals simultaneously.

Advantages Of Coaxial cable:

The data can be transmitted at high speed.

It has better shielding as compared to twisted pair cable.

It provides higher bandwidth.

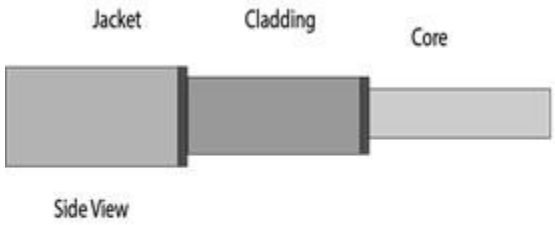
Disadvantages Of Coaxial cable:

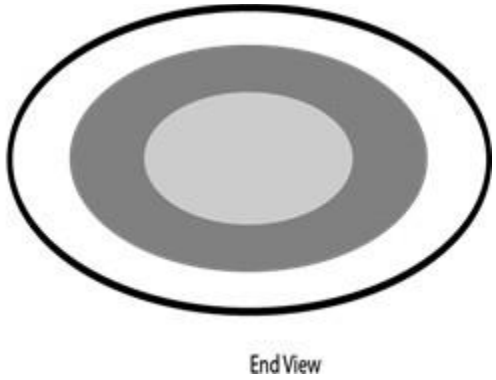
It is more expensive as compared to twisted pair cable.

If any fault occurs in the cable causes the failure in the entire network.

Fibre Optic

- Fibre optic cable is a cable that uses light signals for communication.
- Fibre optic is a cable that holds the optical fibres coated in plastic that are used to send the data by pulses of light.
- The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.
- Fibre optics provide faster data transmission than copper wires.





Basic elements of Fiber optic:

Core: The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.

Cladding: The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.

Jacket: The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

Following are the advantages of fibre optic cable over copper:

- **Greater Bandwidth:** The fibre optic cable provides more bandwidth as compared copper. Therefore, the fibre optic carries more data as compared to copper cable.
- **Faster speed:** Fibre optic cable carries the data in the form of light. This allows the fibre optic cable to carry the signals at a higher speed.
- **Longer distances:** The fibre optic cable carries the data at a longer distance as compared to copper cable.
- **Better reliability:** The fibre optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.
- **Thinner and Sturdier:** Fibre optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

Unguided Media

- It is also referred to as Wireless or Unbounded transmission media.
- No physical medium is required for the transmission of electromagnetic signals.

Features:

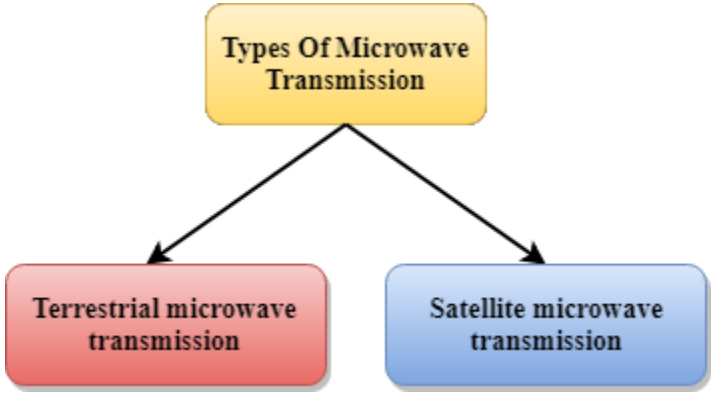
- The signal is broadcasted through air
- Less Secure
- Used for larger distances

Radio waves

- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
- The range in frequencies of radio waves is from 3Khz to 1 khz.
- In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
- An example of the radio wave is **FM radio**

- **Applications Of Radio waves:**
- A Radio wave is useful for multicasting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio wave.
- **Advantages Of Radio transmission:**
- Radio transmission is mainly used for wide area networks and mobile cellular phones.
- Radio waves cover a large area, and they can penetrate the walls.
- Radio transmission provides a higher transmission rate.

Microwaves



Terrestrial Microwave Transmission

Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.

Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.

Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focussed.

In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.

It works on the line of sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.

Characteristics of Microwave:

Frequency range: The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
Bandwidth: It supports the bandwidth from 1 to 10 Mbps.
Short distance: It is inexpensive for short distance.
Long distance: It is expensive as it requires a higher tower for a longer distance.
Attenuation: Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

Advantages Of Microwave:

Microwave transmission is cheaper than using cables.
It is free from land acquisition as it does not require any land for the installation of cables.
Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.
Communication over oceans can be achieved by using microwave transmission.

Disadvantages of Microwave transmission:

Eavesdropping: An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.
Out of phase signal: A signal can be moved out of phase by using microwave transmission.
Susceptible to weather condition: A microwave transmission is susceptible to weather condition. This means that any environmental change such as rain, wind can distort the signal.
Bandwidth limited: Allocation of bandwidth is limited in the case of microwave transmission.

Satellite Microwave Communication

- A satellite is a physical object that revolves around the earth at a known height.
- Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems.
- We can communicate with any point on the globe by using satellite communication.

How Does Satellite work?

- The satellite accepts the signal that is transmitted from the earth station, and it amplifies the signal. The amplified signal is retransmitted to another earth station.

Advantages Of Satellite Microwave Communication:

- The coverage area of a satellite microwave is more than the terrestrial microwave.
- The transmission cost of the satellite is independent of the distance from the centre of the coverage area.
- Satellite communication is used in mobile and wireless communication applications.
- It is easy to install.
- It is used in a wide variety of applications such as weather forecasting, radio/TV signal broadcasting, mobile communication, etc.

Disadvantages Of Satellite Microwave Communication:

- Satellite designing and development requires more time and higher cost.
- The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.
- The life of the satellite is about 12-15 years. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.

