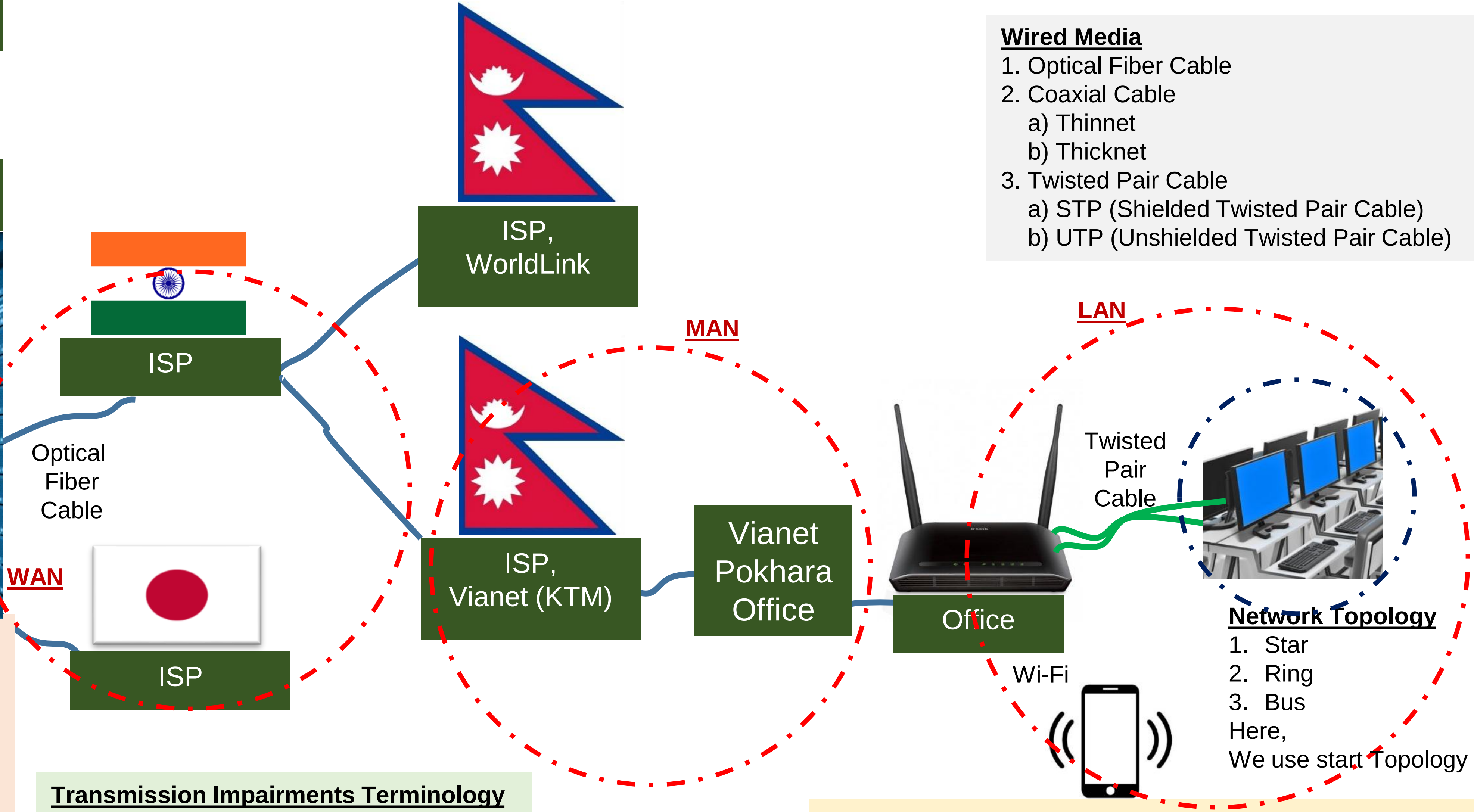
Communication and Networking

Marks: 9
LQA: 1
MCA: 1

Networking

Data Center



Network Topology

1. Star
2. Ring
3. Bus

Here,
We use start Topology

Wired Media

1. Optical Fiber Cable
2. Coaxial Cable
   a) Thinnet
   b) Thicknet
3. Twisted Pair Cable
   a) STP (Shielded Twisted Pair Cable)
   b) UTP (Unshielded Twisted Pair Cable)

Data Center

- A data center is a physical location that stores computing machines and their related hardware equipment.
- Used for storing, managing, and distributing data.
- Each data center houses tens of thousands of computer servers, which are networked together and linked to the outside world through fiber optic cables.
- Some Data Center: Google, Amazon, Facebook, Microsoft etc.

Transmission Impairments Terminology

1. Jitter
2. Echo & Singing
3. Crosstalk
4. Distortion
5. Noise
6. Bandwidth
7. Number of Receivers

Types of Network

1. LAN
2. MAN
3. WAN

Wireless Media

1. Infrared
   a) Short Distance (TV Remote, Wireless Keyboard etc.)
2. Microwaves
   a) Mobile Phones, Wireless LANs (Wi-Fi), F.M. Radio etc.
3. Satellite
   a) Weather detection, GPS (Ground Positioning System, Broadcasting, Earth Observation System etc.)

Communication System

- Process of exchanging messages between sender and receiver through any given chhanel using required protocol.
- The sender transmits the data and the receiver receives it

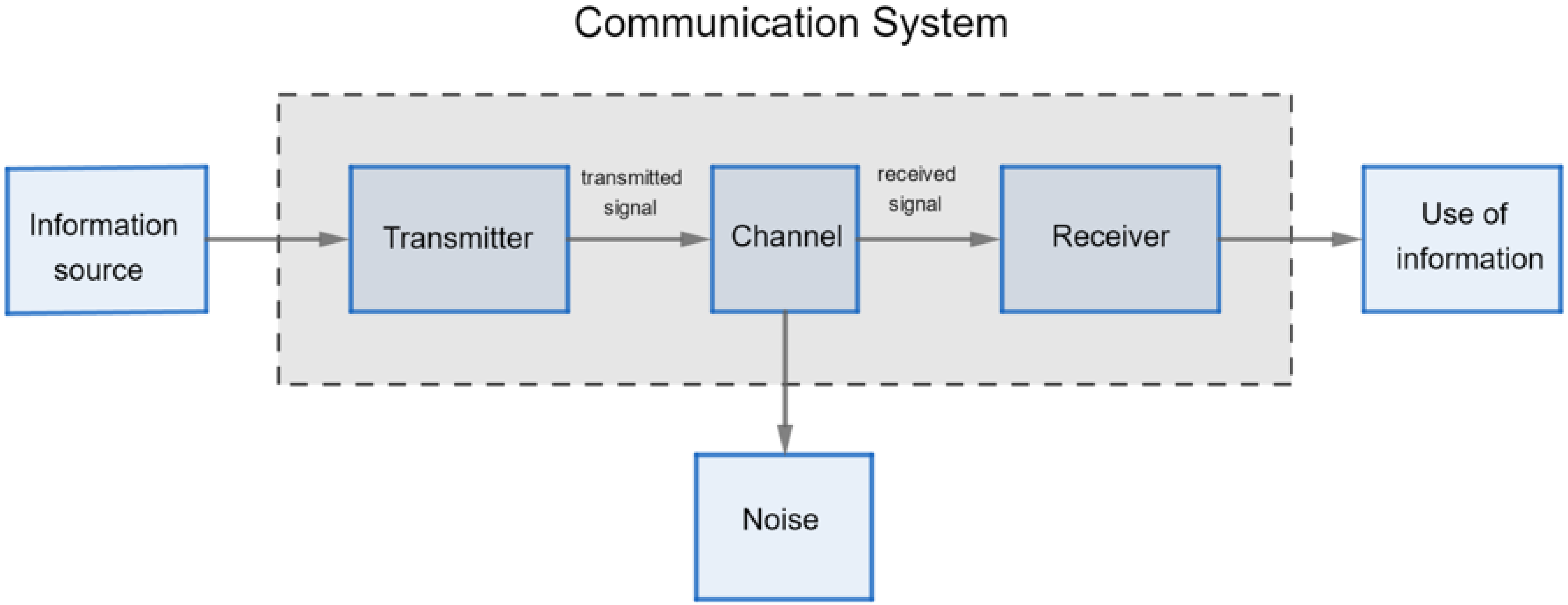

Communication System

Figure: Block Diagram of Communication System

Element of Data Communication

❑ Data

It is the message which is exchanged during communication.

❑ Transmitter

It is the source from where the message is transmitted.

❑ Receiver

It is the destination where the message is sent.

❑ Transmission Media

It is a channel through which data and information are exchanged between sender and receiver.

❑ Noise

Noise is an unwanted signal which interferes with the original message signal

❑ Protocol

It is the rule which guides communication.

Computer Network

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

Advantages /Purpose/ Merits/ Benefits of Networking

- ❑ Sharing devices such as printers, scanners etc. saves money.
- ❑ Site (software) licenses are likely to be cheaper than buying several standalone licenses.
- ❑ Files can easily be shared between users.
- ❑ Network users can communicate by email and instant messenger.
- ❑ Security is good - users cannot see other users' files unlike on stand-alone machines.
- ❑ Data is easy to backup as all the data is stored on the file server.
- ❑ The networks provide centralized control and management.
- ❑ The network allows people to easily access their files from any computer throughout the network.
- ❑ Workgroup software (such as Microsoft Office) allows many users to work on a document or project concurrently..

Disadvantages of Networking

- ❑ Purchasing the network cabling and file servers can be expensive.
- ❑ The network itself is difficult to establish, manage and operate.
- ❑ Skilled manpower is required to establish, maintain and operate a networking system.
- ❑ If the file server breaks down the files on the file server become inaccessible.
- ❑ Viruses can spread to other computers throughout a computer network.
- ❑ There is a danger of hacking, mostly with wide area networks.

Communication Mode

- ❑ Communication mode defines the direction of data flow in the communication system.
- ❑ Types of communication mode: Simplex, Half-duplex and Full duplex (Duplex)

1) Simplex

- ❑ The flow of data signal in simplex mode of communication is unidirectional.
- ❑ Only one of two devices on a link can transmit data and the other can receive.
- ❑ It is just like a one way street.
- ❑ Example: communication between keyboard and CPU, Radio and TV broadcasting etc. are Simplex modes of communication.

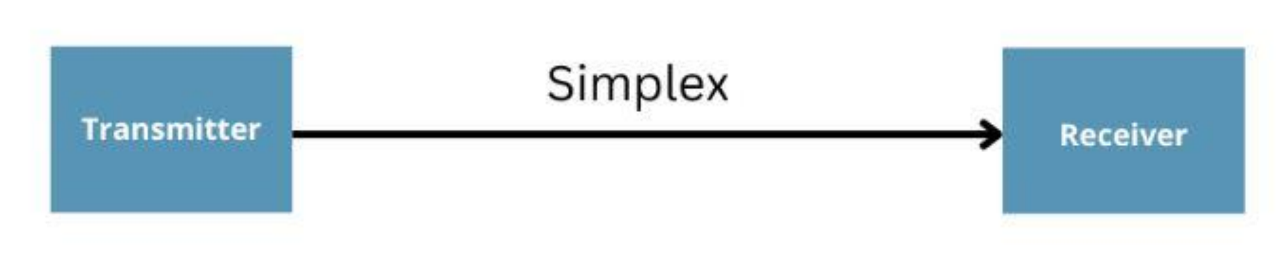


Figure: Simplex Communication Flow

2) Half Duplex

- The flow of data signal in half duplex mode of communication is bidirectional but both devices cannot receive and transmit data at the same time.
- When one device is sending the other can only receive and vice versa.
- Example: communication between walkies-talkie.

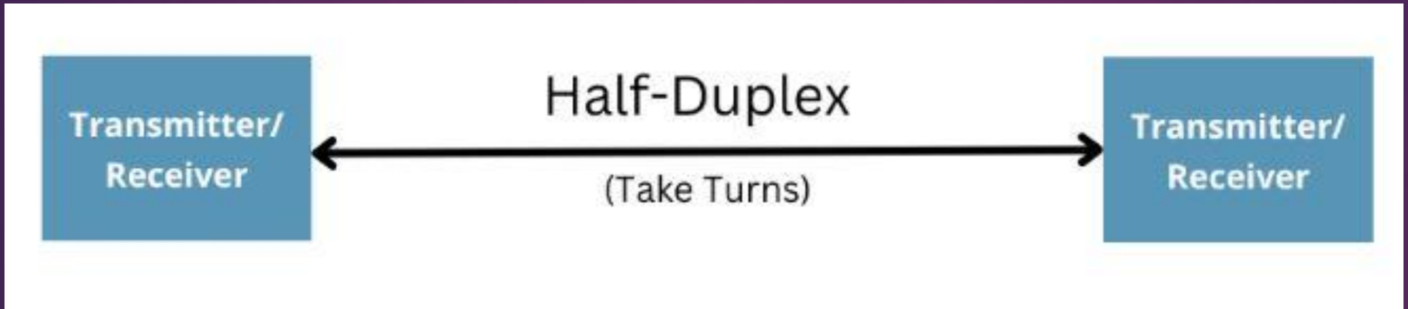


Figure: Half Duplex Communication Flow

3) Full Duplex

- ❑ It is also known as Duplex Mode.
- ❑ The flow of data signal in full duplex mode of communication is bidirectional.
- ❑ Both devices can receive and transmit data at the same time.
- ❑ It is just like a two way street with traffic flowing in both directions at the same time.
- ❑ Example: Communication in Telephone, Cell Phones etc.

