INTRODUCTION

A network is an interconnection of two or more computers or networking devices with the help of transmission media and protocols.

Computer network brings communication (information exchange) faster, reliable, cheaper and secure.

A communication system has five major components:

- **Message:** The message is data or information to be communicated and it is in the form of text, number, picture, audio and video.
- **Sender:** The sender device sends the message to the receiver and it can be computer, workstation or any networking devices.
- **Receiver:** The receiver device receives the messages from the medium and it can be computer, workstation or any networking devices.
- **Transmission medium:** The transmission medium is physical connection in which a message can travel from sender to receiver and vice versa. The medium can be wired or wireless.
- **Protocols:** A protocol is a set of common rules that manages the data communication. Without protocol two devices can be connected but not be communicated.

Advantages of computer networking

i. Sharing data and resources.
ii. Faster and cheaper communication.
iii. Centralized control.
iv. Backup and recovery.
v. Remote access.

Disadvantages of computer networking

i. Privacy issue
ii. Experience to setup
iii. Hacking
iv. Needs technical person
v. Spread of virus

Modes of communication

Data communication can be classified into three types on the basis of direction of communication flow:

a) Simplex

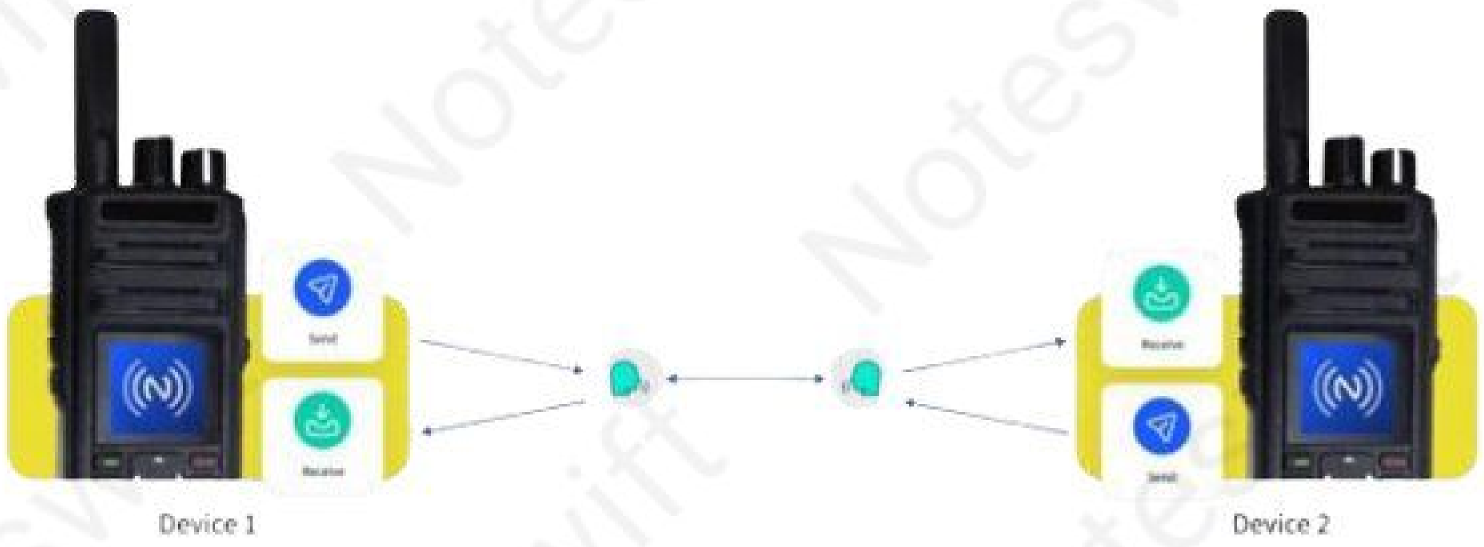
Simplex mode is a transmission mode in which information is sent in one direction only, also known as unidirectional.

Example of Simplex communication

b) Half-duplex

Half-duplex mode is a communication mode where two devices can communicate with each other, but not simultaneously.

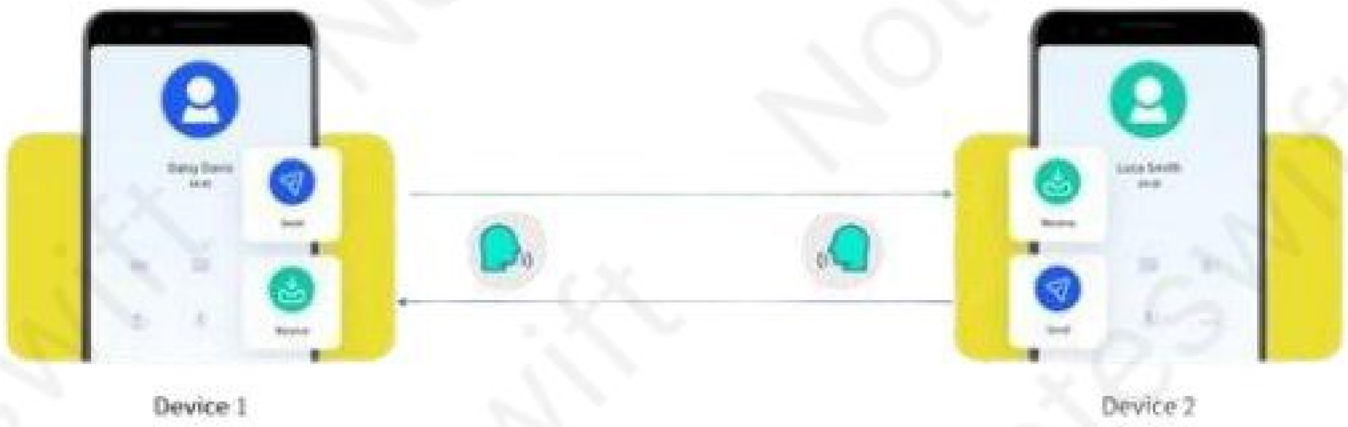
Half Duplex Communication



c) Full duplex

Full-duplex communication is a method that allows data to be sent and received simultaneously. It's similar to a two-way road, where traffic can flow in both directions at the same time.

Full Duplex Communication



Types of computer network

1) On the basis of geographical area

On the basis of geographical area, computer networks are classified into following three categories:

a) **Local Area Network (LAN)**
A local area network (LAN) is privately owned small sized network which spans only in small geographical area such as within a room, office, building or up to few kilometers (2 or 3 kilometers). For example, network used in our college or office. It is simpler, cheaper and highly secured network.

b) **Metropolitan Area Network (LAN)**
A metropolitan area network (MAN) is a computer network that connects computers within a metropolitan area, which could be a single large city, multiple cities and towns, or any given large area with multiple buildings. A MAN is larger than a local area network (LAN) but smaller than a wide area network (WAN). For example, cable TV network, Internet Service Provider (ISP) in a city, etc.

c) **Wide Area Network (WAN)**
A wide-area network (WAN) is the technology that connects your offices, data centers, cloud applications, and cloud storage together. It is called a wide-area network because it spans beyond a single building or large campus to include multiple locations spread across a specific geographic area, or even the world. For example, internet, networking of a bank, etc.

2) **On the basis of network architecture**
Network architecture refers to the various services provided by the network and it also deals with how data is transmitted from one computer to others. On the basis of network architecture, computer networks are classified into two types:

i. **Client Server Network Architecture**
A client-server network is a type of internet network that uses a central computer, called the server, to manage resources and control user access. The server provides services or functions to one or more clients, which request them. Clients are the devices that request services and use the services provided by the servers.