Infrared

- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared in the range from 300 GHz to 400 THz.
- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Characteristics

- It supports high bandwidth, and hence the data rate will be very high.
- Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

Connectors

- **1. Repeater** – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.
- **2. Hub** – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

Types of Hub

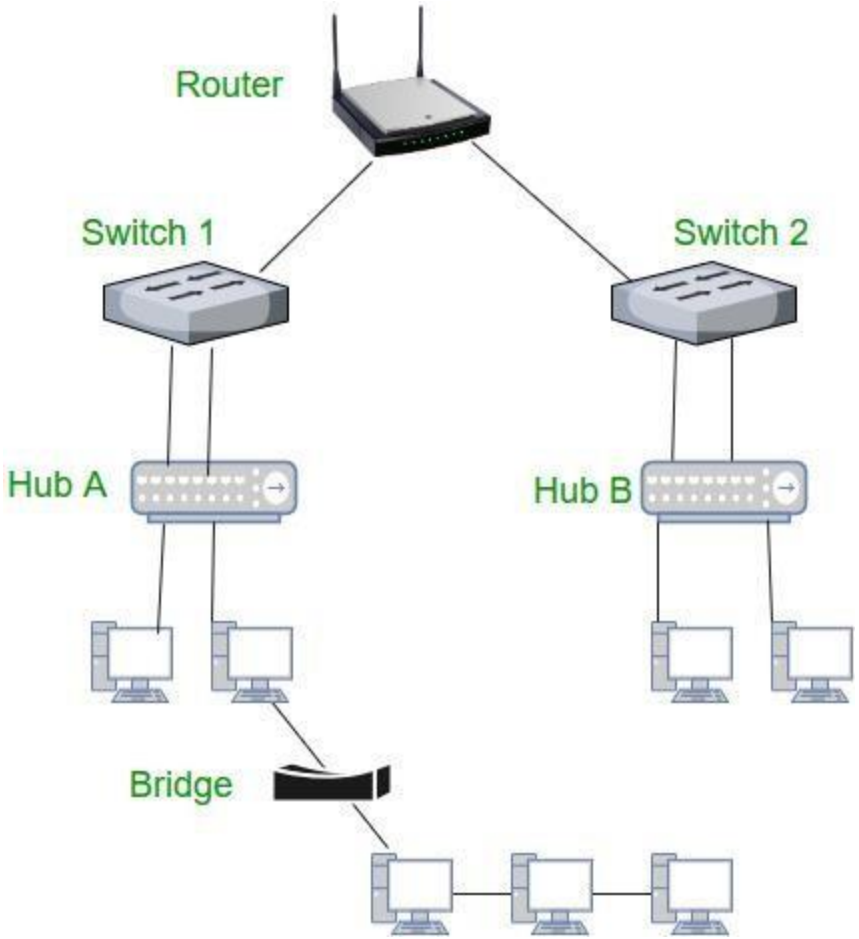
- **Active Hub:-** These are the hubs that have their own power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
- **Passive Hub :-** These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can’t be used to extend the distance between nodes.
- **Intelligent Hub :-** It works like active hubs and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

Bridge

- A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.
- **Types of Bridges**
- **Transparent Bridges:-** These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
- **Source Routing Bridges:-** In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

Switch

- A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance.
- A switch is a data link layer device.
- The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only.
- In other words, the switch divides the collision domain of hosts, but broadcast domain remains the same.



Routers – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

- **Gateway** – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. Gateway is also called a protocol converter.
- **Brouter** – It is also known as the bridging router is a device that combines features of both bridge and router. It can work either at the data link layer or a network layer. Working as a router, it is capable of routing packets across networks, and working as the bridge, it is capable of filtering local area network traffic.
- **NIC** – NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and router or modem. NIC card is a layer 2 device which means that it works on both physical and data link layer of the network model.

Ethernet

- Ethernet is a type of communication protocol that is created at Xerox PARC in 1973 by Robert Metcalfe and others, which connects computers on a network over a wired connection.
- It is a widely used LAN protocol, which is also known as Alto Aloha Network.
- It connects computers within the local area network and wide area network

Type of ethernet	Speed	Distance	Topology	Media
Standard	10Mbps	100m to 2km	Bus, star	Coaxial cable, Fiber, CAT2, UTP
Fast	100Mbps	100m to 5km	Point to point, star, ring	STP, CAT5,UTP, Fiber
Gigabit	1Gbps	100m to 5km	Point to point, star	STP, Fiber
Ten-gigabit	10Gbps	300m to 40km	Point to point, star	Fiber

Advantages of Ethernet

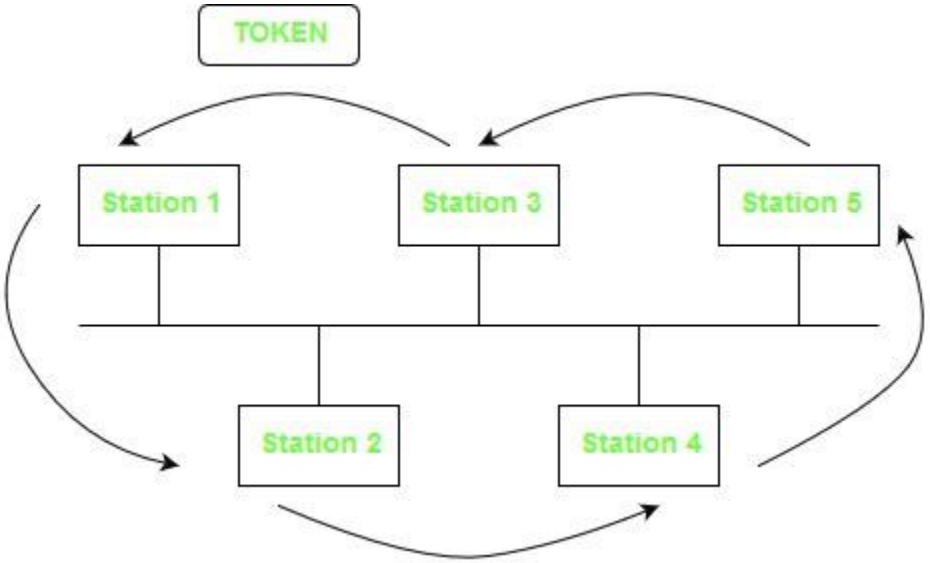
- It is not much costly to form an Ethernet network. As compared to other systems of connecting computers, it is relatively inexpensive.
- Ethernet network provides high security for data as it uses firewalls in terms of data security.
- Also, the Gigabit network allows the users to transmit data at a speed of 1-100Gbps.
- In this network, the quality of the data transfer does maintain.
- In this network, administration and maintenance are easier.
- The latest version of gigabit ethernet and wireless ethernet have the potential to transmit data at the speed of 1-100Gbps.