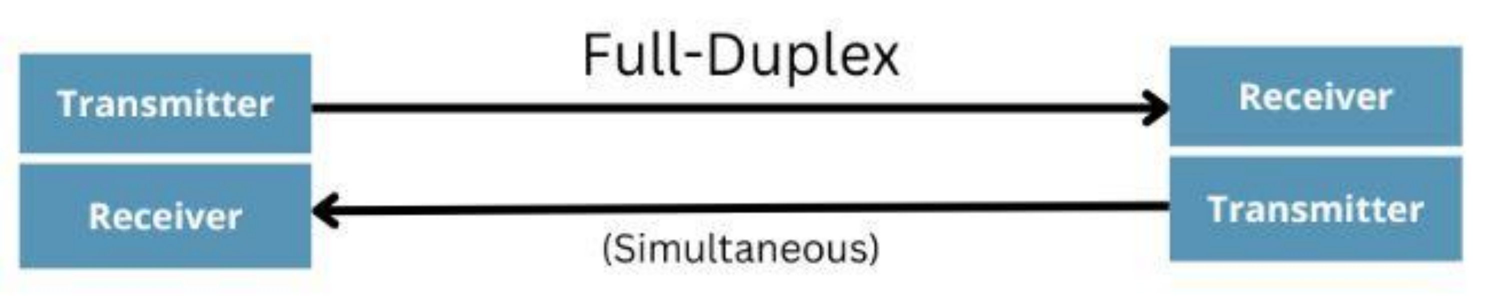


Figure: Full Duplex Communication Flow

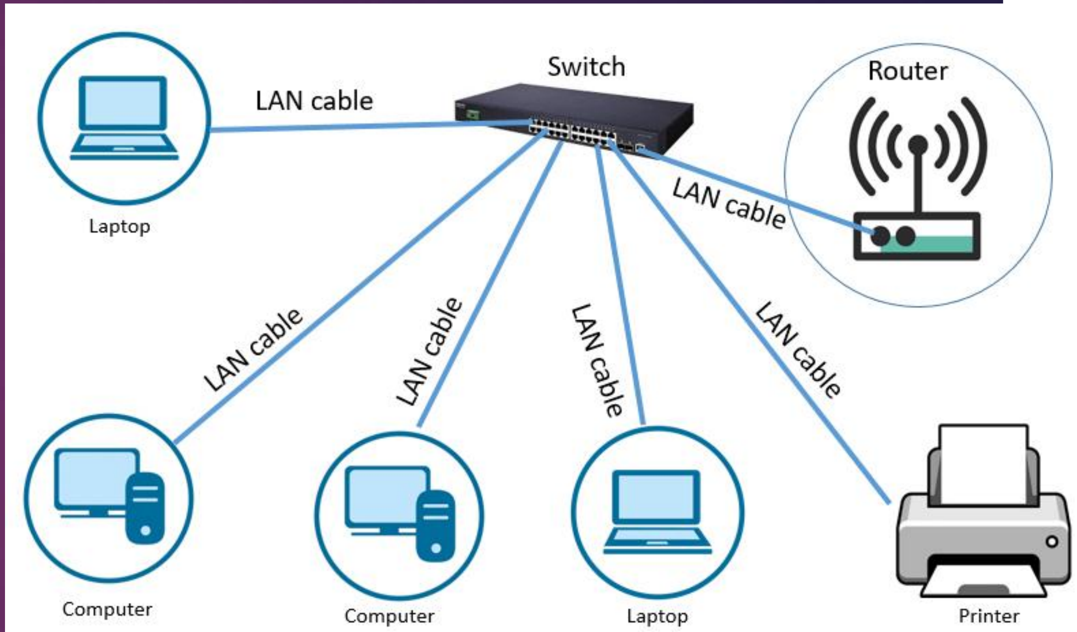
Concept of LAN, MAN and WAN

❑ Based on geographical area coverage; the computer network is classified into three basic types, which include:

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

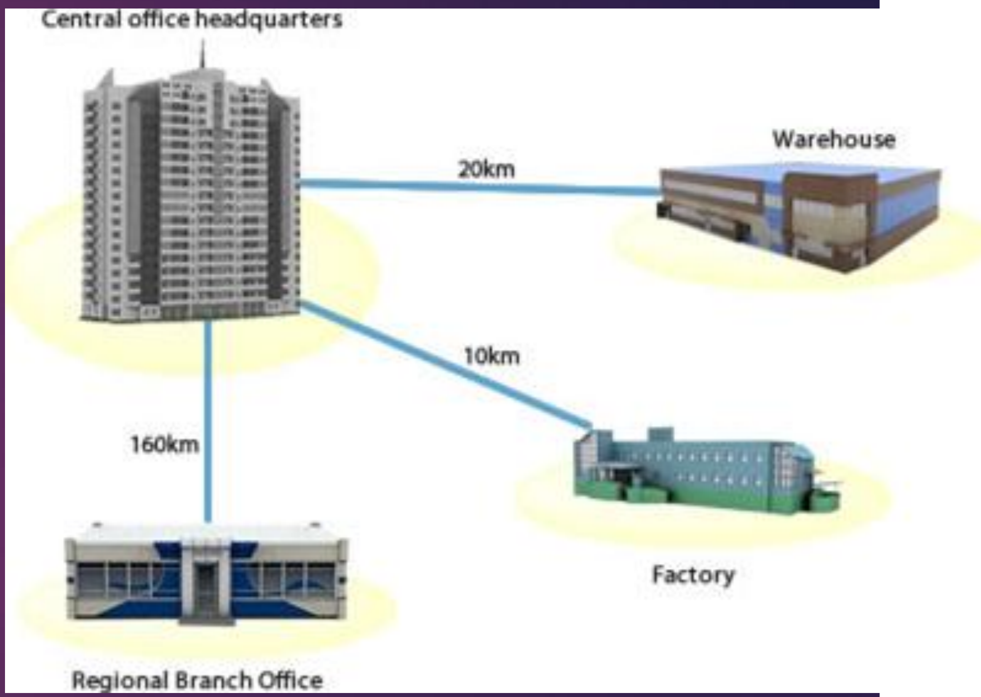
Local Area Network (LAN)

- ❑ A network that is limited to a small area such as a room, a building or a school is called Local Area Network (LAN).
- ❑ We can use a large number of computers in a LAN.
- ❑ It is a simple, cheap and high secured network.
- ❑ We can create a LAN by using cable or wireless media.
- ❑ It has a high speed data transfer rate 100Mbps (Megabits per Second)
- ❑ It has Low error rate 1000 times lower than WAN.
- ❑ Common example of LAN is the network in our college.



Metropolitan Area Network (MAN)

- ❑ A Metropolitan Area Network (MAN) is larger than LAN and smaller than WAN.
- ❑ It covers a larger geographical area such as: a university, a bank, an entire city, a whole country.
- ❑ A metropolitan area network (MAN) can be either a public or privately owned network.
- ❑ It is an expensive, complex, and less secured network than LAN.
- ❑ It has lower data transfer rate 10Mbps.
- ❑ It has low error rate 100 times lower than WAN.
- ❑ Common examples of MAN are Cable TV Network, Internet Service Provider (ISP) in a city etc.



Wide Area Network (WAN)

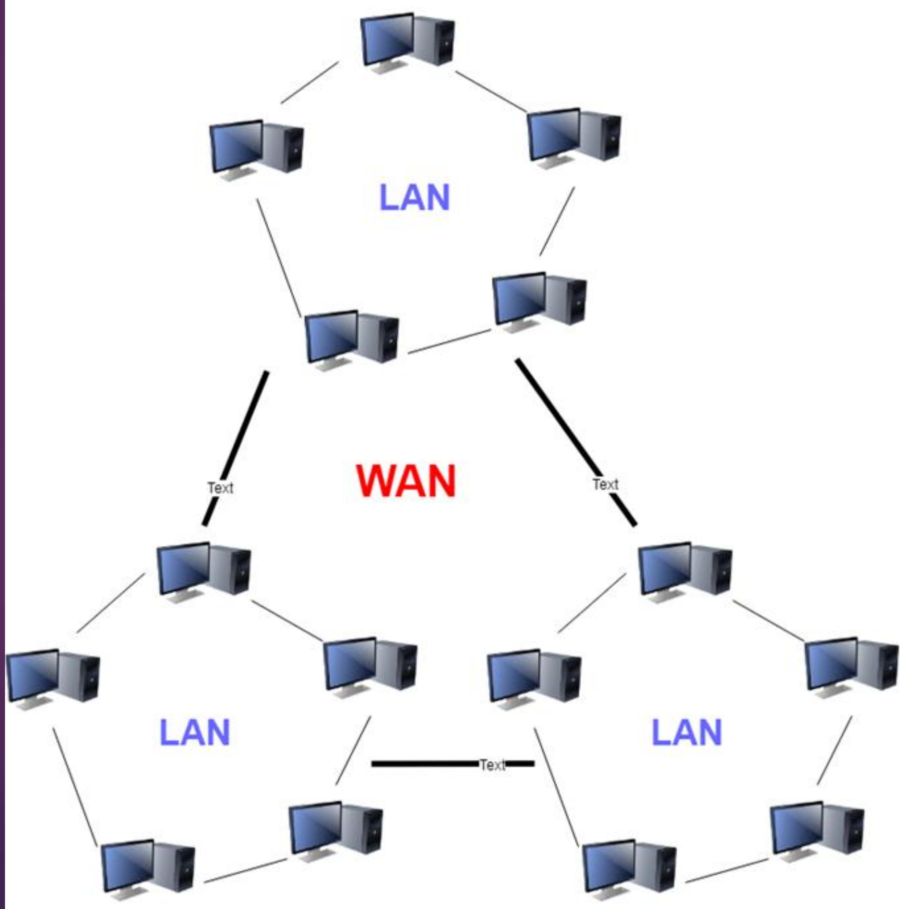
❑ The communication networks, which cover large geographical (whole world) areas, are called Wide Area Networks.

❑ It is also known as Long Haul Networks (LHNs).

❑ It often connects multiple smaller networks, such as local area networks (LANs) or metropolitan area networks (MANs).

❑ It is the most expensive and most complex type of network.

❑ The Internet is an example of WAN.



Difference among LAN, MAN and WAN:

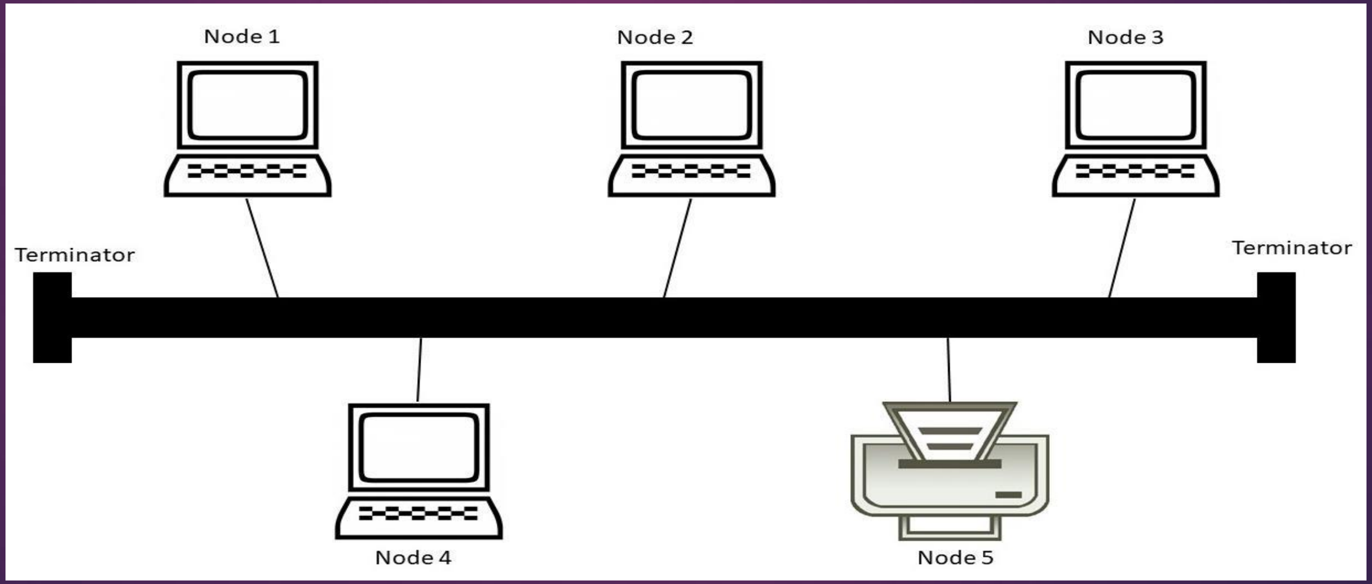
LAN	MAN	WAN
LAN stands for Local Area Network.	MAN stands for Metropolitan Area Network.	WAN stands for Wide Area Network.
It is used for building like Office.	It is used for City like Pokhara.	It is used for Countries.
Transmission speed of data is high.	Transmission speed of data is average.	Transmission speed of data is low.
Range: Short	Range: Average	Range: Wide
LAN network ownership is private.	MAN network ownership is private or public.	WAN network ownership is private or public.
Easy to maintain.	Difficult to maintain than LAN.	Difficult to maintain than MAN as well as LAN.
LAN network error rate is low.	MAN network error rate is average.	WAN network error rate is high.
LAN setup cost is low.	MAN setup cost is high.	WAN setup cost is very high.

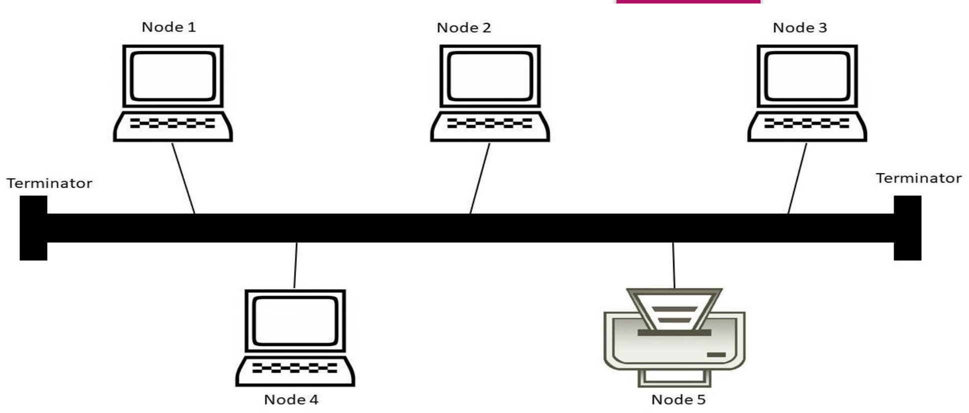
Network Topologies

- ❑ Topology defines the structure of the network of how all the components are interconnected to each other.
- ❑ The main objective of the network topology is to find out the most economical and efficient way of transmission channel.
- ❑ The most common LAN topologies are Bus Topology, Star Topology, Ring Topology, Tree Topology, Mesh Topology and Hybrid Topology.

Bus Topology

- ❑ Bus Topology is also known as linear topology.
- ❑ It is a topology for a Local Area Network in which all the nodes are connected to a single backbone cable.
- ❑ The backbone cable to which the nodes are connected is called a bus or trunk.





Advantages:

❑ Easy to setup network

❑ It is inexpensive topology.

❑ If any node in the network downs, then it does not affect other nodes.

❑The length of cable required is less than a star topology.

❑ It is more flexible because we can easily connect and disconnect any number of nodes in the bus.

Disadvantages:

❑ Entire network shuts down if there is a break in the main cable.

❑ It is very difficult to find out the fault in the bus.

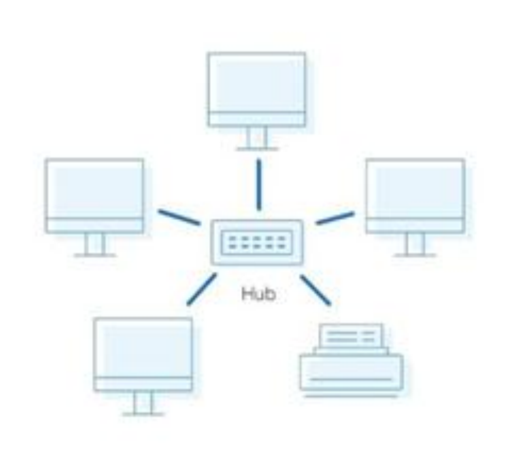
❑Bus topology is not good for large networks.

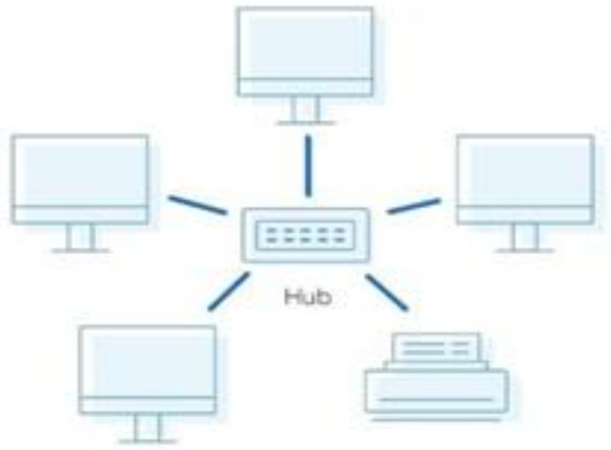
❑ Data traffic is very high.