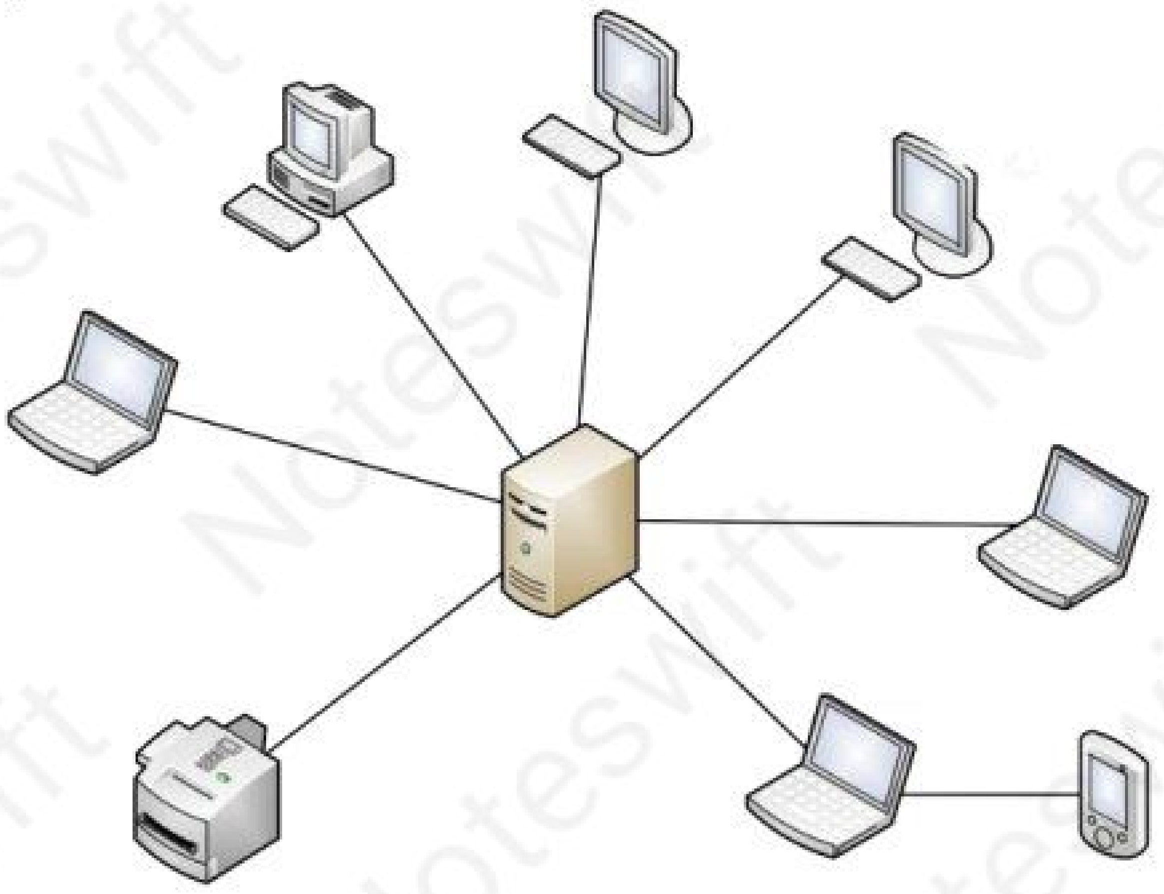


Fig: - Client Server Architecture

Advantages of client server architecture

i. High security.
ii. Centralized administration.
iii. Reliable architecture.
iv. Easy to manage the network.

Disadvantages of client server architecture

i. Data traffic may lead to data collision.
ii. If server fails, the whole network gets disturbed.
iii. Resources are centralized to server. Hence it needs authentication.
iv. More expensive to setup.

ii. **Peer to peer network architecture**

In this architecture, each node/workstation has same capabilities and responsibilities in a network. Here each node act like a server and client.

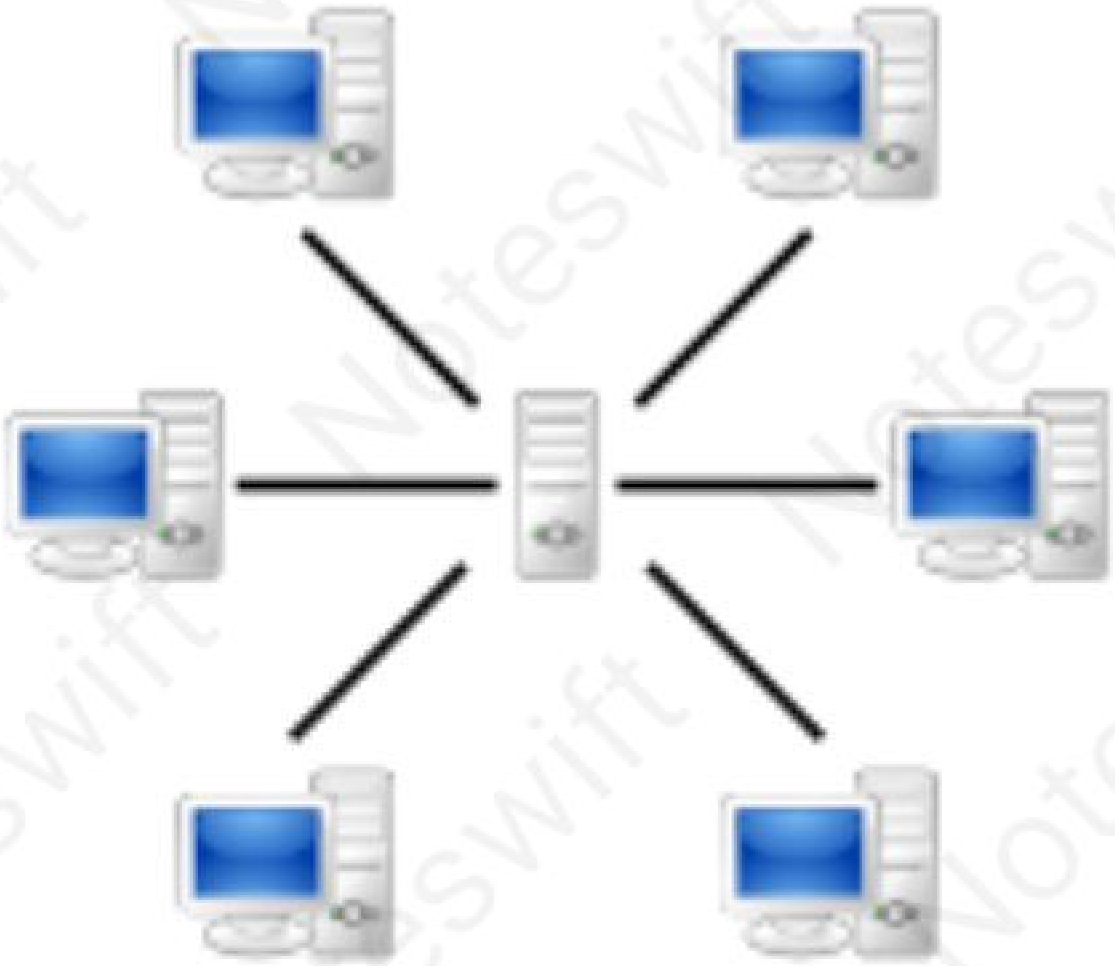


Fig: - Peer to Peer Architecture

Advantages of peer to peer architecture

i. Simple and easy to install.
ii. Cheaper than client server.
iii. All nodes have equal right to access the resources.
iv. Suitable for small size network.
v. No data collision.

Disadvantages of peer to peer architecture

i. Very low performance for large size network.
ii. Network security problem.
iii. No central backup and recovery mechanism.
iv. Lack of proper monitoring of resources.