Disadvantages of Ethernet

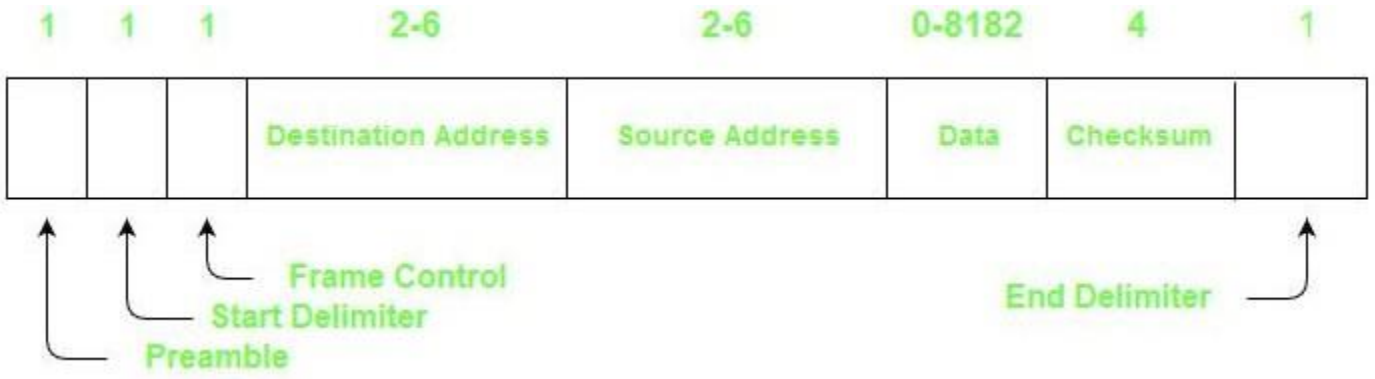
- It needs deterministic service; therefore, it is not considered the best for real-time applications.
- The wired Ethernet network restricts you in terms of distances, and it is best for using in short distances.
- If you create a wired ethernet network that needs cables, hubs, switches, routers, they increase the cost of installation.
- Data needs quick transfer in an interactive application, as well as data is very small.
- In ethernet network, any acknowledge is not sent by receiver after accepting a packet.
- If you are planning to set up a wireless Ethernet network, it can be difficult if you have no experience in the network field.
- Comparing with the wired Ethernet network, wireless network is not more secure.
- The full-duplex data communication mode is not supported by the 100Base-T4 version.
- Additionally, finding a problem is very difficult in an Ethernet network (if has), as it is not easy to determine which node or cable is causing the problem.

Token Bus

- **Token Bus (IEEE 802.4)** is a popular standard for the token passing LANs.
- In a token bus LAN, the physical media is a bus or a tree and a logical ring is created using coaxial cable.
- The token is passed from one user to another in a sequence (clockwise or anticlockwise).
- Each station knows the address of the station to its “left” and “right” as per the sequence in the logical ring.
- A station can only transmit data when it has the token



Frame Format:

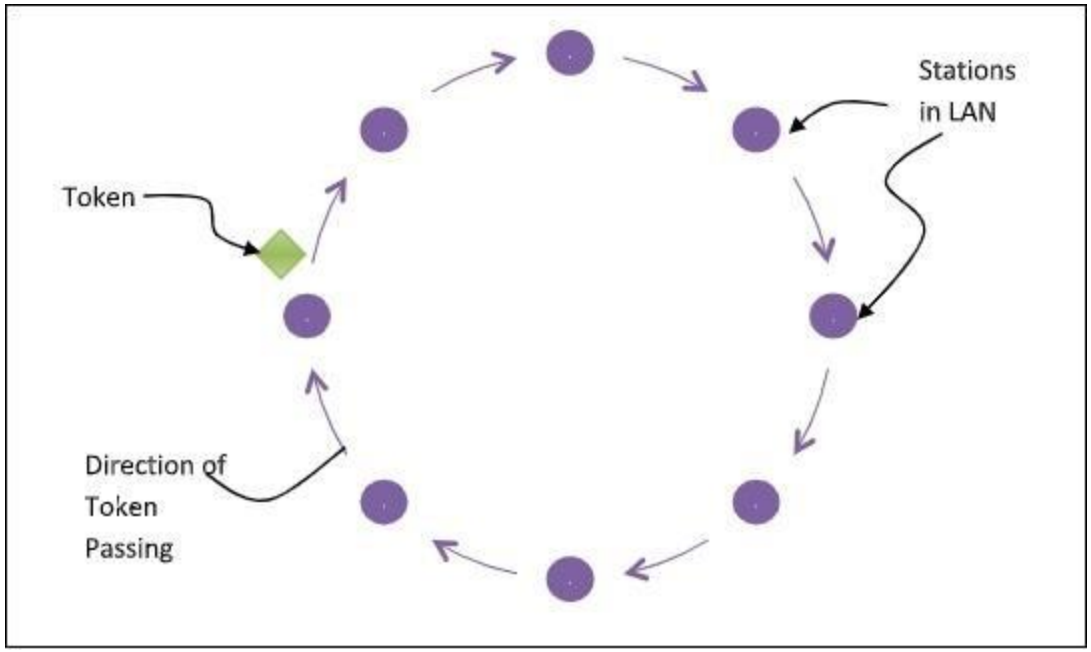


Contd..

- **Preamble –** It is used for bit synchronization. It is 1 byte field.
- **Start Delimiter –** These bits marks the beginning of frame. It is 1 byte field.
- **Frame Control –** This field specifies the type of frame – data frame and control frames. It is 1 byte field.
- **Destination Address –** This field contains the destination address. It is 2 to 6 bytes field.
- **Source Address –** This field contains the source address. It is 2 to 6 bytes field.
- **Data –** If 2 byte addresses are used then the field may be upto 8182 bytes and 8174 bytes in case of 6 byte addresses.
- **Checksum –** This field contains the checksum bits which is used to detect errors in the transmitted data. It is 4 bytes field.
- **End Delimiter –** This field marks the end of frame. It is 1 byte field.

Token Ring

- **Token Ring** protocol is a communication protocol used in Local Area Network (LAN).
- In a token ring protocol, the topology of the network is used to define the order in which stations send.
- The stations are connected to one another in a single ring. It uses a special three-byte frame called a **"token"** that travels around a ring.
- It makes use of Token Passing controlled access mechanism. Frames are also transmitted in the direction of the token.
- This way they will circulate around the ring and reach the station which is the destination



Token Passing Mechanism in Token Ring

If a station has a frame to transmit when it receives a token, it sends the frame and then passes the token to the next station; otherwise it simply passes the token to the next station. Passing the token means receiving the token from the preceding station and transmitting to the successor station. The data flow is unidirectional in the direction of the token passing. In order that tokens are not circulated infinitely, they are removed from the network once their purpose is completed.