❑ Adding nodes to the network would slow down the network.

Star Topology

- ❑ Nodes in the network are connected to each other with the help of a central connecting device hub or switch or server.
- ❑ It is based on client server architecture.
- ❑ The communication is done through the central server with the help of a hub or switch in the entire network..
- ❑ It is the most popular and widely used topology for LAN.





Advantages:

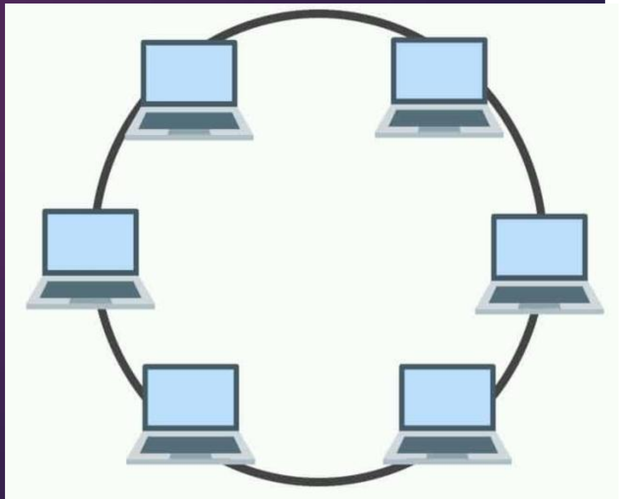
- ❑ Centralized control.
- ❑ Easy fault detection because the links are often easily identified.
- ❑ If a node fails, it will not affect other nodes.
- ❑ It is high-performing as no data collisions can occur/
- ❑ In star topology, adding, removing and more the nodes are easy.

Disadvantages:

- ❑ If the hub fails, attached nodes are disabled.
- ❑ The installation of star topology is costly.
- ❑ Performance depends on the hub’s capacity.

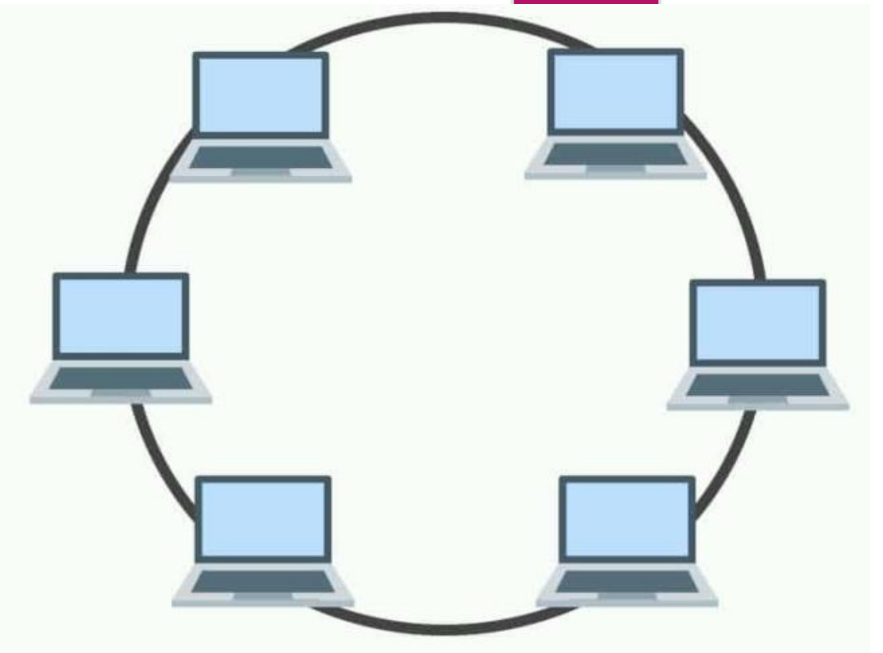
Ring Topology

- ❑ Nodes are interconnected to each other by making a closed circular structure.
- ❑ It is based on peer to peer network architecture.
- ❑ Communication is done in a single direction only.
- ❑ In this topology one node receives the message, then it compares the destination address of the message and its own address, if it matches then it accepts the message otherwise the message is retransmitted to the next node in the network.



Advantages:

- There is no server so each node has equal access facilities.
- Requires less wire.
- Easy Installation.
- It is cheap to install and expand.
- In this data flows in one direction which reduces the chance



Disadvantages:

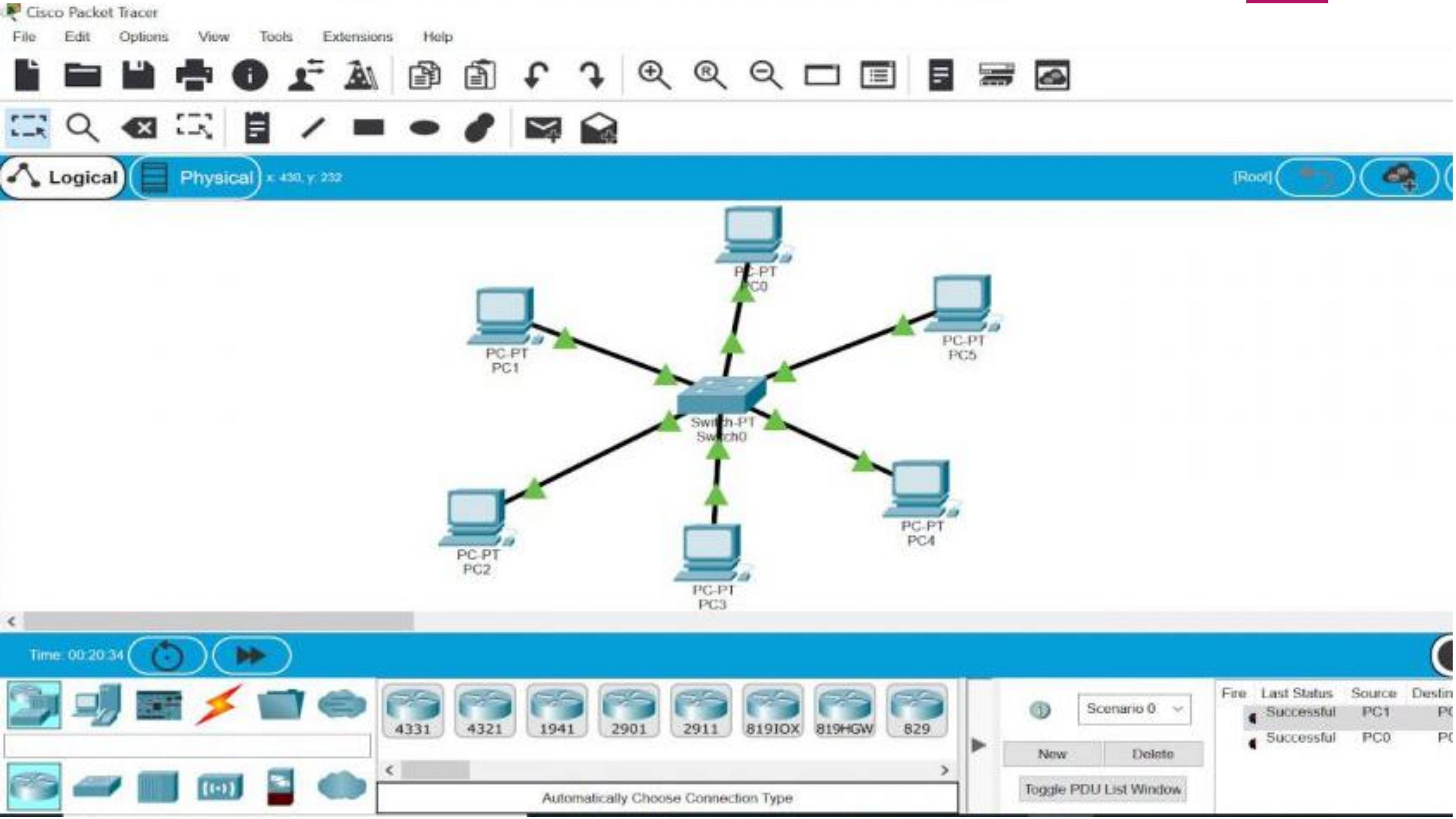
- It is difficult to add and remove new nodes.
- It is very difficult to find out the errors in the network.
- If there is a problem in any node or connection then the entire network goes down.
- Slow data transmission speed.

Network Tools

Packet Tracer

Packet Tracer is a tool built by Cisco System. It is a cross-platform, visual, innovative and powerful network simulation tool that can be used for a practice build own network with routers, switches, wireless and much more. It provides Drag and Drop GUI Interface.

Cisco Packet Tracer provides a simulated network environment where users experiment with different network topologies, protocols, and configurations without risking damage to physical equipment or the network



Fire	Last Status	Source	Destin
●	Successful	PC1	PC
●	Successful	PC0	PC

Network Tools

Remote Login

Remote Login is a process in which user can login into remote site i.e. computer and use services that are available on the remote computer. With the help of remote login a user is able to understand result of transferring and result of processing from the remote computer to the local computer.. Popular Remote Login Tools are: Any Desk, TeamViewer, Chrome Remote Desktop, GoToMyPC etc.

Advantages of Remote Login:

- Successful Troubleshooting from Remote Locations
- Remote Access Makes Collaboration Easy
- Cost Saving
- Monitor your network from Anywhere
- Faster Tracking & Detection

Disadvantages of Remote Login:

- Security Issues
- Version Problems
- Hardware Issues Still Need On – Site Work

Network Connecting Devices

NIC

Network Interface Card (NIC) is a hardware component that is present on the computer. It is used to connect different networking devices such as computers and servers to share data over the connected network.

USB NIC

Wireless NIC for Laptop

Wireless NIC for Desktop

Wired NIC

Network Connecting Devices

MODEM

The word MODEM stands for Modulator and Demodulator. It is a hardware device that allows a computer to send and receive information over telephone lines. . In another word, Modem translates data from binary codes to analog data that can be transmitted over the telephone network and translates analog data into binary codes.

Network Connecting Devices

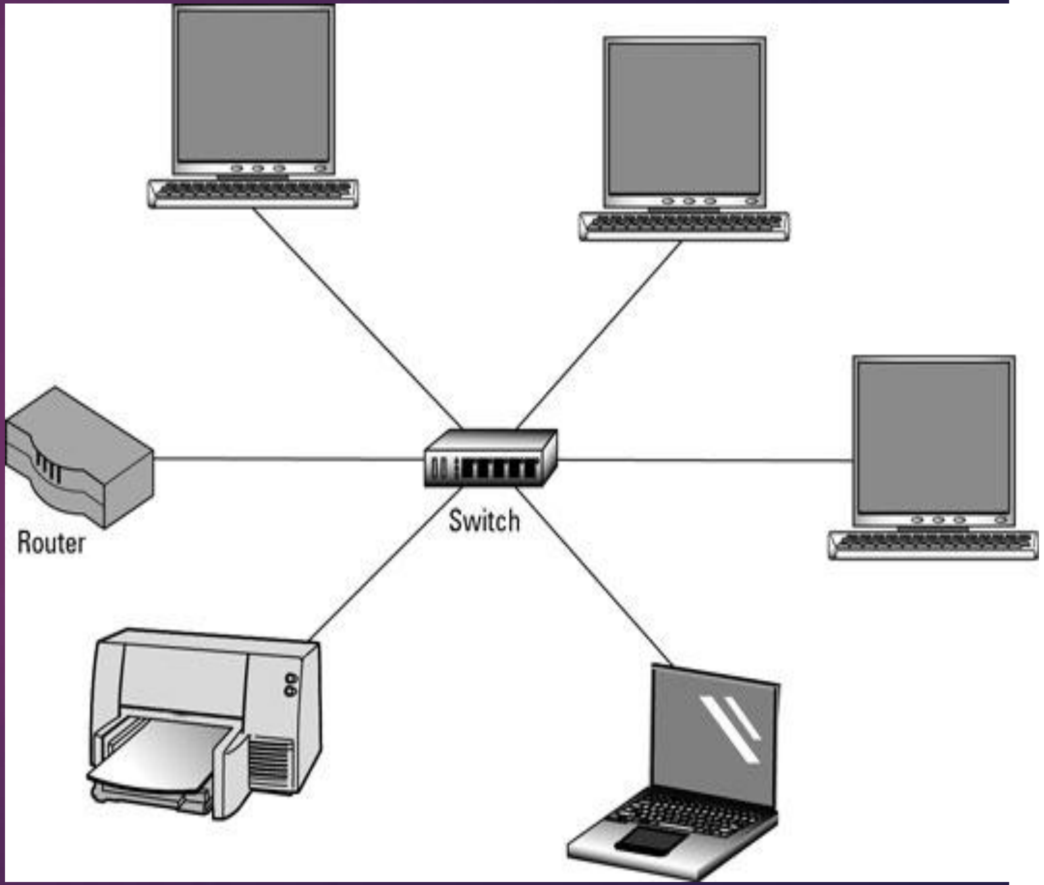
ROUTER

The router is a physical device that is designed to receive, analyze, and forward data packets between computer networks.

Network Connecting Devices

SWITCH

A network switch connects devices (such as computers, printers, and wireless access points) in a network to each other, and allows them to 'talk' by exchanging data packets. It is also known as an intelligent hub.



Transmission Impairments Terminology

The quality of the signal at the beginning of the medium is not the same as the signal at the end of the medium. The various factors which decrease the quality of signals are called impairments. Some of the transmission impairments terminologies are: Attenuation, Jitter, Echo and Singing, Crosstalk, Distortion, Noise, Bandwidth, Number of receivers.

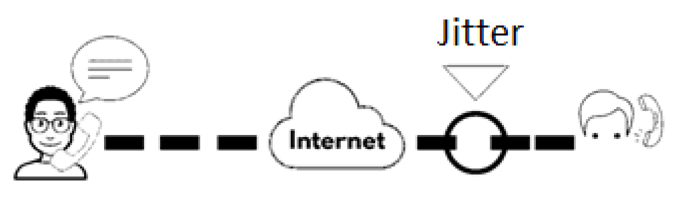
Transmission Impairments Terminology

Attenuation

Attenuation is the loss of signal strength in networking connections. It is measured in decibels (dB). Example: Attenuation due to rain, clouds can lead to the worries of the wireless, mobile, satellite and other communication.

Jitter

Jitter is the difference in time delay in milliseconds (ms) between data packets over a network, i.e. the delay between when a signal is transmitted and when it is received.



Transmission Impairments Terminology

Crosstalk

Crosstalk is an unwanted signal in a communication channel such as in a telephone, radio, or computer which is caused by transference of energy from another device as by leakage. It occurs when one voice device picks up the signal from another circuit making the conversation jumping from wire pair to the other.

Distortion

The change in original transmitted signal waveform is known as distortion. Due to distortion, the receiver does not receive the original signal rather a distorted signal is received. This reduces quality of communication and is one of the reasons for network impairments.

Transmission Impairments Terminology

Noise

The random or unwanted signal that mixes up with the original signal is called Noise. Noise can decrease transmission strength and disturb overall communication efficiency.