Transmission Media

Transmission media refers to the physical connection through which data are transmitted between sender and receiver devices. They are classified as follows:

1) **Guided Media**

Guided media is a physical link between devices that can send data through wires. For example, twisted pair cable, co-axial cable, optical fiber, etc.

i. **Co-axial cable**

This cable consists of a copper wire conductor which is surrounded by an insulator over which there is sleeve of copper is surrounded which is then covered by protective plastic.

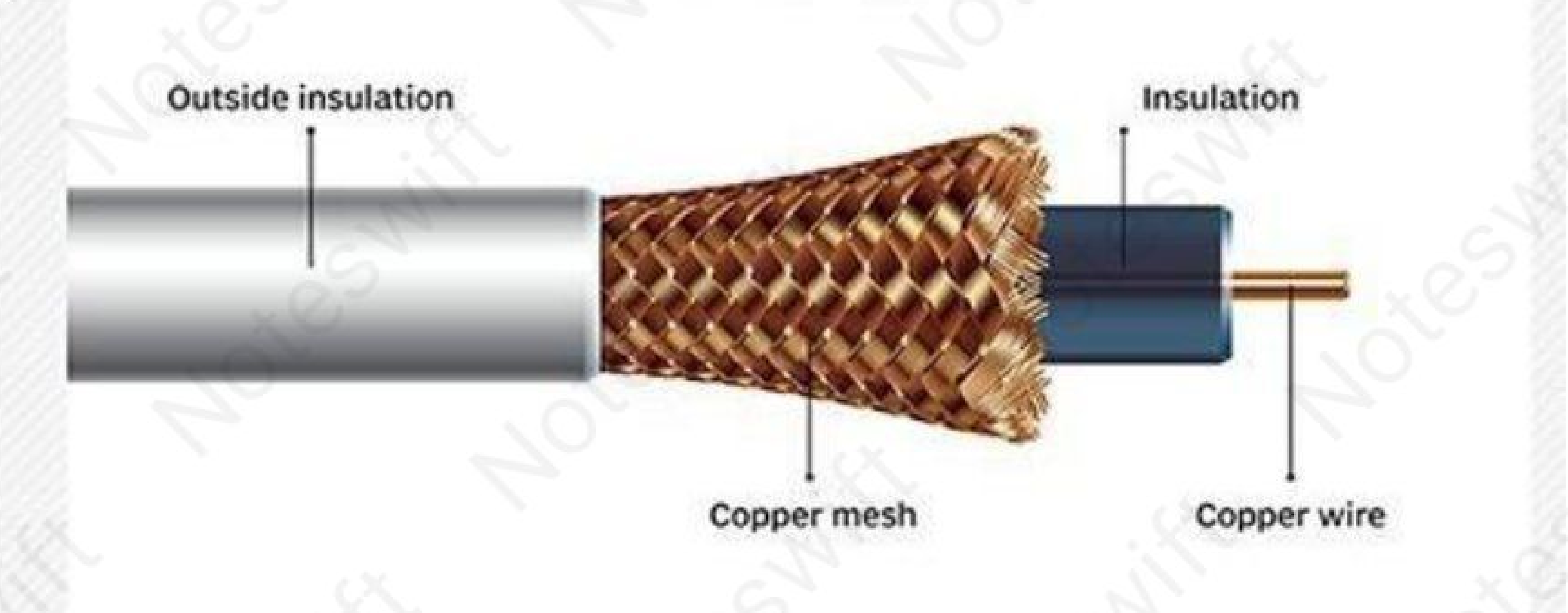


Fig: - Co-axial cable

Features:

a) It can carry signal up to 500 meter and bandwidth up to 100 Mbps.
b) It supports multiple channels in a medium and less effective by electromagnetic interference.
c) The data within co-axial cable can easily be tapped.
d) It is not suitable for digital data transmission.

ii. **Twisted pair cable**

Twisted par cable is made up of copper wires to each other and finally surrounded by insulating jacket. One wire of the pair is used for receiving signal and other wire is used for transmitting data. It is used for both analog and digital transmission.

It is available in different categories i.e. CAT 1, CAT 2, …, CAT 6, CAT 7, etc.

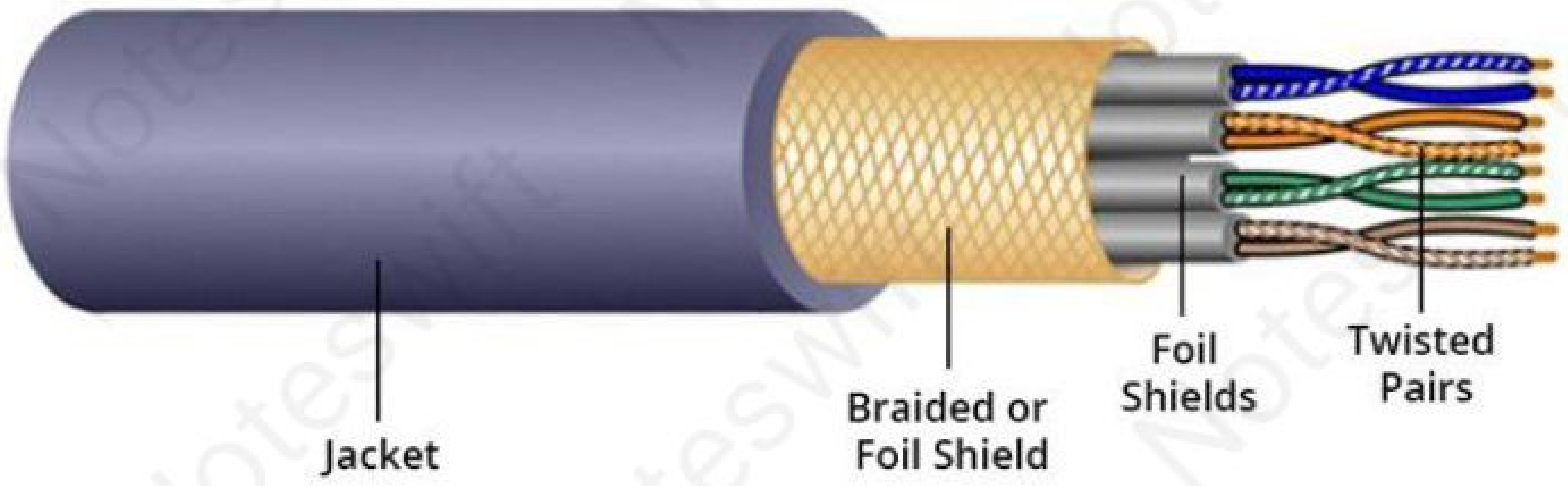


Fig: - Twisted pair cable

Features:

a) It is easier to connect any two wires and flexible for wiring.
b) It has higher data transfer rate up to 1 Gbps.
c) It is not possible to transmit data for a long distance (up to 200m).
d) It emits electromagnetic interference.

iii. **Optical fiber**

It is made up of a glass or plastic that transfer signals in form of light. The main core glass is surrounded by a strong cladding with lower index of refraction. It works on the principle of total internal reflection.