IPX/SPX

- **IPX** is a networking protocol that conducts the activities and affairs of the end-to-end process of timely, managed and secured data.
- Originally used by the Novell NetWare operating system and it was later adopted by Windows.
- As they replaced NetWare LANS they became widely used on networks deploying Microsoft Windows LANs.
- IPX/SPX or Internetwork Packet Exchange/Sequenced Packet Exchange was developed by Novell to be a replacement to the TCP/IP Protocol Suite.
- This was introduced in Novell's networking software called Netware in the early 1980s.
- IPX introduced in the 1980s remained fairly popular till the 1990s. After which the TCP/IP protocol has largely replaced it.

Working of IPX

- IPX is the network layer and SPX is the transport layer of the IPX/SPX network protocol.
- IPX and IP protocol have similar functions and this defines how data is sent and received between devices.
- The transport layer protocol or SPX protocol is used to establish and maintain a connection between devices.
- Together, they can be used to transfer data and create a network connection between systems.
- IPX does not require a consistent connection to be maintained while packets are being sent from one system to another, this is what is called being connectionless.
- It can resume the transfer from the point where it was interrupted due to bad connection or power loss.

Applications

- IPX provides peer-to-peer support connectivity. Like IP, IPX also contains end-user data and is connectionless, just like network addresses.
- Novell's original NetWare client was written for DOS. In the 1990s, video games like Quake, Descent, and WarCraft 2 were supported with IPX for network gaming. Kali was the name of a service used as an emulator to let gamers play online

Advantages

- IPX/SPX was primarily designed for local area networks (LANs) and is very efficient when used for this only.
- IPX has a larger address space: 48 bits instead of 32 bits in IPv4.
- IPX addresses incorporate the local MAC address:compared to “address assignment” like with IPv4.
- No BootP or DHCP in IPX. (DHCP was invented from BootP was so that IPv4 could allow “plug-and-go” network addressing like what IPX did. It was later added in IPv6.)

Disadvantages

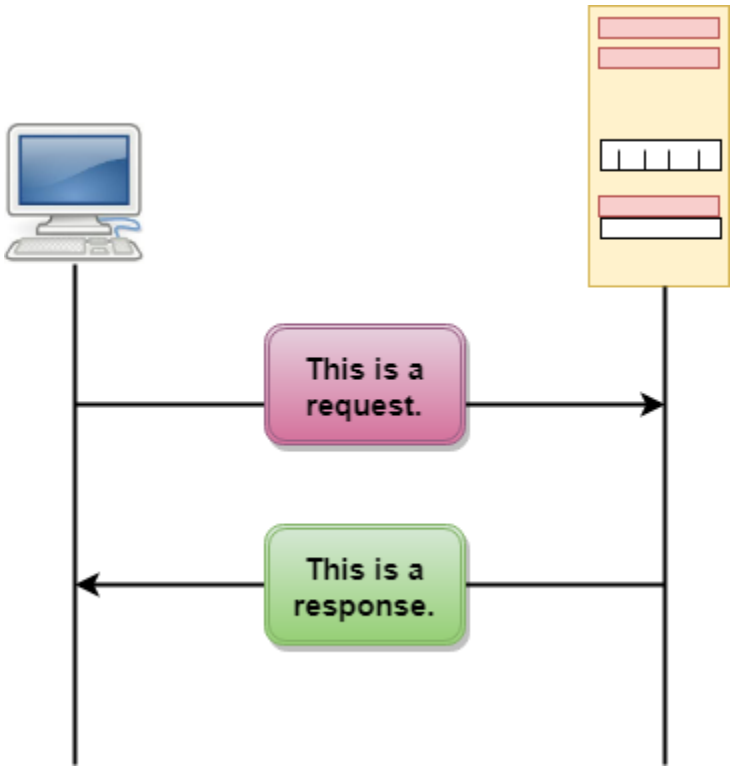
- Nowadays IPX is falling out of trend. TCP/IP is mostly used because of its superior performance over wide area networks and the Internet and its a more mature protocol created with the same purpose in mind. The real advantage of TCP/IP is interoperability and vendor-independent open standards.
- With IPX applications and the use of the internet, the costs are higher if you are implementing VPNs.
- Encapsulating and encrypting of IPX frames in an IP packet requires expensive hardware than performing a straight IPSec VPN.

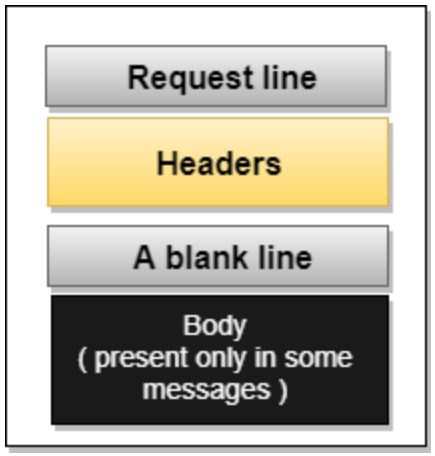
HTTP (Hyper text transfer protocol)

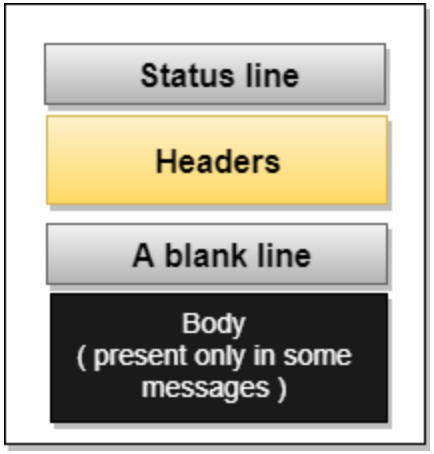
- HTTP stands for **HyperText Transfer Protocol**.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.
- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.
- HTTP is used to carry the data in the form of MIME-like format.
- HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the client to the server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

Features of HTTP:

- **Connectionless protocol:** HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.
- **Media independent:** HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content. It is required for both the client and server to specify the content type in MIME-type header.
- **Stateless:** HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.


This is a request.
This is a response.


Request line
Headers
A blank line
Body
(present only in some messages)


Status line
Headers
A blank line
Body
(present only in some messages)

Methods (Request type)

Method	*Action*
GET	Requests a document from the server
HEAD	Requests information about a document but not the document itself
POST	Sends some information from the client to the server
PUT	Sends a document from the server to the client
TRACE	Echoes the incoming request
CONNECT	Reserved
OPTION	Inquires about available options

Code	*Phrase*	*Description*
	Informational	
100	Continue	The initial part of the request has been received, and the client may continue with its request.
101	Switching	The server is complying with a client request to switch protocols defined in the upgrade header.
	Success	
200	OK	The request is successful.
201	Created	A new URL is created.
202	Accepted	The request is accepted, but it is not immediately acted upon.
204	No content	There is no content in the body.