Echo and Singing

When the signal from the source is sent to the destination and somehow there is any link from destination to source may be partially or fully then the signal repeats itself. This repetition of the signal after the certain time delay is known as Echo. Singing may be regarded as echo that is completely out of control.

Transmission Impairments Terminology

Bandwidth

The rate of data transmission in a given medium per unit time is known as bandwidth. It is generally measured in terms of bps, Kbps, Mbps etc. Higher the bandwidth, higher will be the data transmission and faster will be the communication. But if bandwidth is low then it leads to network congestion causing network impairments.

Number of receivers

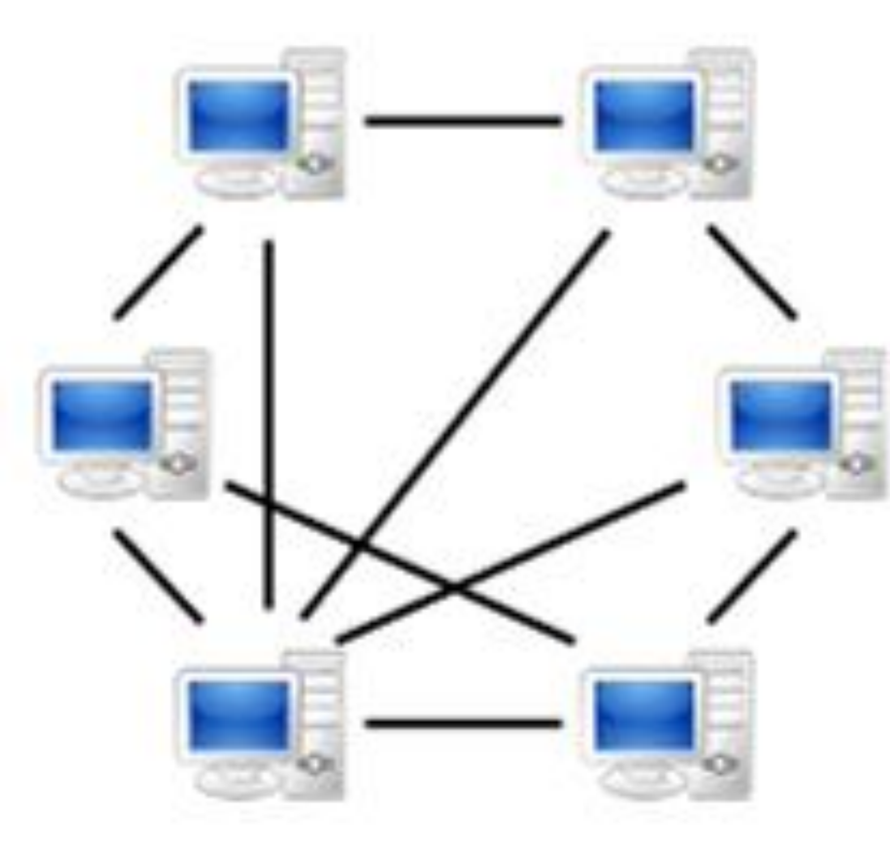
It is concerned with the number of users or destination points where data is received. The greater the number of devices on a network, the more chance of a collision.

Networks Architecture:

- ❑ Network architecture means network layout that tells us how computers are organized and how task are allocated to the computer.
- ❑ Types of network architecture:
    - ❑ Peer to Peer Architecture
    - ❑ Client Server Architecture

Peer to Peer Architecture

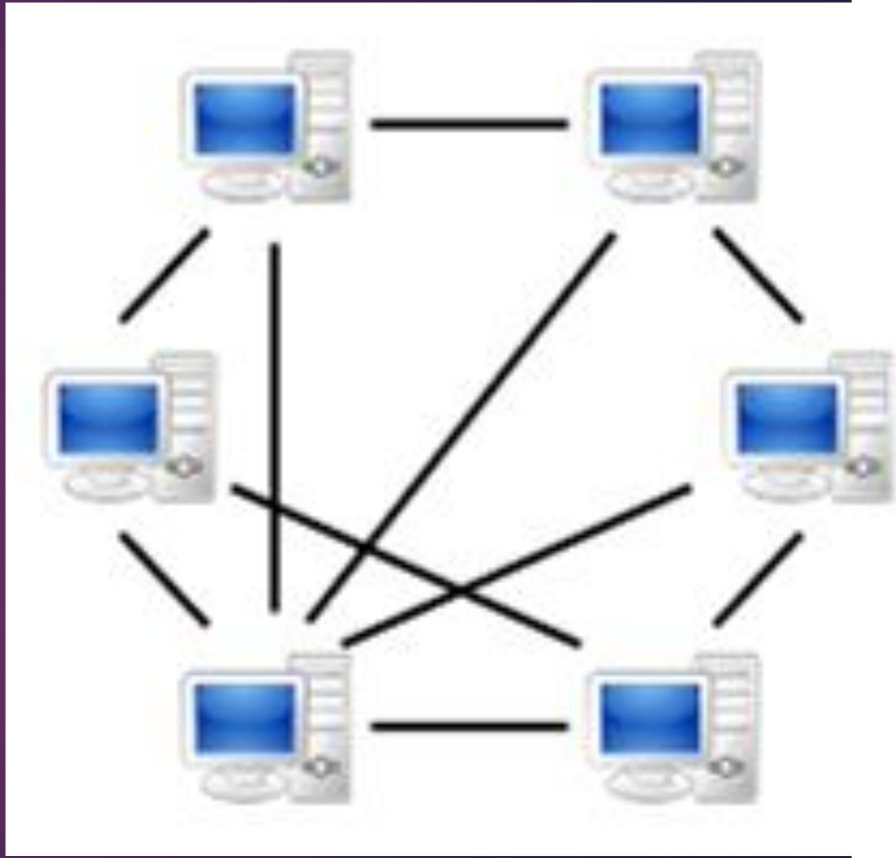
- ❑ It is also known as Point to Point network.
- ❑ In this architecture, each computer can have equal capabilities and responsibilities in a network.
- ❑ There is no server, each workstation acts like a server as well as client.
- ❑ It is a simpler and inexpensive architecture than client server architecture.
- ❑ It is suitable for small sized private owned networks such as personal networks in home, school Cyber cafe.



Peer to Peer Architecture

Advantages:

- ❑ It is a cheaper network, as it has no server.
- ❑ If one computer stops working it will have no effect on the other computers.

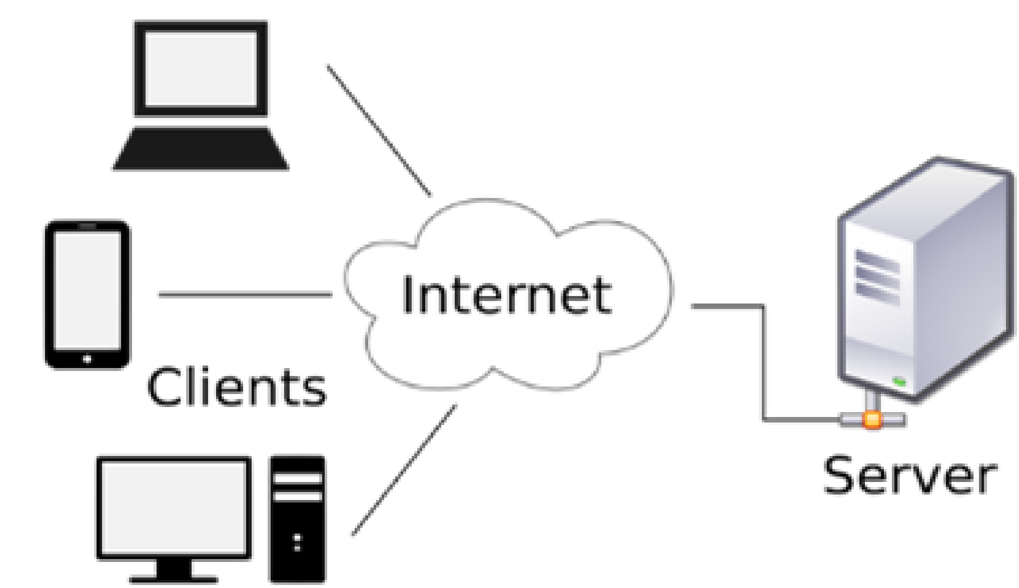


Disadvantages:

- ❑ Security Issues
- ❑ We cannot backup the data because there is no server in this network.

Client-Server Architecture

- ❑ It is also known as Request Response Architecture
- ❑ In this architecture, there are two types of computers, one is server and the other is client.
- ❑ Server is the main computer in a network that controls, manages and provides various services to the clients. Server is a very high performance computer and it is expensive too.
- ❑ A client is a normal computer that is connected to a server. Client requests to the server and the server response for the respective services.
- ❑ Network resources are centralized to the server so all the network activities such as data storage, data processing, data transfer etc. are carried out via server.



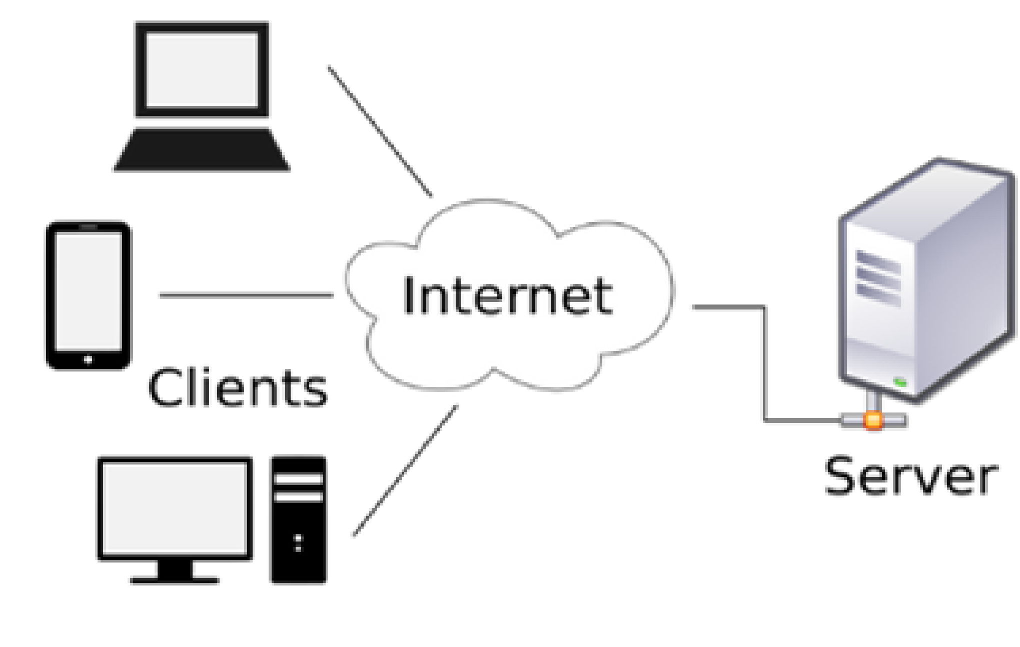
Client Server Architecture

Advantages:

- ❑ It has a centralized system. from which data can be easily backed up
- ❑ Security is better in this network.

Disadvantages:

- ❑ In case of server failure entire network will be failed.
- ❑ Server maintenance cost is high.



Transmission Medium/ Communication Medium

Transmission medium is a communication channel that is used to carry the data from the transmitter to the receiver. Transmission Media is broadly classified into the following types:

1) Guided Media
   a) Twisted Pair Cable
   b) Coaxial Cable
   c) Optical Fiber Cable
2) Unguided Media
   a) Microwave
   b) Satellite
   c) Infrared

Guided Media

❑ Guided transmission media is also known as Bounded or Wired Transmission media.

❑ It uses a “cabling” system that guides the data signals along a specific path.

❑ The most common guided media are:

a) Twisted Pair Cable

i. Unshielded Twisted Pair (UTP)

ii. Shielded Twisted Pair (STP)

b) Coaxial Cable

c) Optical Fiber Cable

Twisted Pair Cable

- ❑ Twisted pair cable is the oldest and most commonly used transmission media.
- ❑ It is made from a pair of copper wires twisted to each other and finally surrounded by an outer insulating jacket.
- ❑ The twisted pair cable is connected with the help of RJ-45 connector (for LAN) or Registered Jack (RJ)-11 connector (for Telephone).
- ❑ It is available in two forms:
  a) Unshielded Twisted Pair (UTP)
  b) Shielded Twisted Pair (STP

Twisted Pair Cable

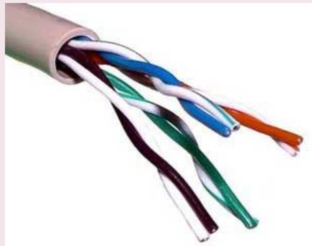
Advantages:

- ❑ It is light and thin, so it is more flexible to fit on a LAN.
- ❑ It is cheaper than other cables.
- ❑ It can transmit data at a higher bandwidth for a short distance
- ❑ It’s relatively easy to implement and terminate.
- ❑ Twisted Pair cable is easy to connect.

Disadvantages:

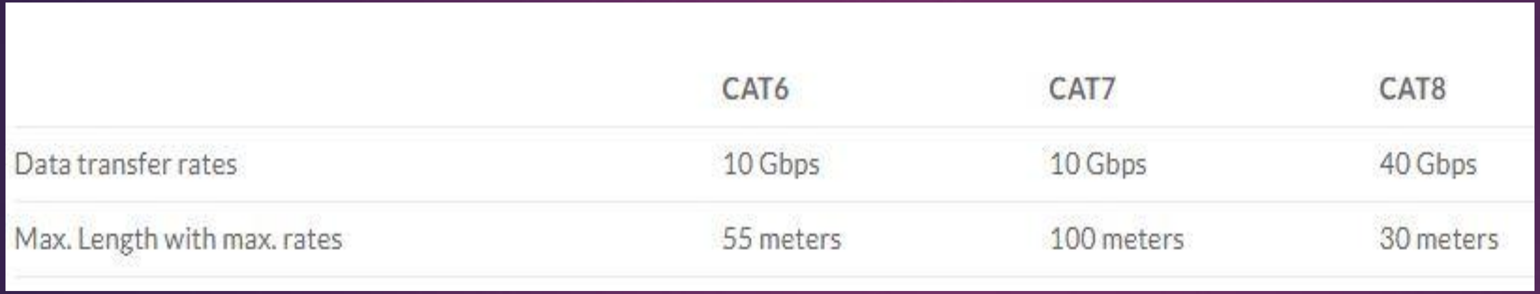
- ❑ It cannot be used for long distance transmission.
- ❑ It is slower for data transmission than other cables.
- ❑ It provides poor security.
- ❑ As they a thin so can be easily breakable.
- ❑ Low durability (must be maintained regularly).

Twisted Pair Cable

UTP	STP
It stands for Unshielded Twisted Pair.	It stands for Shielded Twisted Pair.
It is the most common twisted pair.	It is rarely used.
It cannot carry data signals for longer distances compared to STP.	It can carry data signals for longer distances.
It is cheaper.	It is expensive.
It is Lighter than STP.	It is Heavier than UTP.
UTP cable has lower bandwidth maximum up to 10Mbps.	STP cable has more bandwidth 100Mbps up to 1000 Mbps.
Figure: 	Figure:

CAT

- CAT stands “category"
- It is also called network, LAN or Ethernet cables.
- It is used to connect computer network devices such as routers, computers, servers and switches.