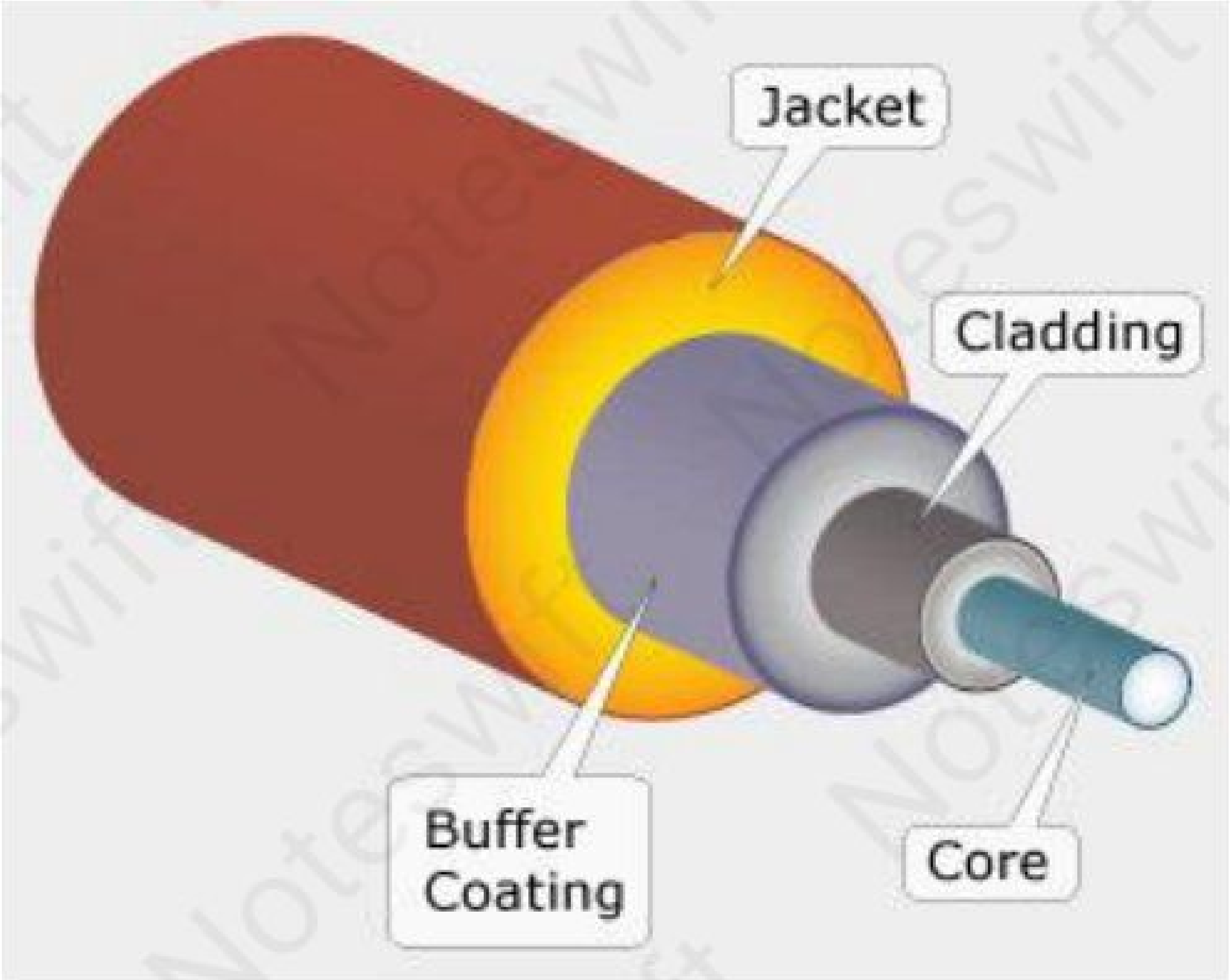


Fig: - Optical Fiber

Features:

a) The speed of optical fiber is highest of all cables i.e. Gbps, Tbps and even more.
b) They are suitable for long data transmission with unlimited bandwidth.
c) They are much thinner and lighter.
d) It is difficult to tap the data because data is transmitted in the form of light.
e) It is not affected by electromagnetic interference.
f) They are highly expensive.
g) It is very difficult to connect any two optical fibers and bend them.

2) Unguided media

Unguided media is also called wireless media in which there is no physical connection between any two communicating devices i.e. it transmits signals via air. For example, infrared, Bluetooth, Wi-Fi, microwaves (radio waves), satellite, etc.

i. **Infrared:** Infrared has the shortest transmission distance that follows the line of sight. It can support distance up to 10m and supports very low bandwidth.

ii. **Bluetooth:** Bluetooth is a short-range wireless technology that is used for exchanging data between fixed and mobile devices over short distance (up to 10m to 20m). It relies on radiofrequency and does not require line of sight that is it can pass through obstacles. For example, speaker, headset, mobile phones, etc.

iii. **Wi-Fi:** Wi-Fi is a wireless networking technology that uses radio waves to provide wireless high-speed internet access. It uses high band frequencies such as 2.4 GHz up to 5 GHz. For example, IoT devices.

iv. **Microwave:** Microwave is a modern technology that uses electromagnetic waves with microwave frequency ranges from 300 MHz to 300 GHz. For example, FM stations, telecommunication towers, etc.

v. **Satellites:** Satellites are kept at around 36000 km above the earth surface which continuously rotates in the same orbit. The communication is done through uplink and downlink using ground stations. It is used for universe study, GPS, military purpose, etc.

Transmission Impairments Technology

Transmission impairments occur when the received signal is different from the transmitted signal.

Some if the impairments are given below:

i. **Jitter:** Jitter is a fluctuation in delay as packets are being transferred across a network. It is also called variation in time between data packets that may be caused by transit points or network traffic.

ii. **Echo:** Echo is a sound that is a copy of another sound is produced when sound waves bounce on the surface.

iii. **Crosstalk:** Cross is a form of interference in which signal in one cable is mixed with another cable.

iv. **Distortion:** Distortion is a change in the form or shape of a signal that can cause an unclear reception.

v. **Noise:** Noise is the mix-up of different unwanted signals or frequencies while communicating the messages from one end to another.

vi. **Bandwidth:** Bandwidth refers to the speed of the internet i.e. it justifies the number of bits (mb, kb) that can be communicated by a sender to receiver in one second.

INTERNET, INTRANET AND EXTRANET

The internet is a global network of computers, phones, servers, and smart appliances that are connected worldwide. It allows users to exchange information between computers on a network, such as through mail, chat, video conferences, and audio conferences.

An intranet is a private network that is only accessible to members of an organization. It's a local area network (LAN) or wide area network (WAN) web-connected site that functions like an internal website. Intranets are used by companies of all sizes and industries to share information, communicate, and collaborate.

An extranet is a private network that allows organizations to securely share information with external parties. Extranets are similar to intranets, but they are typically open to external parties, such as customers, suppliers, and business partners.