Code	*Phrase*	*Description*
	Redirection	
301	Moved permanently	The requested URL is no longer used by the server.
302	Moved temporarily	The requested URL has moved temporarily.
304	Not modified	The document has not been modified.
	Client Error	
400	Bad request	There is a syntax error in the request.
401	Unauthorized	The request lacks proper authorization.
403	Forbidden	Service is denied.
404	Not found	The document is not found.
405	Method not allowed	The method is not supported in this URL.
406	Not acceptable	The format requested is not acceptable.
	Server Error	
500	Internal server error	There is an error, such as a crash, at the server site.
501	Not implemented	The action requested cannot be performed.
503	Service unavailable	The service is temporarily unavailable, but may be requested in the future.

Uniform Resource Locator (URL)

A client that wants to access the document in an internet needs an address and to facilitate the access of documents, the HTTP uses the concept of Uniform Resource Locator (URL).

The Uniform Resource Locator (URL) is a standard way of specifying any kind of information on the internet.

The URL defines four parts: method, host computer, port, and path.

Method: The method is the protocol used to retrieve the document from a server. For example, HTTP.

Host: The host is the computer where the information is stored, and the computer is given an alias name. Web pages are mainly stored in the computers and the computers are given an alias name that begins with the characters "www". This field is not mandatory.

Port: The URL can also contain the port number of the server, but it's an optional field. If the port number is included, then it must come between the host and path and it should be separated from the host by a colon.

Path: Path is the pathname of the file where the information is stored. The path itself contain slashes that separate the directories from the subdirectories and files.

FTP

•FTP stands for File transfer protocol.

•FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.

•It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.

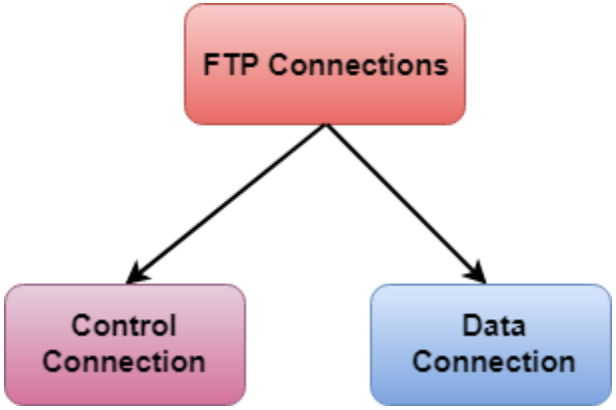
•It is also used for downloading the files to computer from other servers.

Objectives of FTP

•It provides the sharing of files.

•It is used to encourage the use of remote computers.

•It transfers the data more reliably and efficiently.



Control Connection: The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.

Data Connection: The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

FTP Clients

FTP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet.

It allows a user to connect to a remote host and upload or download the files.

It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection.

The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.

Advantages of FTP:

Speed: One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.

Efficient: It is more efficient as we do not need to complete all the operations to get the entire file.

Security: To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.

Back & forth movement: FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

Disadvantages of FTP:

The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provides encryption.

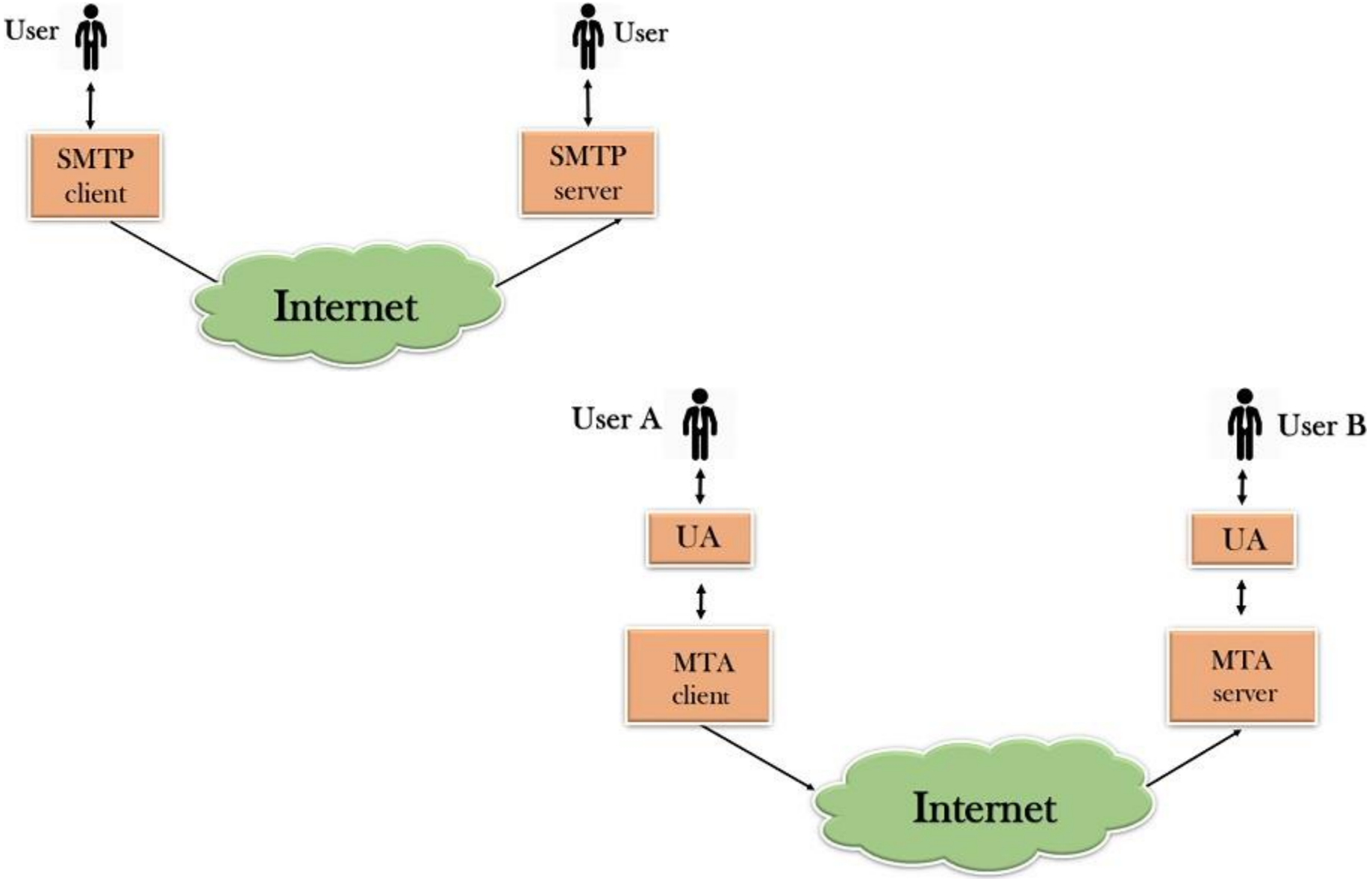
FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.

Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.

It is not compatible with every system.

SMTP

- SMTP stands for Simple Mail Transfer Protocol.
- SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called **Simple Mail Transfer Protocol**.
- It is a program used for sending messages to other computer users based on e-mail addresses.
- It provides a mail exchange between users on the same or different computers, and it also supports:
  - It can send a single message to one or more recipients.
  - Sending message can include text, voice, video or graphics.
  - It can also send the messages on networks outside the internet.
- The main purpose of SMTP is used to set up communication rules between servers. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. They also have a way of handling the errors such as incorrect email address. For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.


User
User
SMTP client
SMTP server
Internet
User A
User B
UA
UA
MTA client
MTA server
Internet

Working of SMTP

Composition of Mail: A user sends an e-mail by composing an electronic mail message using a Mail User Agent (MUA). Mail User Agent is a program which is used to send and receive mail. The message contains two parts: body and header. The body is the main part of the message while the header includes information such as the sender and recipient address. The header also includes descriptive information such as the subject of the message. In this case, the message body is like a letter and header is like an envelope that contains the recipient's address.

Submission of Mail: After composing an email, the mail client then submits the completed e-mail to the SMTP server by using SMTP on TCP port 25.

Delivery of Mail: E-mail addresses contain two parts: username of the recipient and domain name. For example, vivek@gmail.com, where "vivek" is the username of the recipient and "gmail.com" is the domain name.

If the domain name of the recipient's email address is different from the sender's domain name, then MSA will send the mail to the Mail Transfer Agent (MTA). To relay the email, the MTA will find the target domain. It checks the MX record from Domain Name System to obtain the target domain. The MX record contains the domain name and IP address of the recipient's domain. Once the record is located, MTA connects to the exchange server to relay the message.

Receipt and Processing of Mail: Once the incoming message is received, the exchange server delivers it to the incoming server (Mail Delivery Agent) which stores the e-mail where it waits for the user to retrieve it.

Access and Retrieval of Mail: The stored email in MDA can be retrieved by using MUA (Mail User Agent). MUA can be accessed by using login and password.

Telnet

- The main task of the internet is to provide services to users. For example, users want to run different application programs at the remote site and transfers a result to the local site. This requires a client-server program such as FTP, SMTP. But this would not allow us to create a specific program for each demand.
- The better solution is to provide a general client-server program that lets the user access any application program on a remote computer. Therefore, a program that allows a user to log on to a remote computer. A popular client-server program Telnet is used to meet such demands. Telnet is an abbreviation for **Terminal Network**.
- Telnet provides a connection to the remote computer in such a way that a local terminal appears to be at the remote side.