	CAT6	CAT7	CAT8
Data transfer rates	10 Gbps	10 Gbps	40 Gbps
Max. Length with max. rates	55 meters	100 meters	30 meters

TWisted pair Cabling

Straight Through Cabling

(Switch to router, switch to PC, switch to server, Hub to PC, Hub to server)

T568A

Residential purpose

Set 1	Set 2
Green white	Green White
Green	Green
orange white	Orange white
Blue	Blue
Blue White	Blue White
Orange	Orange
BrownWhite	BrownWhite
Brown	Brown

Set 1 ↔ Set 2

T568B

Business purpose

Set 1	Set 2
Orange White	Orange White
Orange	Orange
Green White	Green White
Blue	Blue
Blue White	Blue White
Green	Green
Brown White	Brown White
Brown	Brown

Set 1 ↔ Set 2

Crossover Cabling

(Switch to switch, Switch to Hub, Hub to Hub, router to router, router to PC, PC to PC)

Set 1	Set 2
Orange white	Green white
Orange	Green
Green white	Orange white
Blue	Blue
Blue white	Blue white
Green	Orange
Brown white	Brown white
Brown	Brown

Note ►

Orange white Orange	Transmit Data	Green white Green	Received Data

Coaxial Cable

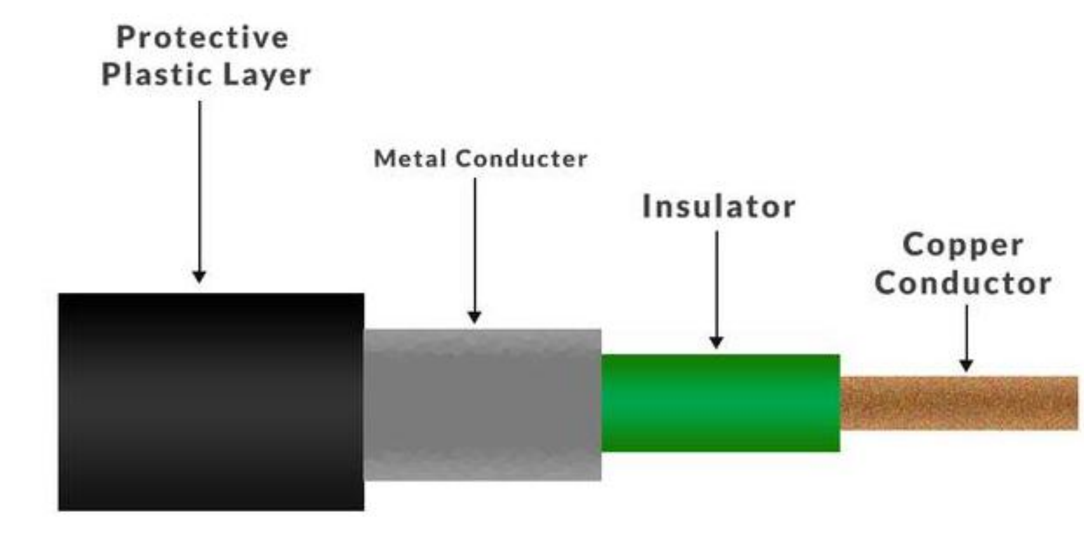
- ❑ Coaxial Cable is also known as coax.
- ❑ It consists of two conductors. They are Metal Conductor and Copper Conductor.
- ❑ The inner copper conductor is surrounded by an insulator, Metal Conductor again surrounded by PVL (Protective Plastic Layer)
- ❑ It is commonly used in cable TV and CCTV at home, school.
- ❑ There are two types of coaxial cable:

  a) Thin Coax

  - It is also known as thinnet
  - 10mbps speed up to 200 meters.

  b) Thick Coax

  - It is also known as thicknet
  - 10mbps speed up to 500 meters.



Coaxial Cable

Advantages:

❑ Coaxial cables support high bandwidth.

❑ It is easy to install coaxial cables.

❑ Less affected by noise.

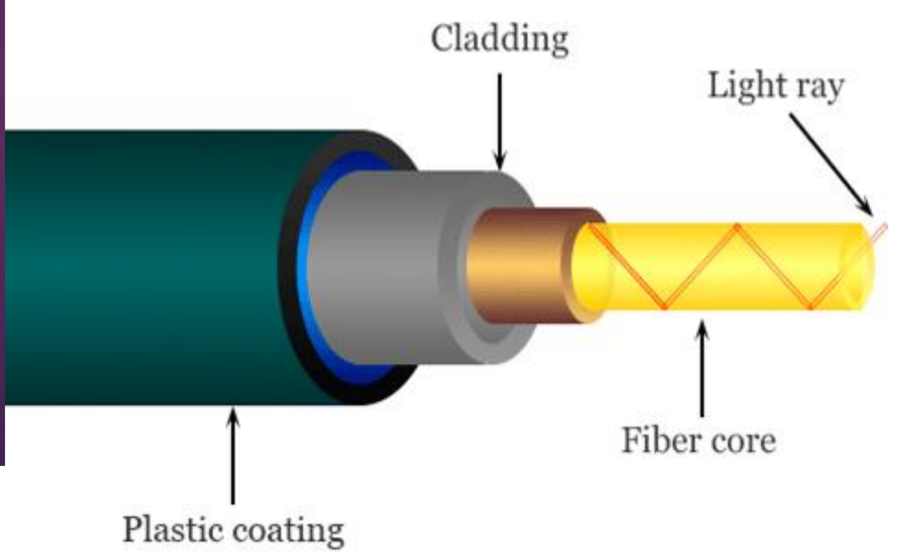
Disadvantages:

❑ Difficult to install compared to twisted pair cable.

❑ It is expensive to install.

Optical Fiber Cable

- ❑ Optical fiber cable is made up of glass or plastic that transmits signals in the form of light.
- ❑ The core in fiber transmitted light signals and cladding guided the light within the core.
- ❑ Optical fiber which is slightly thicker than that of human hair.
- ❑ It is about 10 times faster than coaxial cable and 200 times faster than twisted pair cable.
- ❑ Fiber optics is used for long-distance and high-performance data networking. It is also commonly used in telecommunication services, such as internet, television and telephones.
- ❑ This cable is connected with the help of an S-T connector.



Optical Fiber Cable

Advantages:

- ❑ It is much thinner and lighter than the others.
- ❑ It provides the fastest data transmission then other transmission media.
- ❑ It can be used for both short and long distance transmission.
- ❑ It provides error free and highly secured transmission.

Disadvantages:

- ❑ Difficult to install.
- ❑ It is highly expensive to install.
- ❑ Skilled technical manpower is required to install.

Transmission Media	**Connectors Used**	**Figure**
Twisted Pair Wire	RJ (Registered Jack) 45	
Coaxial Cable	BNC (Bayonet Neill–Concelman) Connector	
Optical Fiber	Standard Connector (SC)	

Unguided Media

- ❑ Guided transmission media is also known as Unbounded or Wireless Transmission media.
- ❑ Transmission media which do not use any physical connection between two communicating devices
- ❑ The most common guided media are:
  a) Microwave
  b) Satellite
  c) Infrared

Microwave

- ❑High frequency electromagnetic waves are known as Microwaves.
- ❑It cannot bend and pass obstacles like hills or buildings so it requires line of sight transmission.
- ❑The line of sight is only 50 kilometers to the horizon.
- ❑Common examples of microwave frequencies are:
  - ○ Long distance telephone communication
  - ○ Cellular Phones
  - ○ Television Networks
  - ○ Wireless LAN

Microwave

Advantages:

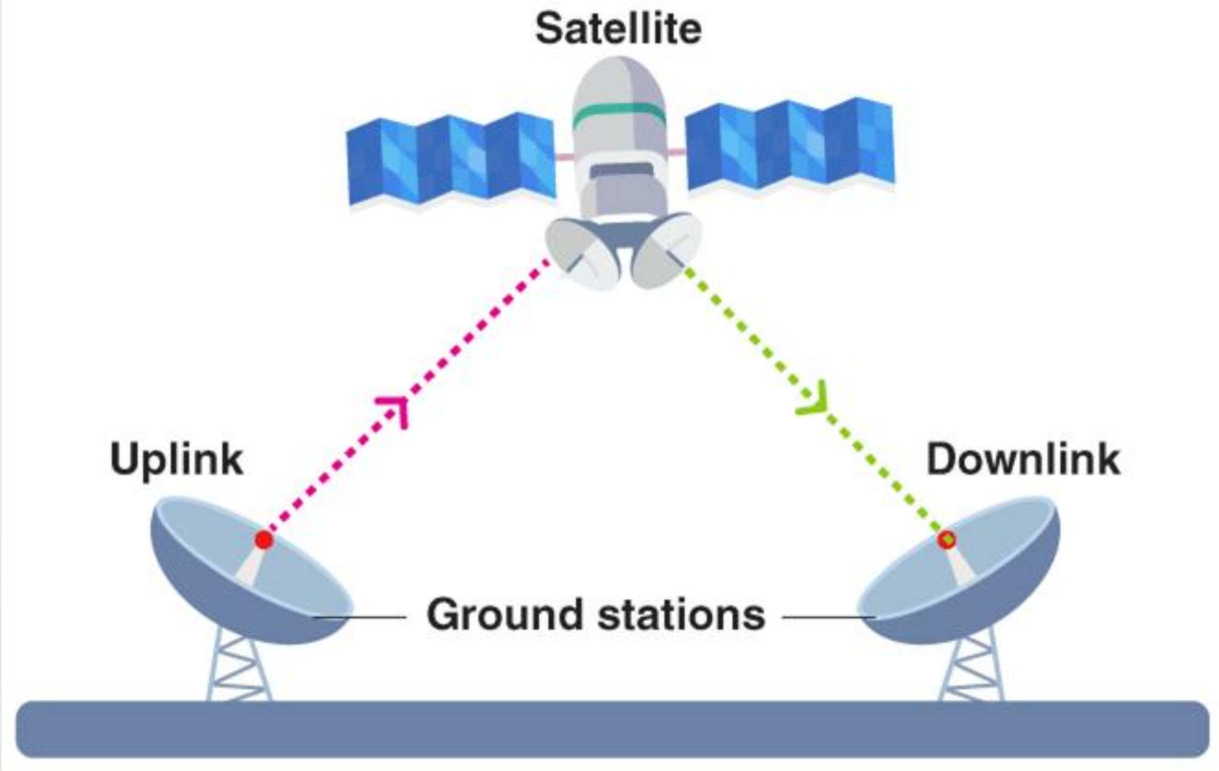
- ❑ It has a higher bandwidth than radio waves.
- ❑ The quality of data transmission is better than radio waves.
- ❑ It can carry 2500 voice channels at the same time.

Disadvantages:

- ❑ It cannot bend and pass obstacles so require line of sight for data transmission.
- ❑ The transmission is affected by weather conditions like rain.

Satellite

- ❑A communications satellite is an artificial satellite.
- ❑Transmitter and a receiver at different locations on Earth.
- ❑The satellite is the repeater that orbits in space, which is 22000 miles above from the earth surface.



Satellite

Advantages:

- It covers all geographical areas of earth.
- It has higher bandwidth than radio or microwave data transmission.

Disadvantages:

- Installation of satellites is very expensive.
- Slower speeds than cable networks.

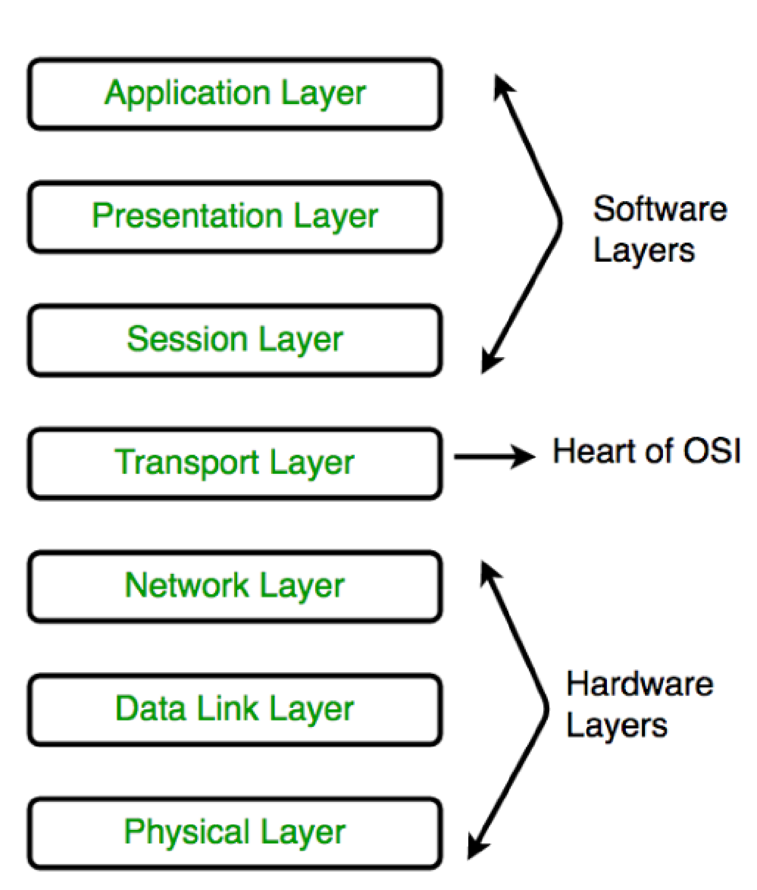
Infrared

- ❑ Infrared signals can be used for short-range communication in a closed area using line of sight communication.
- ❑ As infrared signals have a high frequency, they cannot penetrate the wall. So, it prevents interference from one system to another system.
- ❑ It is mainly used in wireless remote control, wireless mouse, wireless keyboard etc.