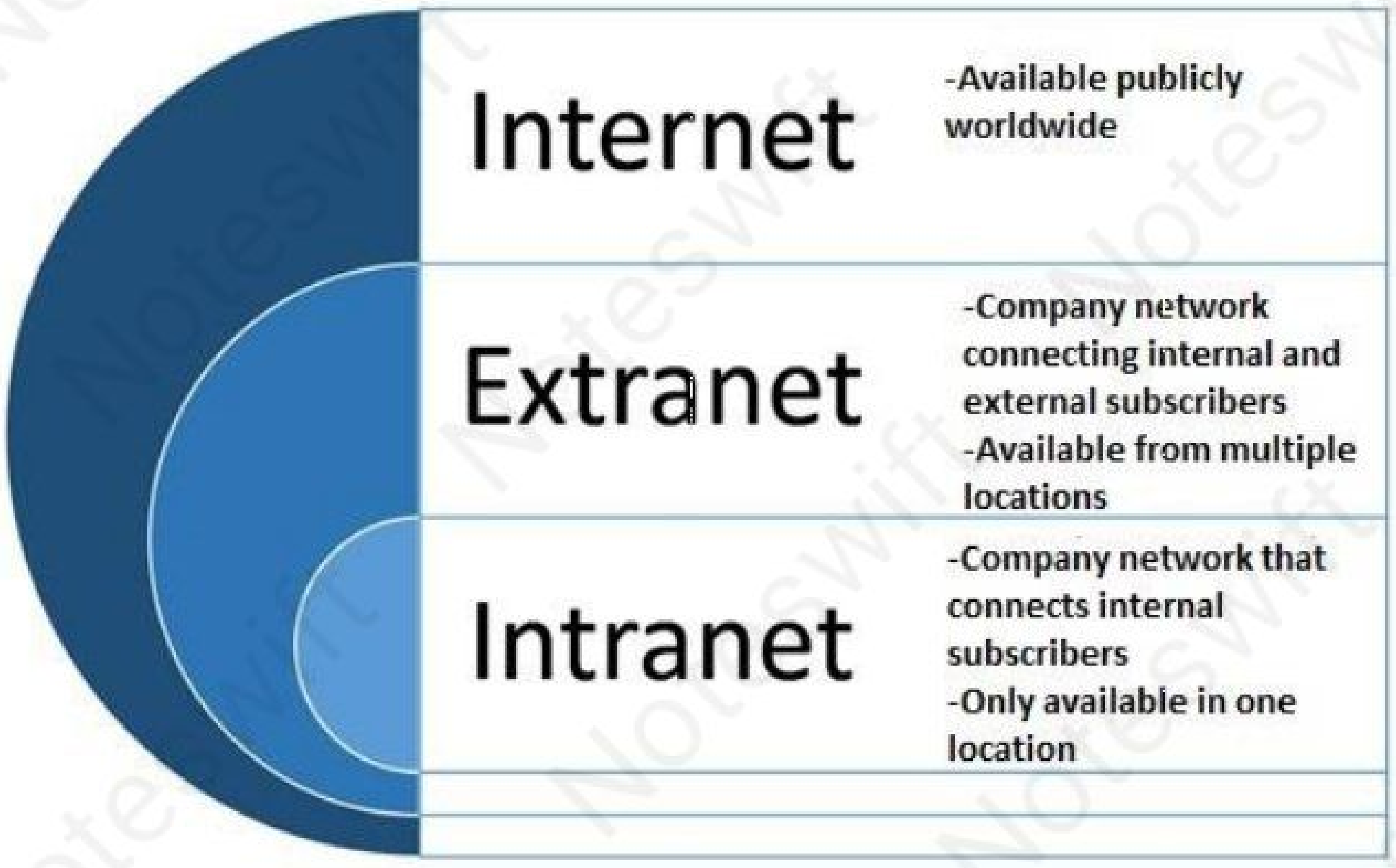
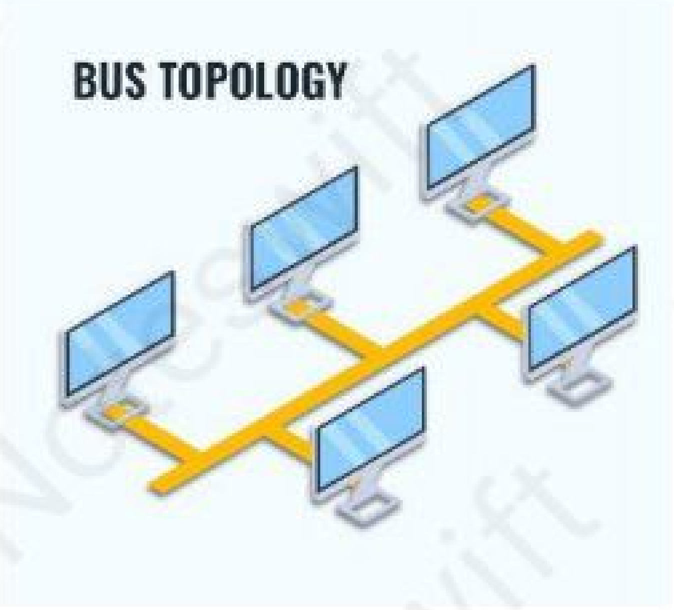

Internet
-Available publicly worldwide
Extranet
-Company network connecting internal and external subscribers
-Available from multiple locations
Intranet
-Company network that connects internal subscribers
-Only available in one location

Fig: - Difference between internet, intranet and extranet

Network Topology

Network topology is the way of arrangement of computers in a network.

1) **Bus Topology: -** Bus topology is a type of network topology in which all the computers or digital devices are connected. There are termination points on the both sides to protect the data signal loss.



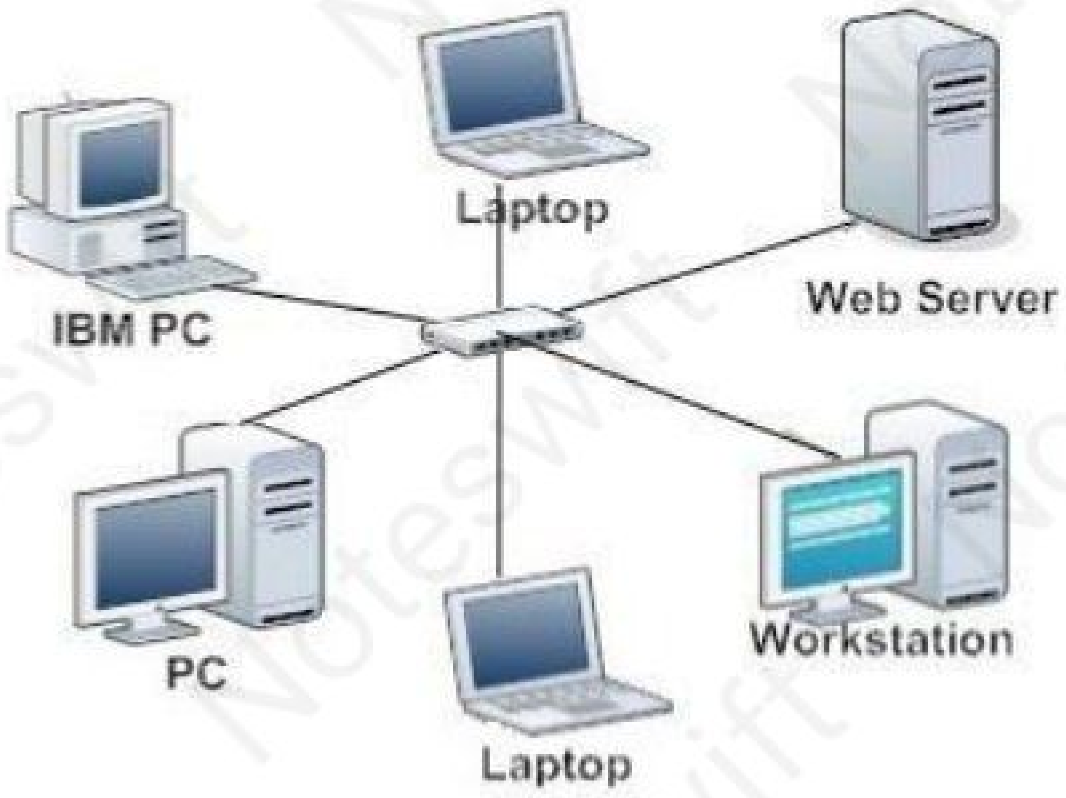
Advantages of bus topology

i. Cheapest topology
ii. More flexible
iii. Easy setup

Disadvantages of bus topology

i. Data collision
ii. Depends on main wire. If the main wire is destroyed, then there is loss in network.
iii. Can't handle huge data traffic.

2) **Star Topology: -** Star topology works as a client-server network architecture in which there is a main central node and all other nodes are connected to the central one.