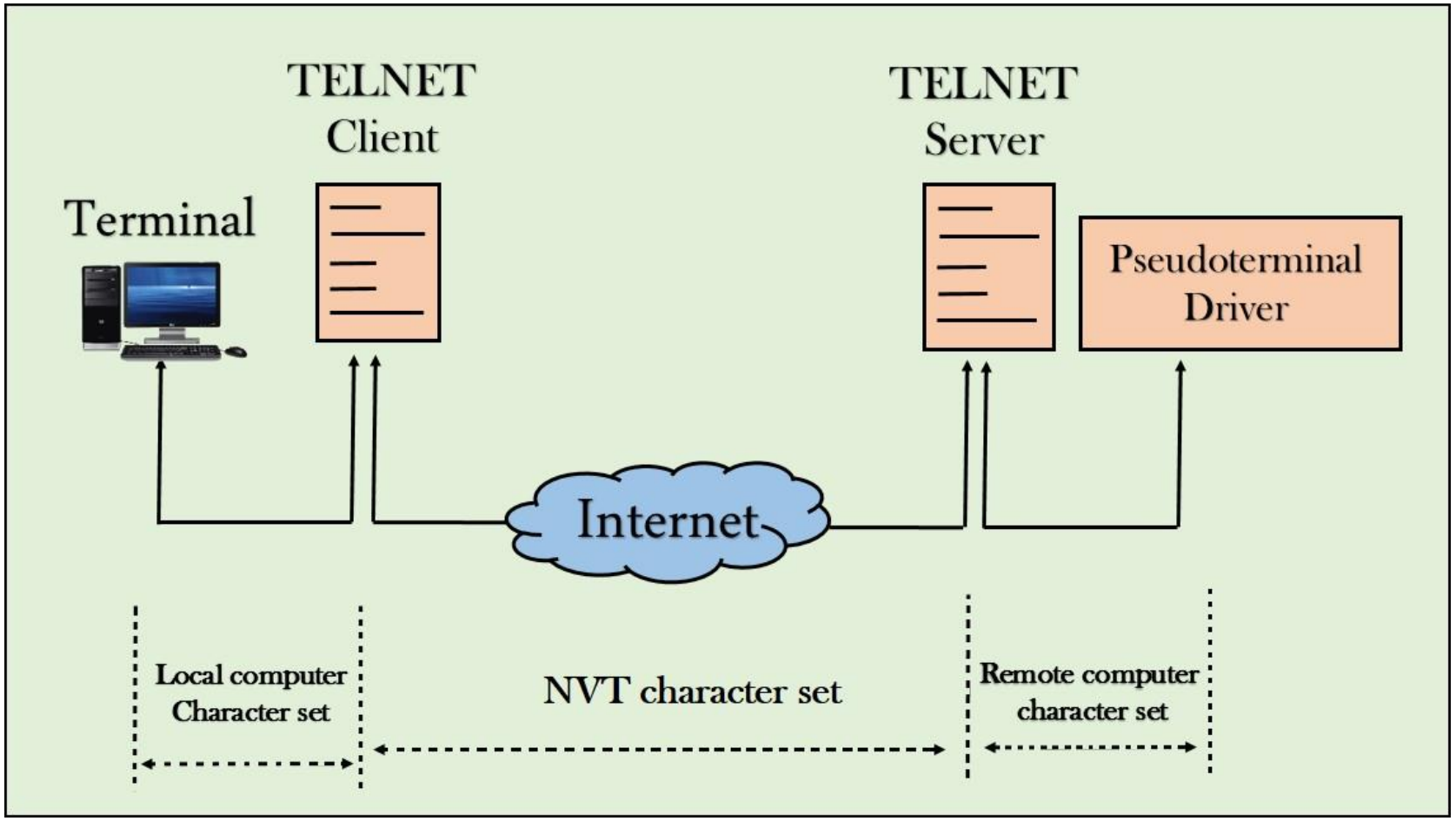
How remote login occurs

At the local site

- The user sends the keystrokes to the terminal driver, the characters are then sent to the TELNET client. The TELNET client which in turn, transforms the characters to a universal character set known as network virtual terminal characters and delivers them to the local TCP/IP stack

At the remote site

- The commands in NVT forms are transmitted to the TCP/IP at the remote machine. Here, the characters are delivered to the operating system and then pass to the TELNET server. The TELNET server transforms the characters which can be understandable by a remote computer. However, the characters cannot be directly passed to the operating system as a remote operating system does not receive the characters from the TELNET server. Therefore it requires some piece of software that can accept the characters from the TELNET server. The operating system then passes these characters to the appropriate application program.


TELNET
Client
TELNET
Server
Terminal
Pseudoterminal
Driver
Internet
Local computer
Character set
NVT character set
Remote computer
character set

- The network virtual terminal is an interface that defines how data and commands are sent across the network.
- In today's world, systems are heterogeneous. For example, the operating system accepts a special combination of characters such as end-of-file token running a DOS operating system *ctrl+z* while the token running a UNIX operating system is *ctrl+d*.
- TELNET solves this issue by defining a universal interface known as network virtual interface.
- The TELNET client translates the characters that come from the local terminal into NVT form and then delivers them to the network. The Telnet server then translates the data from NVT form into a form which can be understandable by a remote computer.

TCP/IP addressing

- **TCP/IP** includes an Internet addressing scheme that allows users and applications to identify a specific network or host with which to communicate.
- 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, subnetworks, hosts, and sockets, and for using special addresses for broadcasts and local loopback.
- Internet addresses are made up of a network address and a host (or local) address. This two-part address allows a sender to specify the network as well as a specific host on the network. A unique, official network address is assigned to each network when it connects to other Internet networks. However, if a local network is not going to connect to other Internet networks, it can be assigned any network address that is convenient for local use.
- The Internet addressing scheme consists of Internet Protocol (IP) addresses and two special cases of IP addresses: broadcast addresses and loopback addresses.

Application Type	Application-layer protocol	Transport Protocol
Electronic mail	Send: Simple Mail Transfer Protocol SMTP [RFC 821]	TCP 25
	Receive: Post Office Protocol v3 POP3 [RCF 1939]	TCP 110
Remote terminal access	Telnet [RFC 854]	TCP 23
World Wide Web (WWW)	HyperText Transfer Protocol 1.1 HTTP 1.1 [RFC 2068]	TCP 80
File Transfer	File Transfer Protocol FTP [RFC 959]	TCP 21
	Trivial File Transfer Protocol TFTP [RFC 1350]	UDP 69
Remote file server	NFS [McKusik 1996]	UDP or TCP
Streaming multimedia	Proprietary (e.g., Real Networks)	UDP or TCP
Internet telephony	Proprietary (e.g., Vocaltec)	Usually UDP

Networking Protocols

Networking Protocols include :

FTP - File Transfer Protocol : Port 21
SSH - Secure Shell : Port 22
Telnet - Port 23
SMTP - Simple Mail Transfer Protocol : Port 25
DNS - Domain Naming System (or Service) : Port 53
HTTP - Hypertext Transfer Protocol : Port 80
POP3 - Post Office Protocol : Port 110
IMAP - Internet Message Access Protocol : Port 143
HTTPS - HTTP Secure : Port 443
RDP - Remote Desktop Protocol : Port 3389
TCP - Transmission Control Protocol
UDP - User Datagram Protocol
ARP - Address Resolution Protocol
RARP - Reverse ARP
DHCP - Dynamic Host Configuration Protocol : Server Port 67, Client Port 68
MTP - Media Transfert Protocol
SFTP - Secure File Transfer Protocol
SSL - Secure Socket Layer
TLS - Transport Layer Security
E6 - Ethernet globalization protocols
NTP - Network time protocol
PPP - Point to Point Protocol
NNTP - Network News Transfer Protocol
QOTD - Quote Of The Day
Bitcoin Protocol - Protocol for Bitcoin transactions and transfers on the web
ICMP - Internet Control Message Protocol
IGMP - Internet Group Management Protocol
GGP - Gateway-to-Gateway Protocol
IP-in-IP - IP in IP (encapsulation)

Internet addresses

The Internet Protocol (IP) uses a 32-bit, two-part address field.

Subnet addresses

Subnet addressing allows an autonomous system made up of multiple networks to share the same Internet address.

Broadcast addresses

The TCP/IP can send data to all hosts on a local network or to all hosts on all directly connected networks. Such transmissions are called *broadcast messages*.

Local loopback addresses

The Internet Protocol defines the special network address, 127.0.0.1, as a local loopback address.

Internet addresses

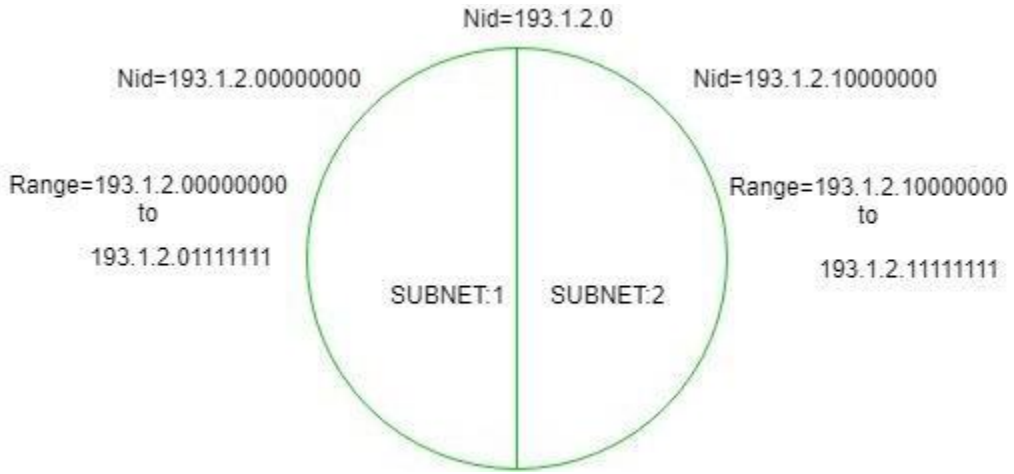
- The Internet Protocol (IP) uses a 32-bit, two-part address field.
- The 32 bits are divided into four *octets* as in the following:
- 01111101 00001101 01001001 00001111
- These binary numbers translate into:
- 125 13 73 15
- The two parts of an Internet address are the network address portion and the host address portion. This allows a remote host to specify both the remote network and the host on the remote network when sending information.
- By convention, a host number of 0 is used to refer to the network itself.