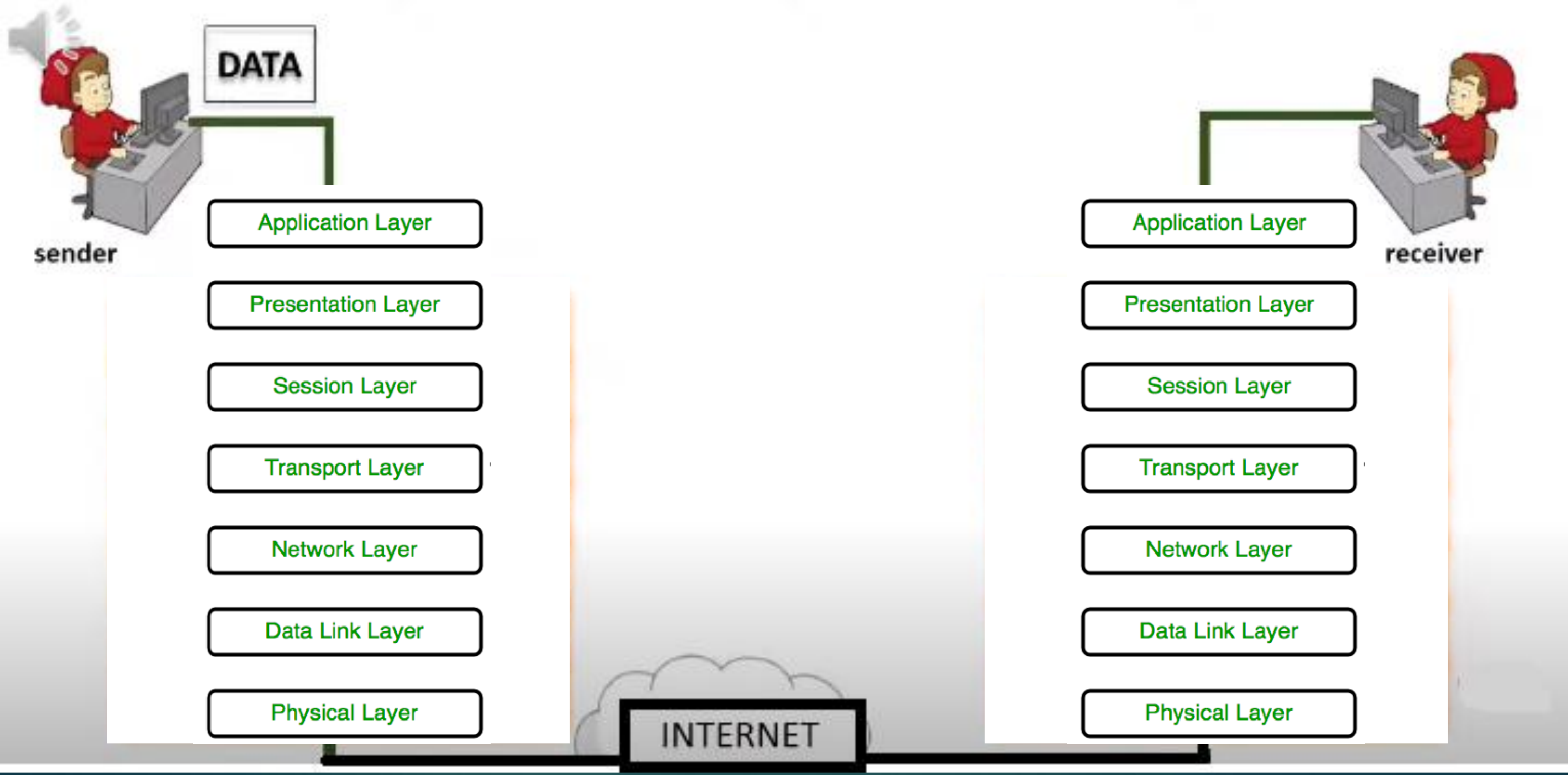
OSI Model

- ❑ OSI stands for Open System Interconnection.
- ❑ OSI model was developed by ISO (International Organization for Standardization) in 1984.
- ❑ Most of the network communication protocols are based on the OSI model.
- ❑ It is a 7 Layer architecture. They are:

  Physical layer, Data Link layer, Network layer, Transport layer, Session Layer, Presentation layer and Application layer.
- ❑ Physical, Data Link and Network layers are known as Hardware/ Lower Layers.
- ❑ Transport Layer is also known as Heart of OSI model.
- ❑ Session, Presentation and Application Layers are known as Software/ Upper Layers.



OSI Model



DATA

sender

receiver

Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

Data Link Layer

Physical Layer

Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

Data Link Layer

Physical Layer

INTERNET

This layer provides the services to the user.

It is responsible for translation and compression.

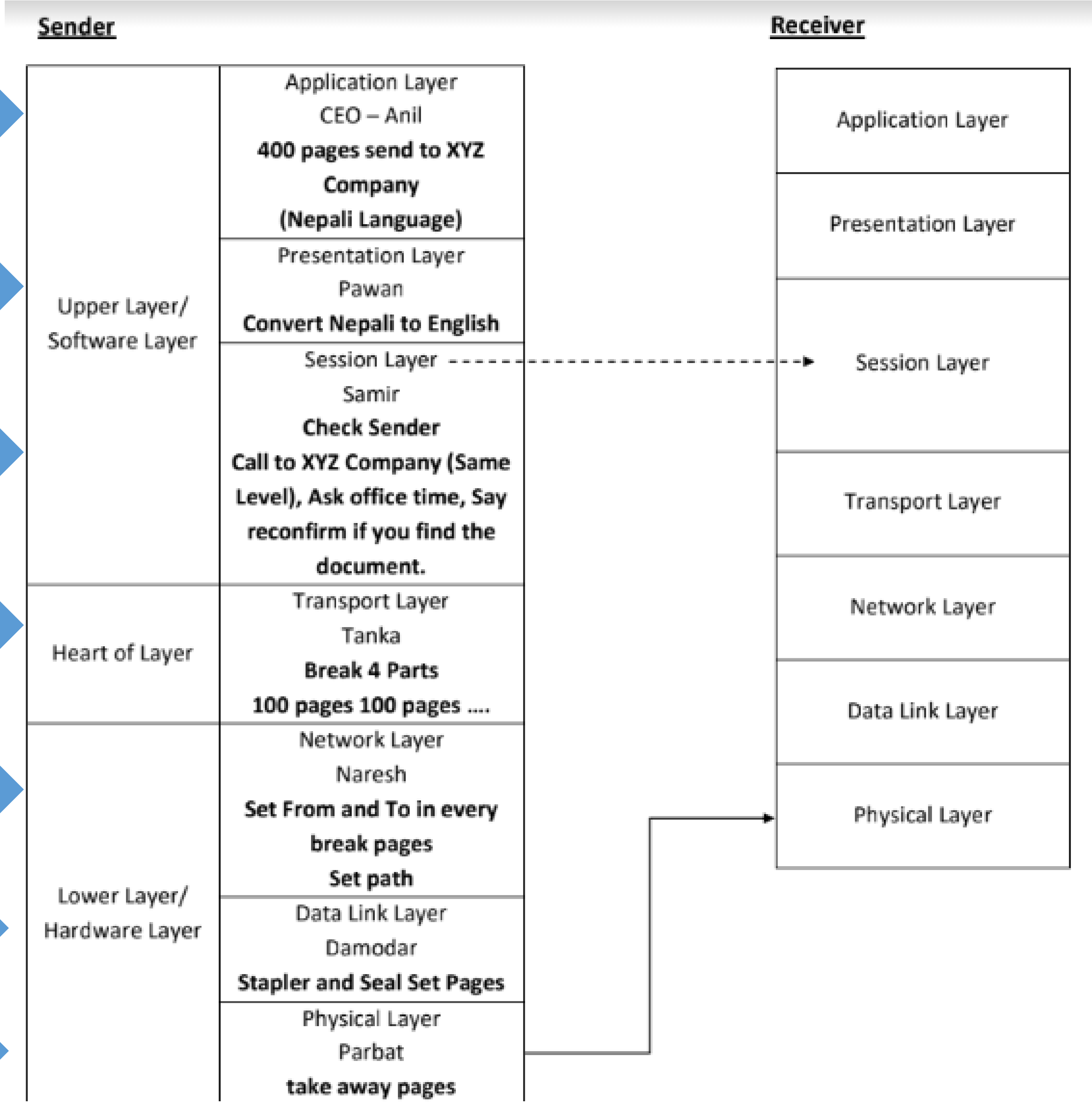
It is used to establish, manage and terminate the sessions.

It provides reliable message delivery from process to process.

It is responsible for moving the packets from source to destination.

It is used for error free transfer of data frames.

It provides a physical medium through bits are transmitted.



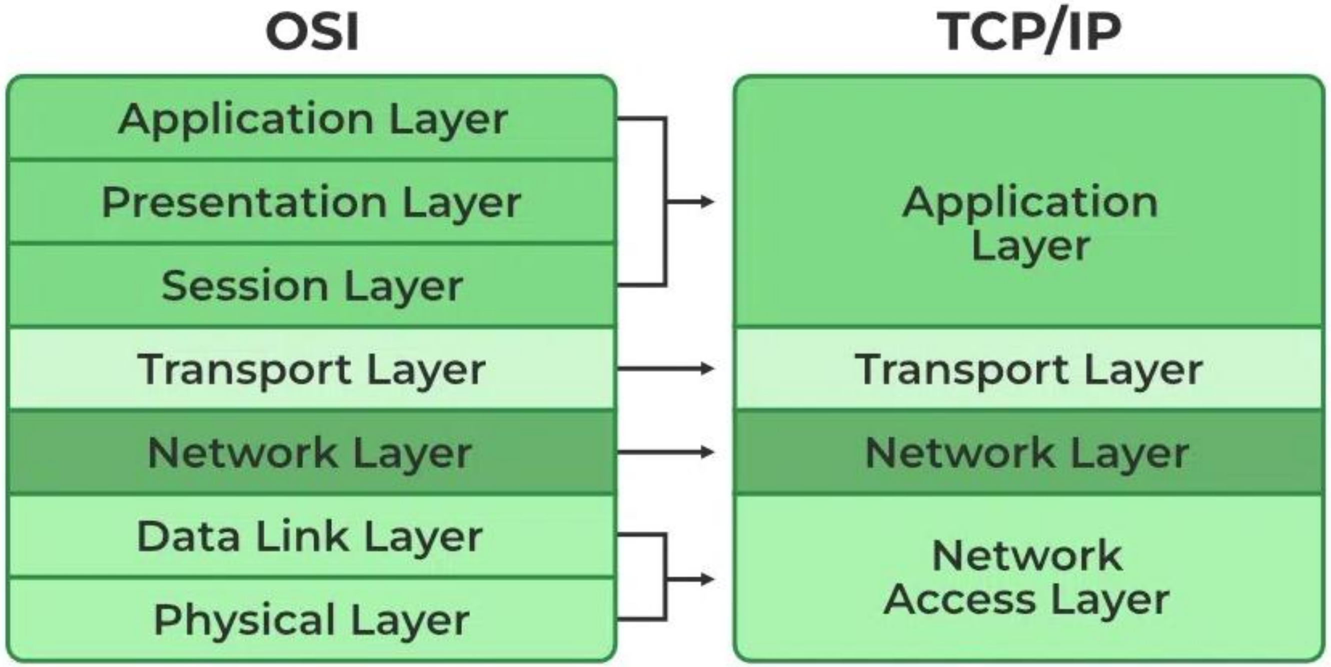
Sender

Upper Layer/ Software Layer	Application Layer CEO – Anil **400 pages send to XYZ Company (Nepali Language)**
	Presentation Layer Pawan **Convert Nepali to English**
	Session Layer Samir **Check Sender Call to XYZ Company (Same Level), Ask office time, Say reconfirm if you find the document.**
Heart of Layer	Transport Layer Tanka **Break 4 Parts** **100 pages 100 pages ....**
Lower Layer/ Hardware Layer	Network Layer Naresh **Set From and To in every break pages** **Set path**
	Data Link Layer Damodar **Stapler and Seal Set Pages**
	Physical Layer Parbat **take away pages**

Receiver

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

TCP/IP



- It stands for Transmission Control Protocol/Internet Protocol.
- TCP/IP is the core protocols of the Internet.
- This model defines how data is transmitted over networks, ensuring reliable communication between devices.
- It consists of four layers: the Link Layer, the Internet Layer, the Transport Layer, and the Application Layer.
- TCP/IP was designed and developed by the Department of Defense (DoD) in the 1960s and is based on standard protocols.
- The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike the seven layers in the OSI model.

Some Basic Terms and Tool Used in Computer Network

IP Address

- IP stands for "Internet Protocol"
- An IP address is a unique address that identifies a device on the internet or a local network.
- An IP address is a string of numbers separated by periods.
- IP addresses are expressed as a set of four numbers.
- Example of IP address: 192.158.1.38.
- Each number in the set can range from 0 to 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255.
- Types of IP Address:

  i. IPv4 ii. IPv6
- Classes of IP Address:

  i. Class A ii. Class B iii. Class C iv. Class D v. Class E

IP Address

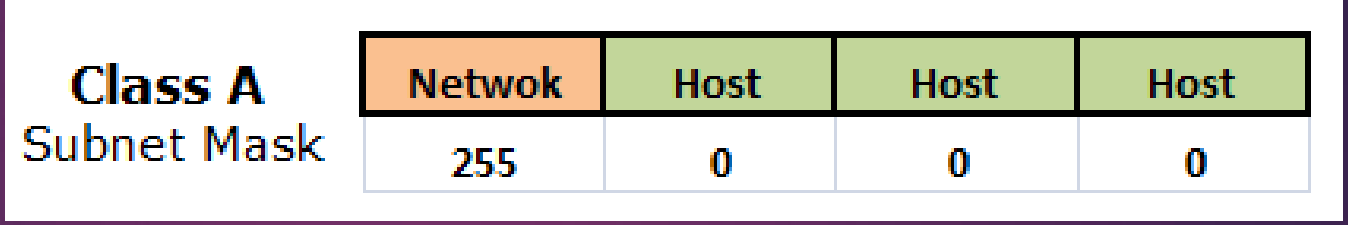
IPV4	IPV6
32-bit address length	128-bit address length
More than 4 billion address (2^{32})	340 undecillion (trillion trillion trillion) unique address (2^{128})
IPv4 consists of 4 fields which are separated by dot (.). Each section contains 8 bits. 8 bits are equal to 1 byte or 1 octet.	IPv6 consists of 8 fields which are separated by colon (:)
IPv4's IP addresses are divided into five different classes. Class A , Class B, Class C , Class D , Class E.	IPv6 does not have any classes of IP address.
Example: 168.212.226.204 or 10101000.11010100.11100010.11001100.	Example: 2001:0000:3238:DFE1:0063:0000:0000:FEFB

IP Address Classes

Class A

In a Class A network, the first eight bits, or the first dotted decimal, is the network part of the address, with the remaining part of the address being the host part of the address (0.0.0.0 to 127.0.0.0). There are 128 possible Class A networks.

Example: 2.134.213.2



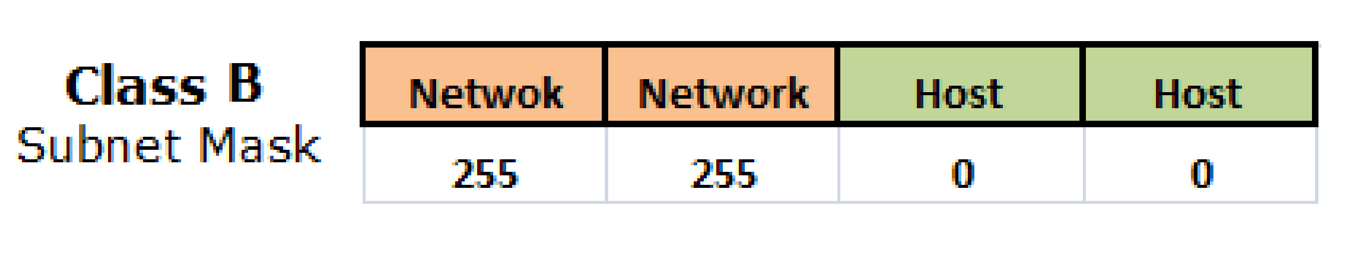
Class A	Netwok	Host	Host	Host
Subnet Mask	255	0	0	0

IP Address Classes

Class B

In a Class B network, the first 16 bits are the network part of the address. In dotted decimal notation, that makes 128.0.0.0 to 191.255.0.0 as Class B networks. There are 16,384 possible Class B networks.