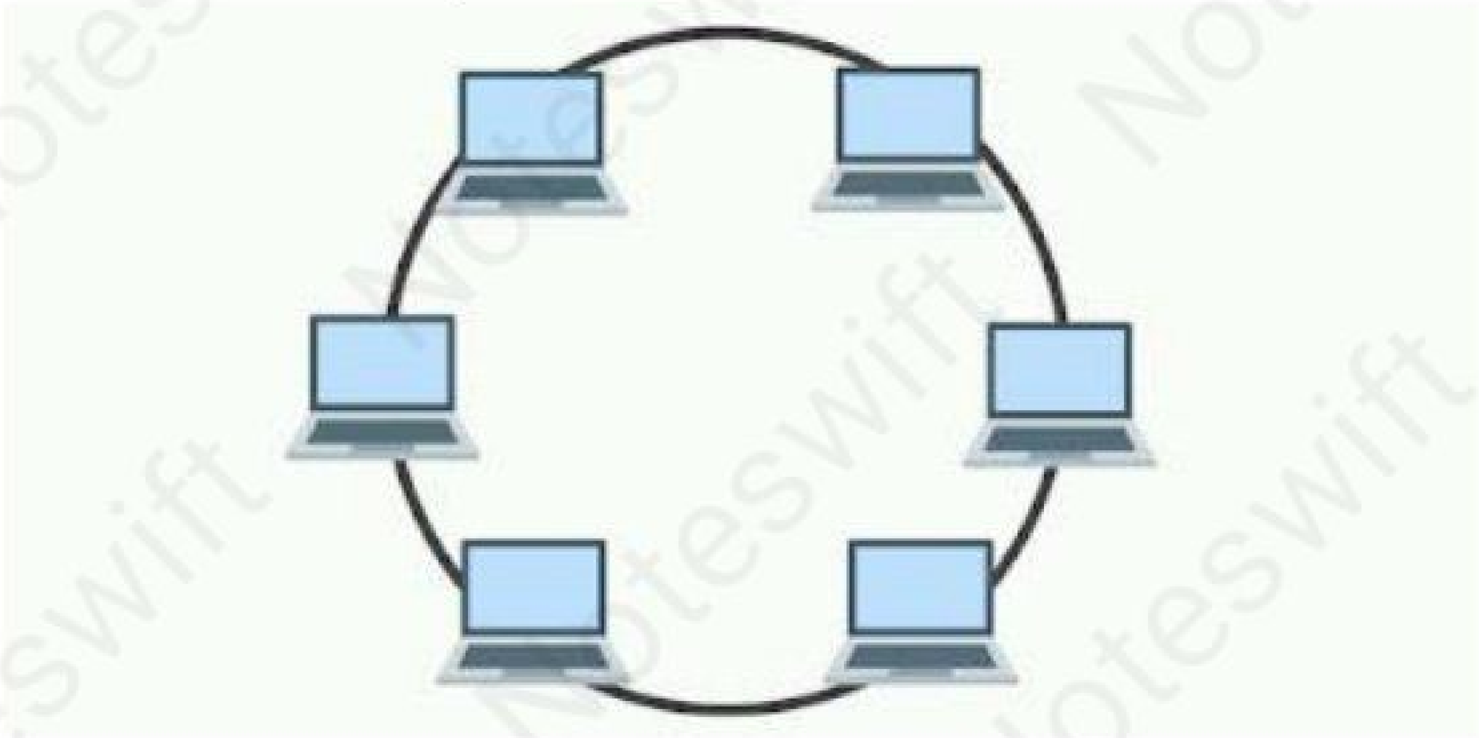
Advantages of star topology

i. Easy to setup.
ii. High data transfer rate.
iii. Safe topology.
iv. It does not affect other nodes while connecting new one.

Disadvantages of star topology

i. Device limitations.
ii. Depends on central node.
iii. More expensive to setup than bus topology.

3) **Ring Topology: -** Ring topology is a type of topology which is in ring shape and each node is connected to one another without any centralized control.



Advantages of ring topology

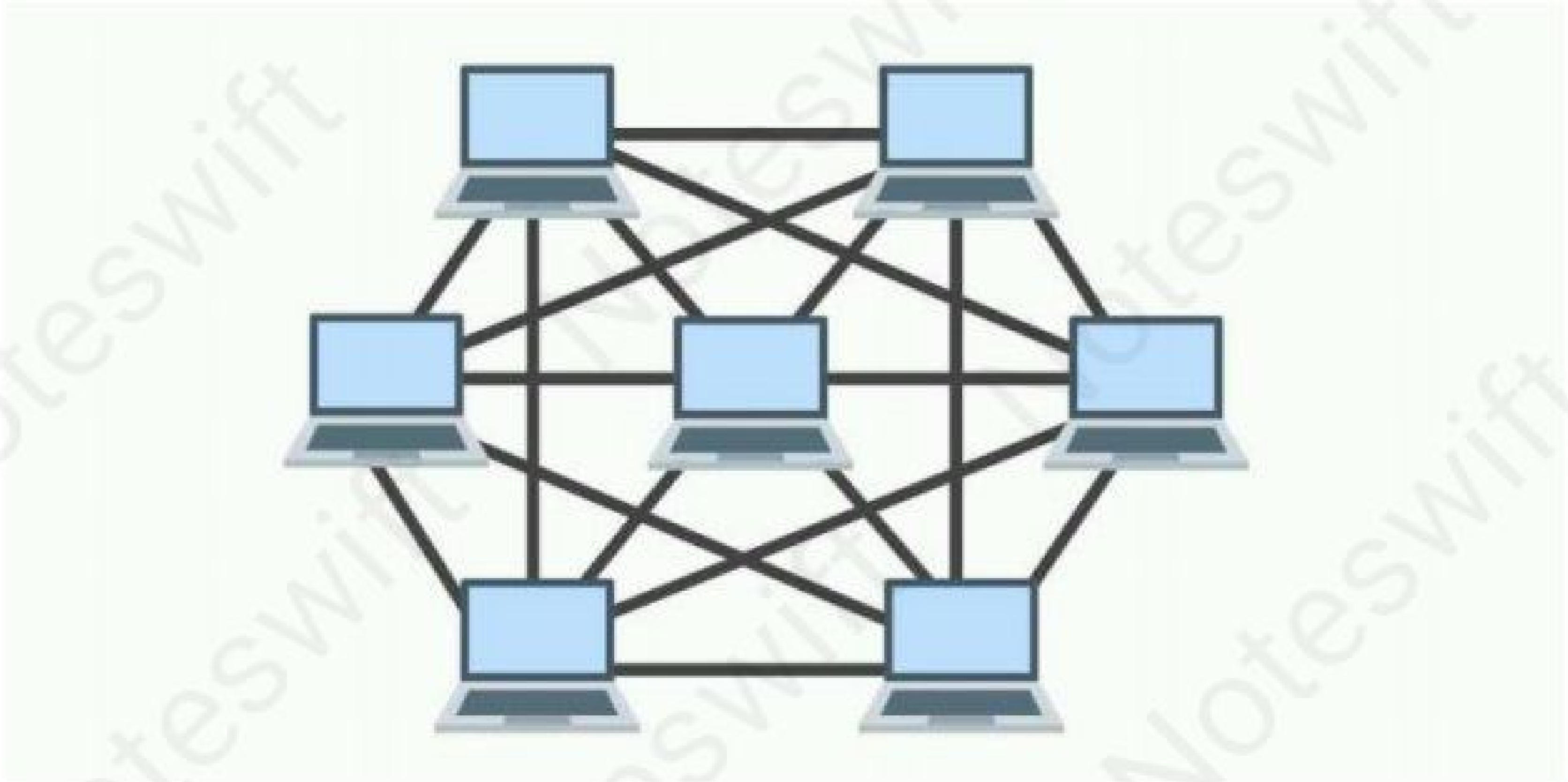
i. Easy to setup.
ii. Cheapest topology.
iii. No authentication is required.
iv. Suitable for small area.

Disadvantages of ring topology

i. Less secure.
ii. Difficult to install or delete new node.
iii. Network speed depends on each
iv. If any of the is damaged, then whole network gets damaged.

4) **Mesh Topology**

In this topology, all the computers are connected with each other via multiple channels i.e. all the computers are connected with direct communication link.