Contd..

- TCP/IP supports three classes of Internet addresses: Class A, Class B, and Class C. The different classes of Internet addresses are designated by how the 32 bits of the address are allocated. The particular address class a network is assigned depends on the size of the network.
- **Class A addresses**
  A Class A address consists of an 8-bit network address and a 24-bit local or host address.
- **Class B addresses**
  A Class B address consists of a 16-bit network address and a 16-bit local or host address.
- **Class C addresses**
  A Class C address consists of a 24-bit network address and an 8-bit local host address.

Subnetting

- **Subnetting** is the practice of dividing a network into two or smaller networks.
- It increases routing efficiency, which helps to enhance the security of the network and reduces the size of the broadcast domain.



so to divide a network into two parts, you need to choose one bit for each Subnet from the host ID part.

In the above diagram, there are two Subnets.
Note: It is a class C IP so, there are 24 bits in the network id part and 8 bits in the host id part.

Contd..

- **For Subnet-1:**
  The first bit which is chosen from the host id part is zero and the range will be from (193.1.2.00000000 till you get all 1's in the host ID part i.e, 193.1.2.01111111) except for the first bit which is chosen zero for subnet id part.Thus, the range of subnet-1:
- 193.1.2.0 to 193.1.2.127
- **For Subnet-2:**
  The first bit chosen from the host id part is one and the range will be from (193.1.2.100000000 till you get all 1's in the host ID part i.e, 193.1.2.11111111).Thus, the range of subnet-2:
- 193.1.2.128 to 193.1.2.255

Network Address and Mask

- Network address – It identifies a network on internet. Using this, we can find range of addresses in the network and total possible number of hosts in the network.
- Mask – It is a 32-bit binary number that gives the network address in the address block when AND operation is bitwise applied on the mask and any IP address of the block.

- The default mask in different classes are :
- Class A – 255.0.0.0
- Class B – 255.255.0.0
- Class C – 255.255.255.0
- Example : Given IP address 132.6.17.85 and default class B mask, find the beginning address (network address).
- Solution : The default mask is 255.255.0.0, which means that the only the first 2 bytes are preserved and the other 2 bytes are set to 0. Therefore, the network address is 132.6.0.0.

Some values calculated in subnetting :

1. Number of subnets : Given bits for mask – No. of bits in default mask
2. Subnet address : AND result of subnet mask and the given IP address
3. Broadcast address : By putting the host bits as 1 and retaining the network bits as in the IP address
4. Number of hosts per subnet : $2^{(32 - \text{Given bits for mask})} - 2$
5. First Host ID : Subnet address + 1 (adding one to the binary representation of the subnet address)
6. Last Host ID : Subnet address + Number of Hosts

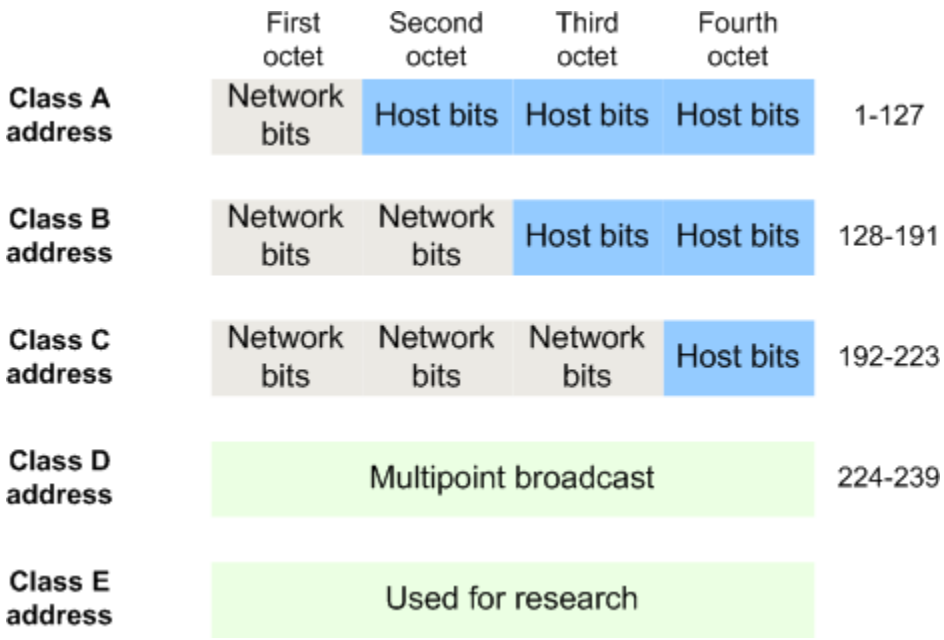
Example : Given IP Address – 172.16.0.0/25, find the number of subnets and the number of hosts per subnet. Also, for the first subnet block, find the subnet address, first host ID, last host ID and broadcast address.

Solution : This is a class B address.

So, no. of subnets = $2^{(25-16)} = 2^9 = 512$.

No. of hosts per subnet = $2^{(32-25)} – 2 = 2^7 – 2 = 128 – 2 = 126$

For the first subnet block, we have subnet address = 0.0, first host id = 0.1, last host id = 0.126 and broadcast address = 0.127


First octet
Second octet
Third octet
Fourth octet
Class A address
Network bits
Host bits
Host bits
Host bits
1-127
Class B address
Network bits
Network bits
Host bits
Host bits
128-191
Class C address
Network bits
Network bits
Network bits
Host bits
192-223
Class D address
Multipoint broadcast
224-239
Class E address
Used for research