Example: 135.58.24.17



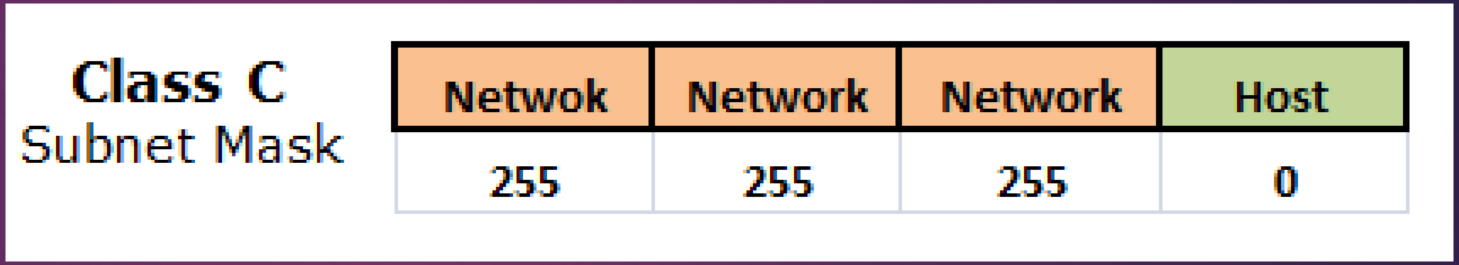
	Netwok	Network	Host	Host
Class B Subnet Mask	255	255	0	0

IP Address Classes

Class C

In a Class C network, that makes the first 24 bits of the address the network address and the remainder as the host address. Class C network addresses range from 192.0.0.0 to 223.255.255.0. There are over 2 million possible Class C networks.

Example: 192.168.178.1



Class C	Netwok	Network	Network	Host
Subnet Mask	255	255	255	0

IP Address Classes

Class D

Class D is reserved for Multicasting addresses. Class D addresses are 32-bit network addresses, meaning that all the values within the range of 224.0.0.0 - 239.255.255.255 are used to uniquely identify multicast groups. There are no host addresses within the Class D address.

Example: 227.21.6.173

Class E

Class E address range is reserved for future or experimental purposes. That addresses from 240.0.0.0 to 255.255.255.255.

Example: 243.164.89.28

MAC Address

- ❑ It stands for Media Access Control address.
- ❑ It is also known as a physical or hardware address.
- ❑ It is used to uniquely identify each node (Computer) of a network.
- ❑ MAC address is usually assigned by the manufacturer of a Network Interface Card (NIC) and is stored in its ROM.
- ❑ MAC address is a 12-digits hexadecimal number (48 bit in length).
- ❑ It's usually six sets of two digits or characters, separated by colons or hyphens.
- ❑ MAC address usually written in one of the following two formats:

MM:MM:MM:SS:SS:SS or MM-MM-MM-SS-SS-SS

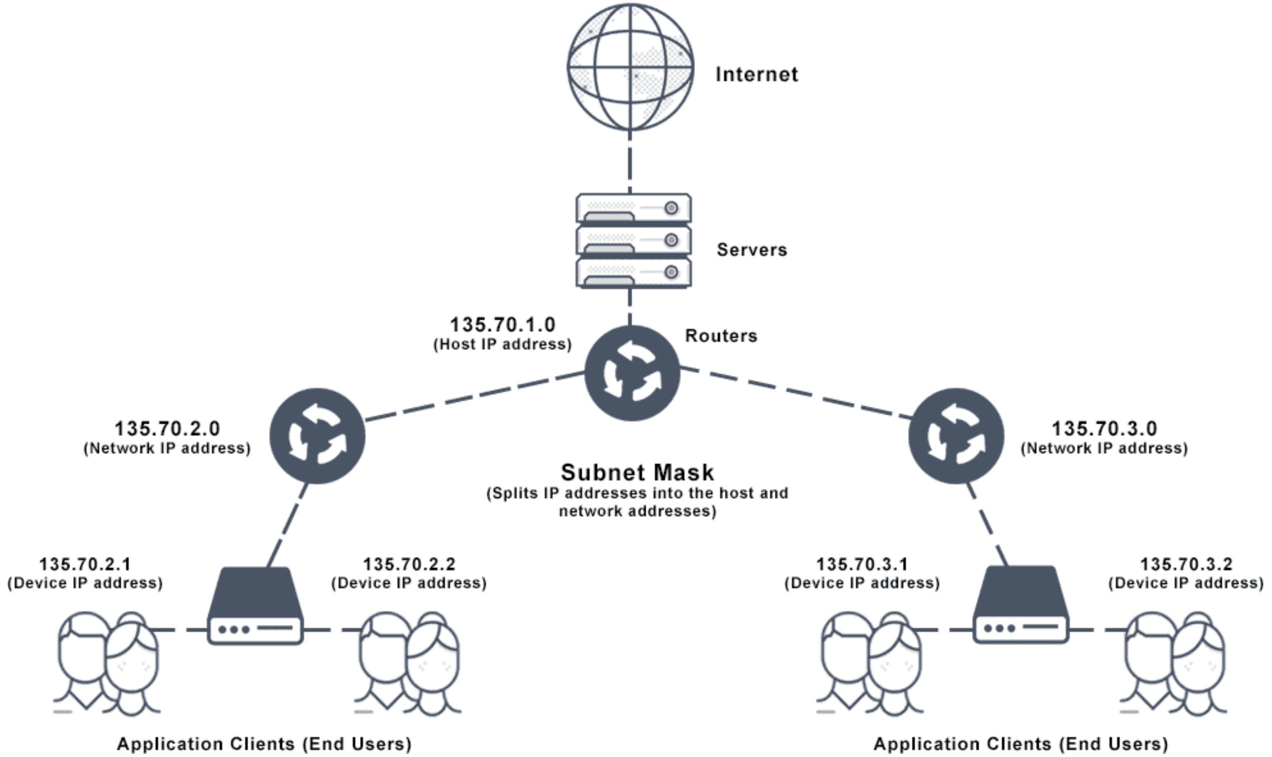
The first half of the number is typically used as a manufacturer ID, while the second half is a device identifier. MAC address ending in FF-FF-FF, it starts again at 00-00-00.

- ❑ An example mac address would be 00:00:5E:00:53:AF

Hints: A MAC address is responsible for local identification and an IP address for global identification.

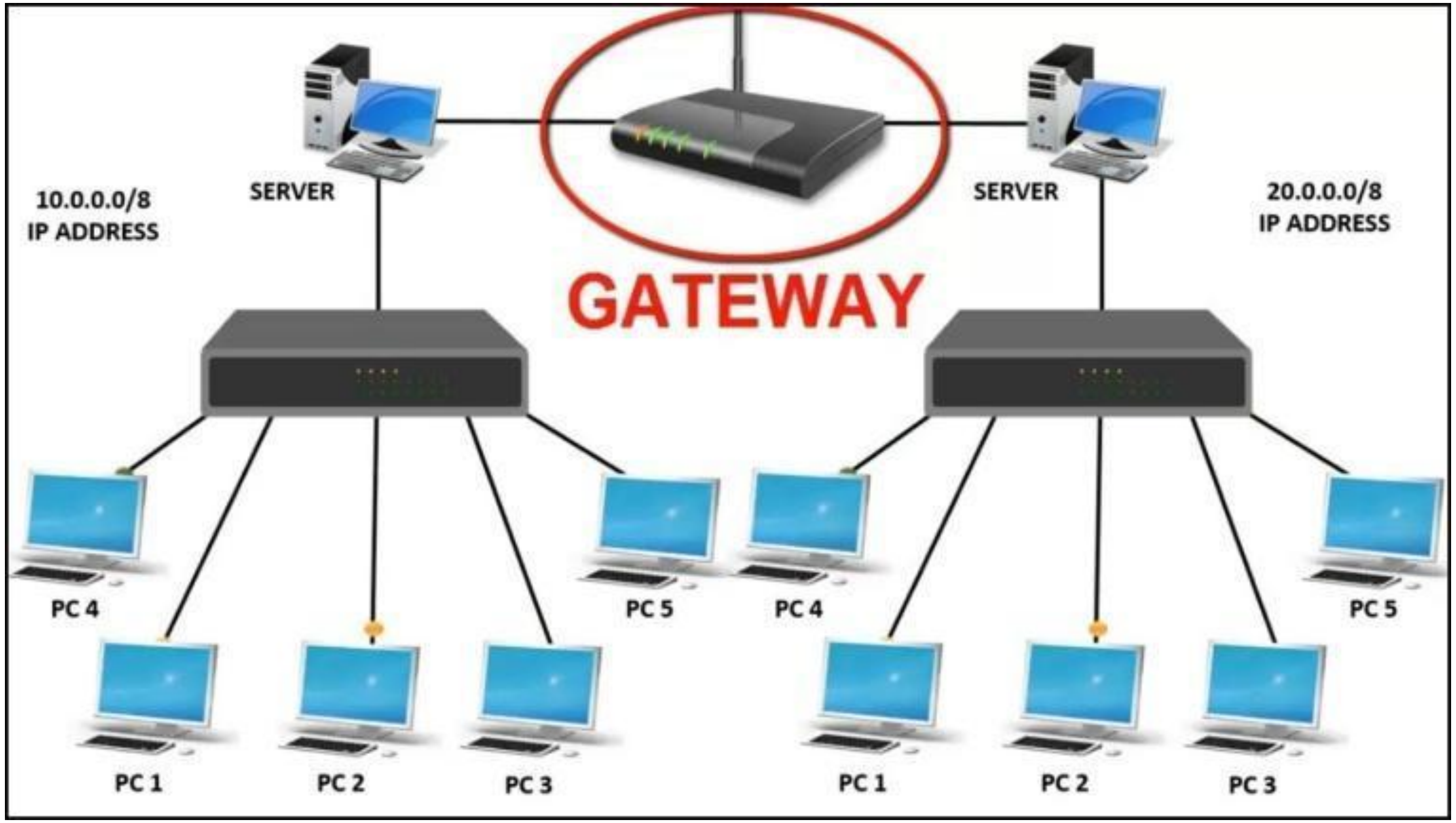
SubNet Mask

- The subnet mask splits the IP address into the host and network addresses.
- The practice of dividing a network into two or more networks is called subnetting.
- Subnet mask can be written either in binary (111111.111111.111111.000000) or decimal (255.255.255.0) form.
- Class A, B and C networks have natural masks, or default subnet masks:
    - Class A: 255.0.0.0
    - Class B: 255.255. 0. 0
    - Class C: 255.255.255.0



Gateway

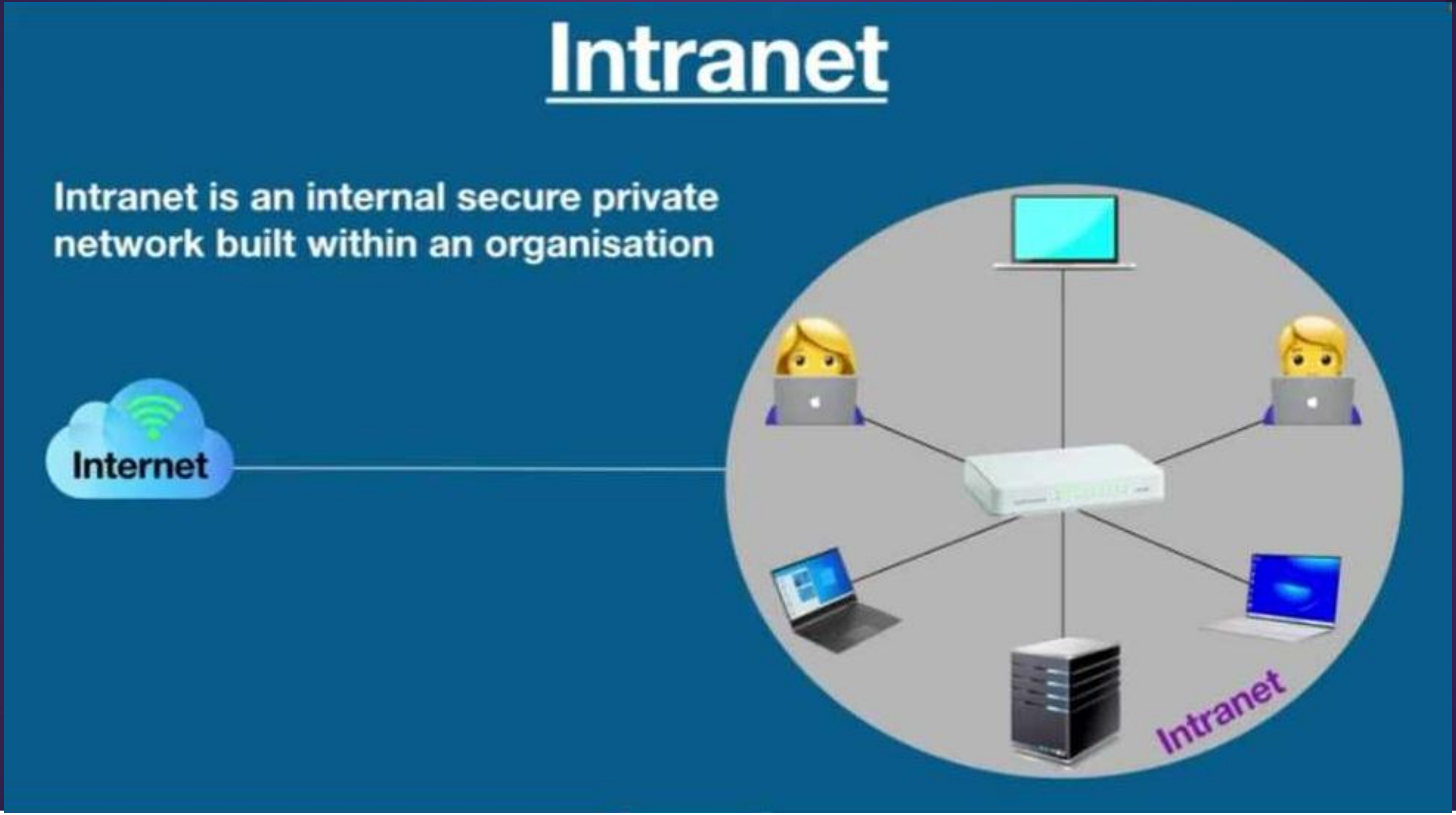
- ❑ Gateway is a network connecting device that can be used to connect two devices in two different networks implementing different transmission protocols.



Internet and Intranet

Internet	Intranet
The Internet is a wide network of computers and is available to all.	Intranet is a network of computers designed for a certain group of users.
The Internet contains a large number of intranets.	Intranet can be accessed from the Internet with specific restrictions.
Number of internet users is very high.	Number of users is limited.
The Internet contains various sources of information.	Intranet only contains group-specific information.
Anyone can access the internet	Accessible only by the organization employees or admin who have login details.
It is not as safe as compared to intranet	Safe and secure network.
It is a public network.	It is a private network.