Advantages of mesh topology

i. It can handle huge data traffic because of multiple links.
ii. It is suitable for small area where real time data transfer is needed.
iii. If one computer gets damaged, it will not affect the whole network.

Disadvantages of mesh topology

i. It is highly expensive and difficult to setup.
ii. It is quite impossible for a large wired network.
iii. It has low security.

5) Tree Topology

Tree topology is a topology seems like hierarchical model in a tree structure.

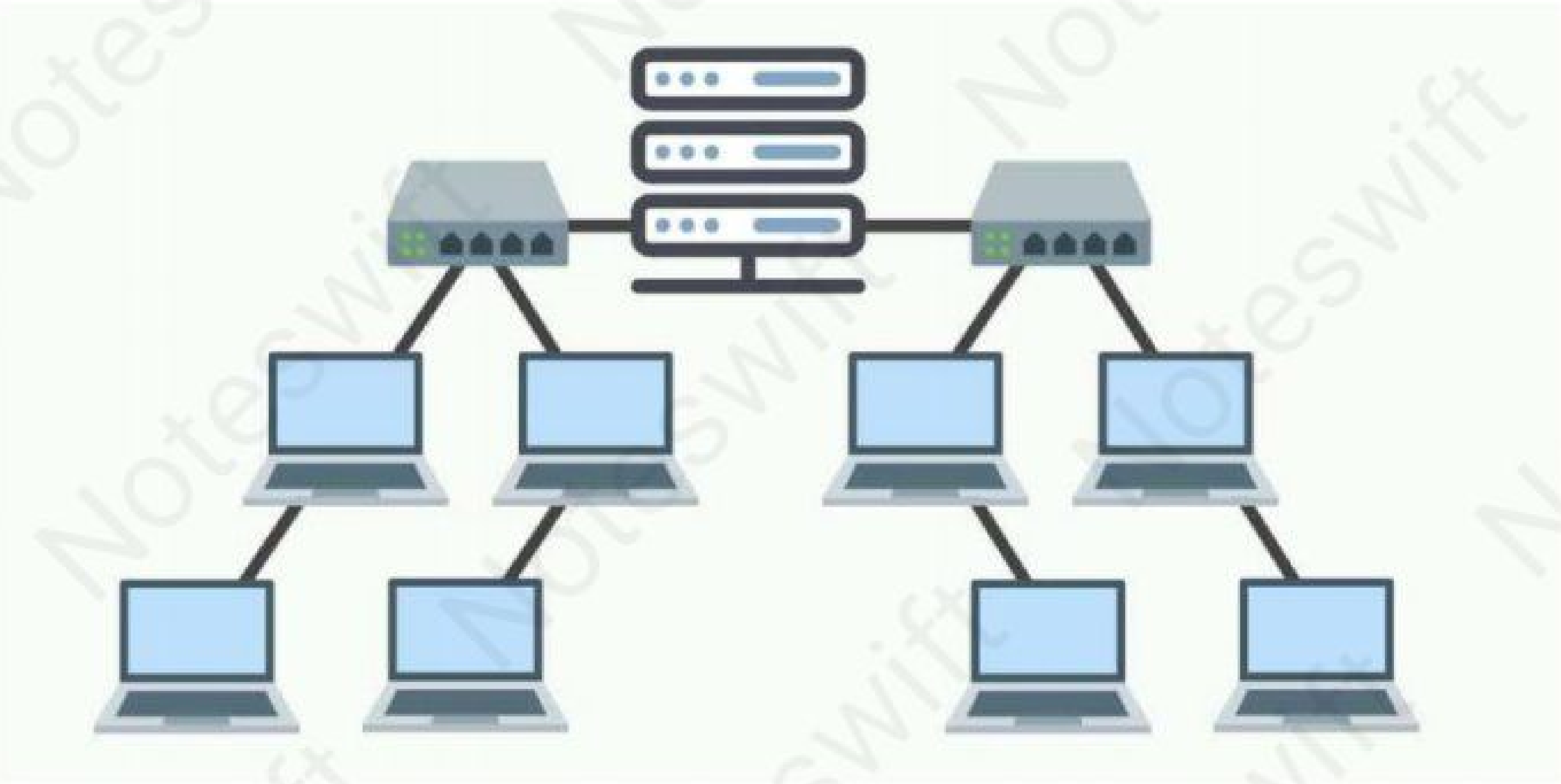


Fig: - Tree Topology

Advantages of tree topology

i. It is highly secure technology.
ii. Easy to setup.
iii. Easier detection of error.

Disadvantages of tree topology

i. If the server node is affected, its child node is also affected.
ii. Slow data transfer rate.
iii. Difficulty in maintenance and configuration.

6) Hybrid Topology

Hybrid topology is a type of network topology in which two or more different topologies are integrated or combined to lay out a network.

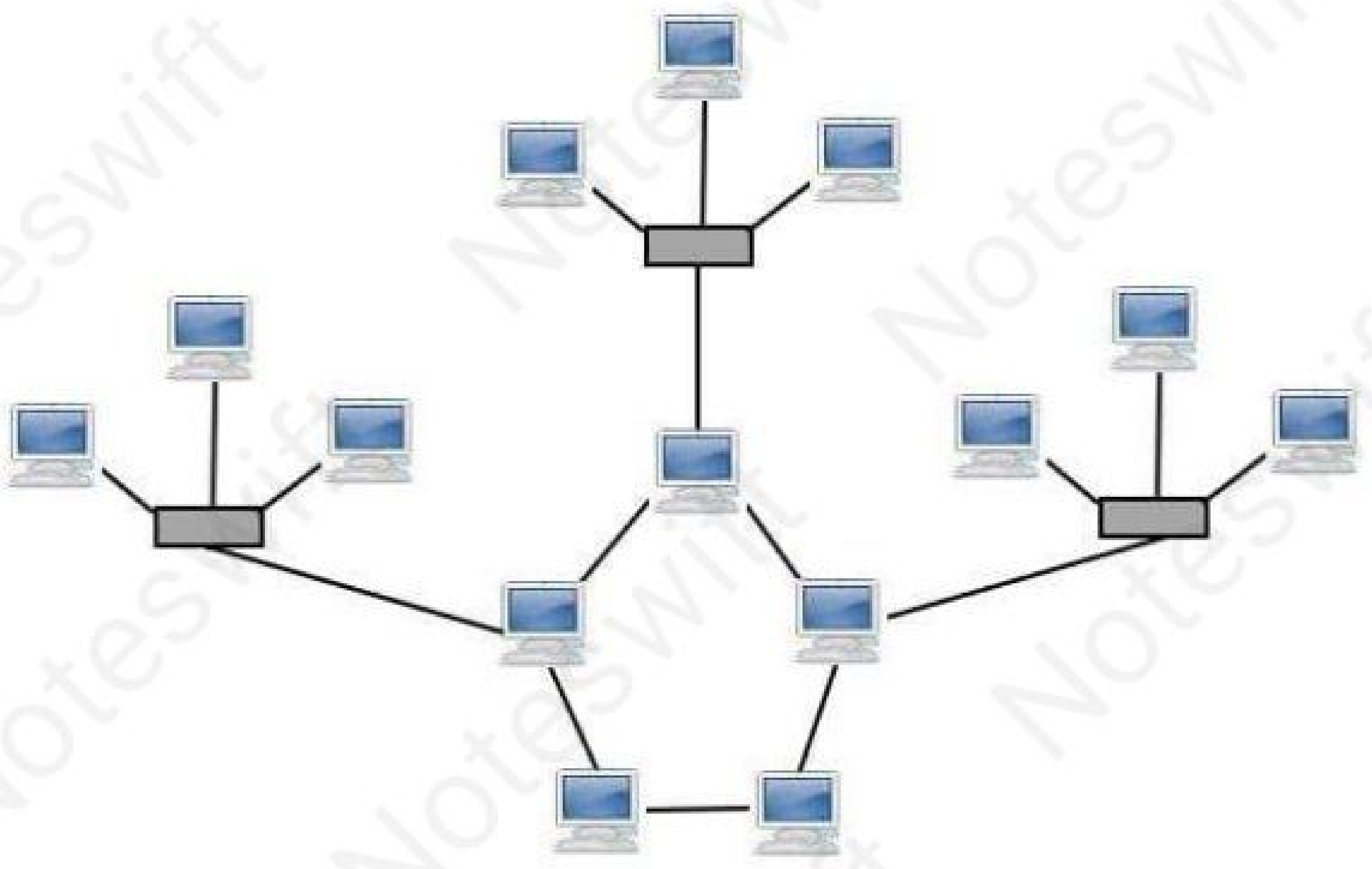


Fig: - Hybrid Topology

Advantages of hybrid topology

i. Easy to setup.
ii. Cheapest topology.
iii. More flexible.

Disadvantages of hybrid topology

i. Data collision.
ii. Depends on main wire and node.
iii. Slow data transfer rate.

Some basic terms and tools in computer network

There are so many basic terms and tools in computer network. Some of them are explained below:

a) **Packet tracer:** Packet tracer is a software by which we can verify the path of a packet through the layers to its destination.
b) **Remote login:** Remote login, also known as remote access, is the ability to access the data stored on a computer from a remote location.
c) **IP address:** IP stands for Internet Protocol, which is the set of rules governing the format of data sent via the internet or a local network. They can be static, dynamic, private and public. IPV_4 has 2^{32} addresses whereas IPV_6 has 2^{128} addresses.
d) **Subnet mask:** A subnet mask is a 32-bit number created by setting host bits to all 0s and setting network bits to all 1s. In this way, the subnet mask separates the IP address into the network and host addresses. The “255” address is always assigned to a broadcast address, and the “0” address is always assigned to a network address.
e) **Gateway:** A gateway is a network node used in telecommunications that connects two different transmission protocols together.
f) **MAC address:** A MAC address (media access control address) is a 12-digit hexadecimal number assigned to each device connected to the network.
g) **Router:** A router receives and sends data on computer networks. Routers are sometimes confused with network hubs, modems or network switches.
h) **Switch/Hub:** Hub and switch are the network connecting devices, both help to connects various devices. Hub works at the physical layer and transmits the signal to the part. Switch route the information and send it over the network.

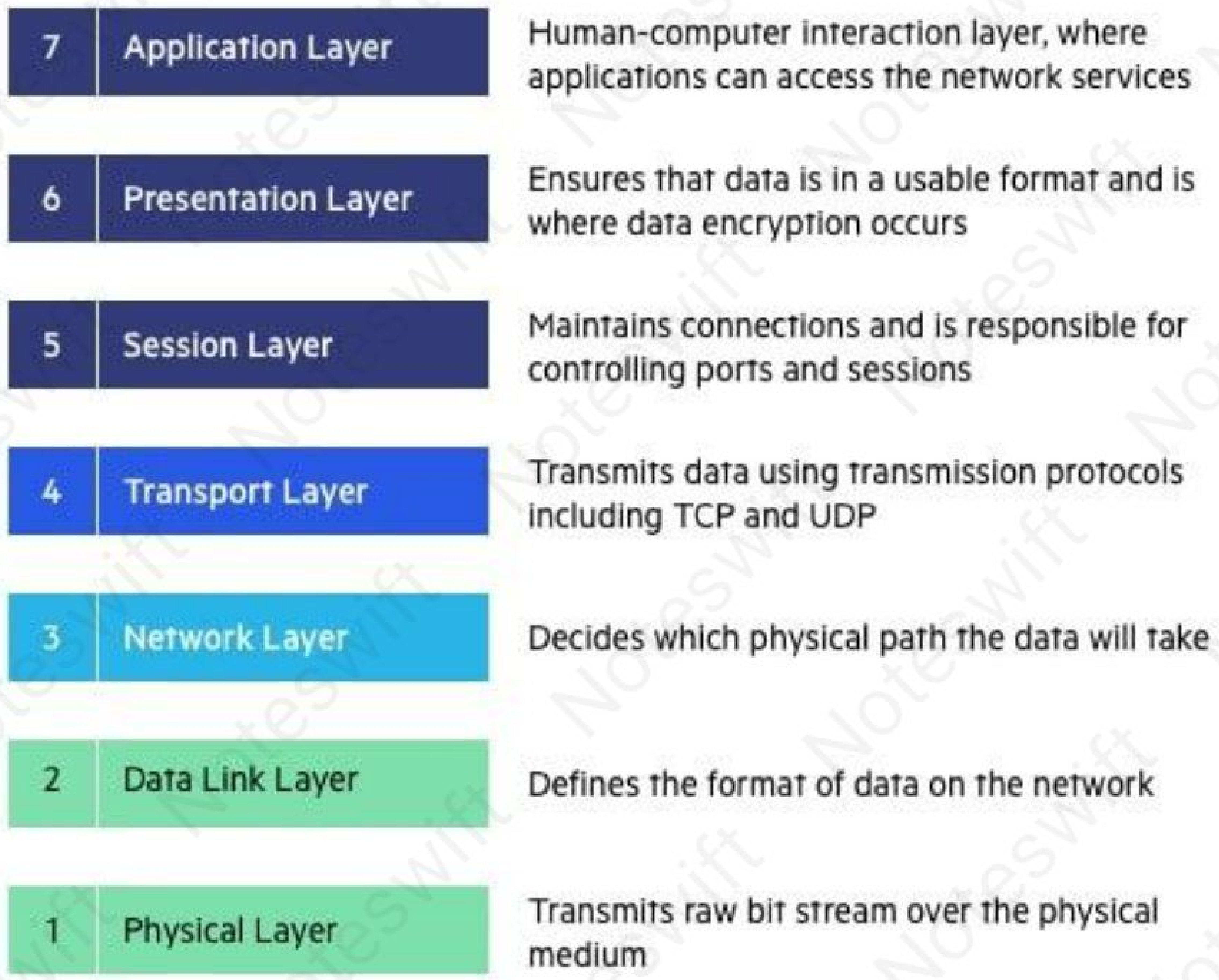
i) **Modem:** A modem is a hardware which connects to a computer, broadband network or wireless router. Modem stands for modulator-demodulator.

j) **NIC card:** A NIC card provides a computer with a dedicated, full-time connection to a network. Each card represents a device and can prepare, transmit and control the flow of data on the network.

OSI Reference Model

An OSI stands for open system inter-connection, is an ISO certified model that describes how information is transmitted from an application of one computer to other.

It consists of 7 layers each of them is responsible for establishing a computer network.



7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

Internet Protocols

Protocols are the set of rules that controls and coordinates the transmission of message over the network, which are responsible for successful communication between different networking devices.

Types of protocols

Some standard protocols are explained below:

i. **TCP: -** TCP, transmission control protocol, is responsible for dividing the data packets into smaller pieces which can be then transferred from one location to another using IP.

ii. **IP: -** IP, Internet Protocol, is responsible for providing the route to the data while transferring through different medium or channels.

iii. **FTP: -** FTP, File Transfer Protocol, is responsible for transferring the files (uploading or downloading) over the network.

iv. **SMTP and POP: -** SMTP stands for Simple Mail Transfer Protocols whereas POP stands for Post Office Protocols. These protocols are used to transmit the data from one mail server to another mail server.

v. **HTTP: -** HTTP, Hypertext Transfer Protocol, is responsible for displaying the web contents (text, images, audio, video, even programming etc.). These days HTTPS is in trend because it is more secure than HTTP and uses encryption and decryption technology.