Intranet



Intranet

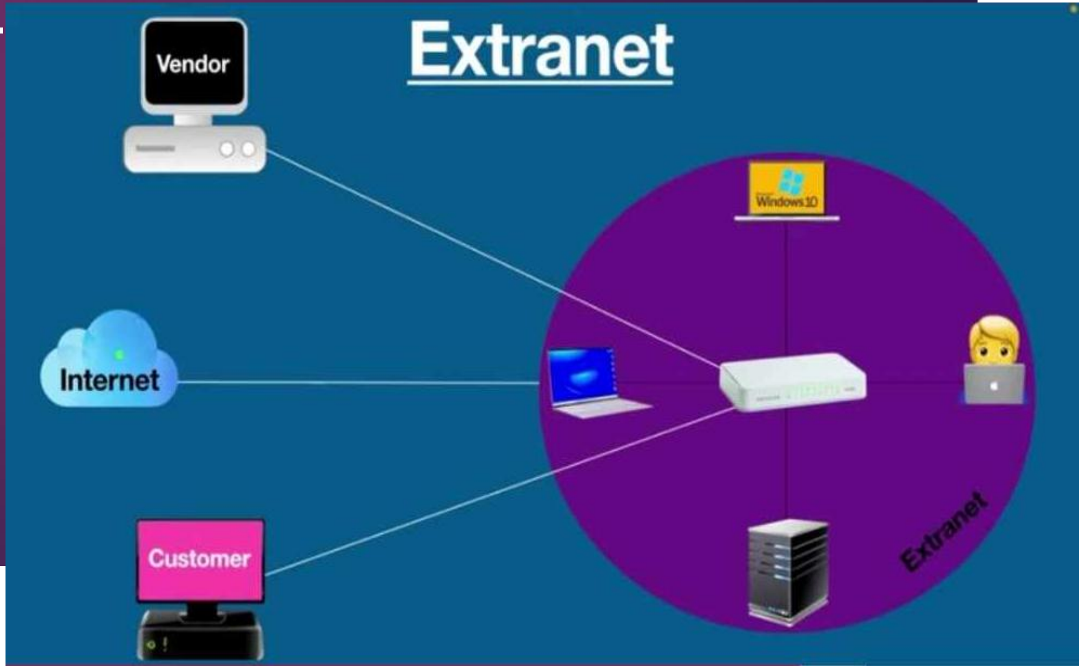
Intranet is an internal secure private network built within an organisation

Extranet

An extranet is technology that connects internal members of your organization with external parties such as customers and suppliers. Extranets are quite similar to intranets, except intranets focus on bringing together internal teams.

Extranet Focus:

- ❑ Communicate through instant and group messaging, or discussions.
- ❑ Store and share files with relevant extranet members.
- ❑ Assign and track tasks across different projects.
- ❑ Control access based on role or by individual user



Need for Satellite Network

A satellite network plays a crucial role in sending the data from one location to another by using an artificial satellite. It is quite an effective method through which data is broadcasted over a large geographical location. Thus, through satellite communication data can reach remote locations.

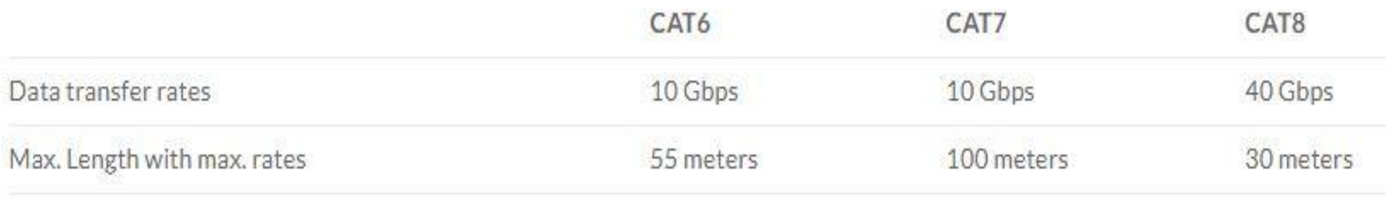
We know that the world is progressing towards globalization and satellite network plays a very crucial role to provide affordable and reliable communication. Satellite communication provides high data rate communication services.

Satellites are basically, artificial stars in the sky but are very much technologically advanced as through this one can find a way around the world, like carrying telephone calls, emails, webpages, TV programs across the sky. Sometimes these are regarded as artificial birds that are present at such high altitudes that they are far beyond the reach of any real bird and such a high altitude facilitates global network infrastructure.

Notes:

- Network Congestion occurs when a network node or link is carrying more data.
- Network Collision occurs when two devices attempt to transmit data on a shared device.
- Network Interference is the signal transmitted by other devices on the same channel that your access point is operating
- **IPCONFIG:** It is the command line tool. It displays IP address, default gateway, and subnet mask for all available adapters.
- **PING:** It is also the command line tool. It is used to test the connection between two devices.
- **Frame Relay:** Frame Relay is a standardized wide area network technology that specifies the physical and data link layers of digital telecommunications channels using a packet switching methodology.
- **X.25:** X.25 is an ITU-T standard protocol suite for packet-switched data communication in wide area networks. It was originally defined by the International Telegraph and Telephone Consultative Committee in a series of drafts and finalized in a publication known as The Orange Book in 1976.

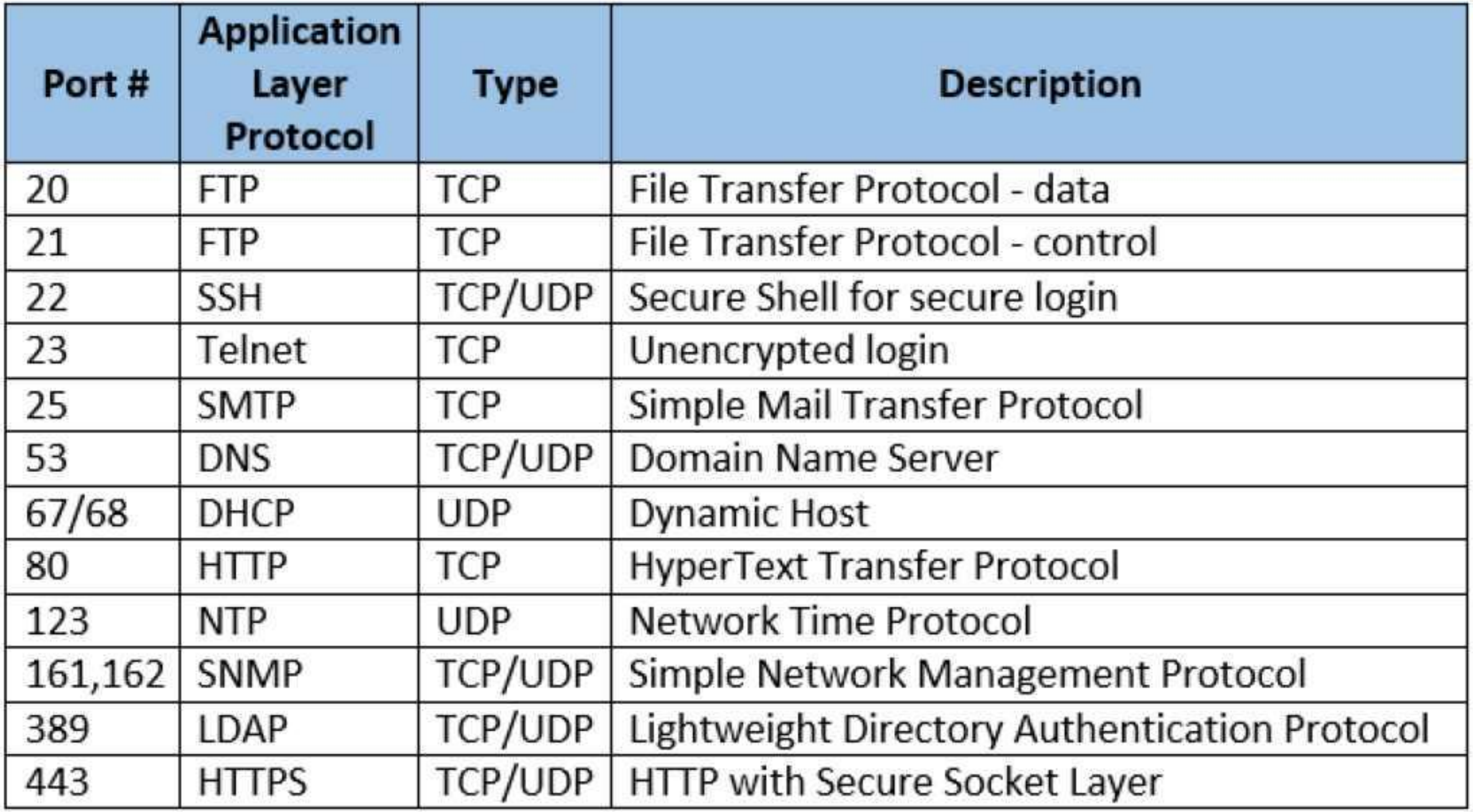
Notes:



	CAT6	CAT7	CAT8
Data transfer rates	10 Gbps	10 Gbps	40 Gbps
Max. Length with max. rates	55 meters	100 meters	30 meters

- **IPCONFIG:** It is the command line tool. It displays IP address, default gateway, and subnet mask for all available adapters.
- **PING:** It is also the command line tool. It is used to test the connection between two devices.
- **Frame Relay:** Frame Relay is a standardized wide area network technology that specifies the physical and data link layers of digital telecommunications channels using a packet switching methodology.
- **X.25:** X.25 is an ITU-T standard protocol suite for packet-switched data communication in wide area networks. It was originally defined by the International Telegraph and Telephone Consultative Committee in a series of drafts and finalized in a publication known as The Orange Book in 1976.

Notes:



Port #	Application Layer Protocol	Type	Description
20	FTP	TCP	File Transfer Protocol - data
21	FTP	TCP	File Transfer Protocol - control
22	SSH	TCP/UDP	Secure Shell for secure login
23	Telnet	TCP	Unencrypted login
25	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	TCP/UDP	Domain Name Server
67/68	DHCP	UDP	Dynamic Host
80	HTTP	TCP	HyperText Transfer Protocol
123	NTP	UDP	Network Time Protocol
161,162	SNMP	TCP/UDP	Simple Network Management Protocol
389	LDAP	TCP/UDP	Lightweight Directory Authentication Protocol
443	HTTPS	TCP/UDP	HTTP with Secure Socket Layer

Model Question of Computer Science by CDC

Group C

Q. No. 6: How do you implement the Class C IP address in the local area network? Describe.

Solution:

IP (Internet Protocol) address is used to identify a particular computer in a network. Every computer in a network is assigned a unique IP address. There are two types of IP addresses: IPV4 and IPV6. IPV4 or (IP Version 4) can be categorized into three classes: Class A, Class B and Class C.

Following are the steps to implement the Class C IP address in the local area network:

1. At the right bottom corner of Desktop, right click on the network (or wifi) icon and click on Open Network & Internet Settings
2. In the network status settings, click on Change adapter options under the Advanced network Settings
3. OR, Press Windows Key + R and then type ncpa.cpl
4. This will open Network Connections window.
5. Right click on desired network and select Properties.
6. In the Wifi Properties dialog box, Click on Internet Protocol Version 4 (TCP/IP) and then click on Properties button
7. There are two options :
    - Obtain IP address automatically – allows to dynamically set IP address automatically
    - Use the following IP address –
        - Choose this option to type the IP address, Subnet Mask, Default Gateway and click on OK
        - If the IP address conflicts with existing one, an error message appears, otherwise, the assigned IP address will be set.

8. Additionally, DNS server addresses can also be set automatically or manually.
9. The assigned IP address can be checked using **ipconfig** command.

Why do people prefer star topology as a LAN to set up in an organization?

Star topology is a popular choice for Local Area Networks (LANS) in any organizations due to several advantages. Here are some reasons why people prefer to use star topology:

1. Reliability: In a star topology, if a cable or device fails, only the affected node is impacted. Other devices continue to function normally. This reliability is crucial for critical systems used in the organization,

2. High Performance: Star topology ensures that data collisions do not occur, Each device has its own dedicated link to the central hub or switch, allowing efficient data transmission without interference.

3. Cost Effective: Unlike other topologies, where each device needs multiple connections, star topology requires only one Input/output port per device. This Simplicity reduces costs, especially in large networks,

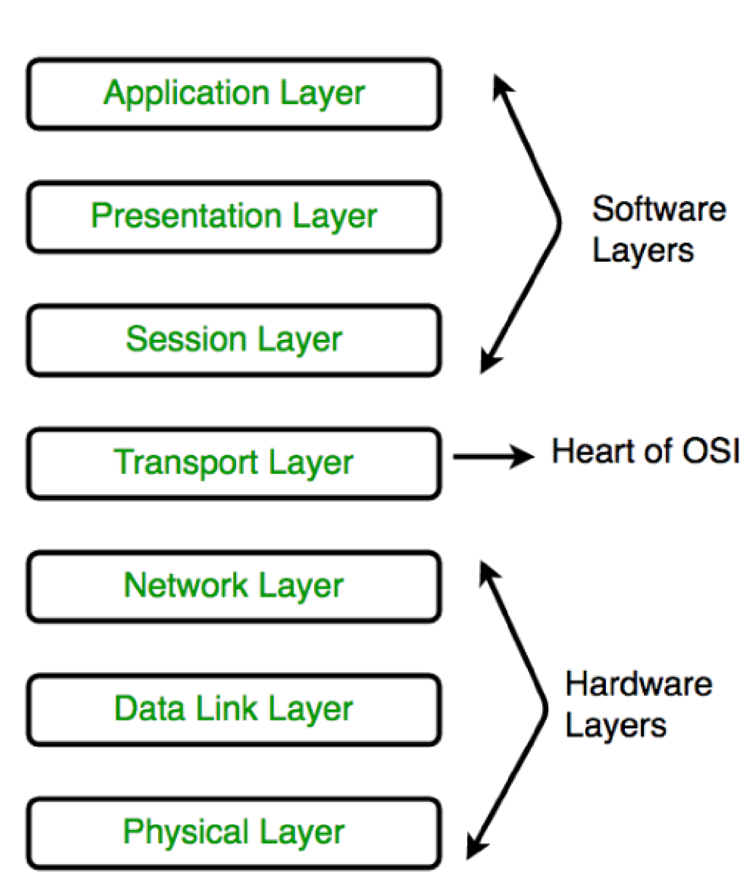
4. Easy Installation, Fault Detection, and Maintenance: Setting up a star network is straightforward, as each device connects directly to the central hub, Additionally, identifying faults is easier because the failed link can be quickly pinpointed. So that maintenance is easier.

Thus, star topology provides reliability, better performance, cost effectiveness, and ease of maintenance qualities that make it suitable for LANs in any organizations.

Explain OSI model.

- ❑ OSI stands for Open System Interconnection.
- ❑ OSI model was developed by ISO (International Organization for Standardization) in 1984.
- ❑ Most of the network communication protocols are based on the OSI model.
- ❑ It is a 7 Layer architecture. They are:

  Physical layer, Data Link layer, Network layer, Transport layer, Session Layer, Presentation layer and Application layer.
- ❑ Physical, Data Link and Network layers are known as Hardware/ Lower Layers.
- ❑ Transport Layer is also known as Heart of OSI model.
- ❑ Session, Presentation and Application Layers are known as Software/ Upper Layers.



Application Layer

The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

Presentation Layer

The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

Session Layer

The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends. The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint.

Transport Layer

The transport layer takes data transferred in the session layer and breaks it into “segments” on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.

Network Layer

The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network. The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node.

Data Link Layer

The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.

Physical Layer

The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.