COMPUTER NETWORK

UNIT 2

LOCAL AREA NETWORK

Requirements to set up LAN Network:

- **Workstation/Personal devices:** The computing devices that will be part of the network . Example laptop, computer, mobile phones, etc.

- **Network devices:** A router and a switch are fundamental. The router connects your LAN to the internet, while the switch connects various devices within the LAN . Example router, switch, modem.

- **Sharing resources:** These are optional, if your enterprise requires shared resources . Example printers, disk drives, etc.

- **wired LAN :** Ethernet cables, wires for connecting other devices

- **wireless LAN:** Wi-Fi

Proccess of design LAN

- **Assess Requirements and Goals**:
  - Understand the client’s needs, including the number of users, devices, and applications.
  - Identify specific requirements such as data speed, security, and scalability.
- **Network Topology**:
  - Choose an appropriate network topology (e.g., star, bus, ring) based on the organization’s layout and requirements.
  - Consider factors like ease of expansion, fault tolerance, and cost.

Continue……

- **Device Selection**:
  - Select switches, routers, and access points (APs) based on the network's scale and functionality. Select switch or router with enough ports to connect all workstations within the network. The choice of networking device is based on the requirements of the network.
  - Consider features like Power over Ethernet (PoE) for wireless APs and IP telephony.
- **IP Addressing and Subnetting**:
  - Plan IP address allocation, including subnet masks and addressing schemes.
  - Ensure efficient utilization of IP addresses and avoid conflicts.
- **Physical Cabling and Connectivity**:
  - Determine cable types (e.g., Ethernet, fiber) and their routes.
  - Properly terminate cables and connect devices (computers, printers, servers). Connect all the devices using wires to configure a LAN network. Standard Ethernet cables are used to connect workstations and servers while Ethernet crossover cable is used to connect the switch to cable routers by connecting the standard port of the switch with router's LAN port. For wireless LAN, connect all the devices to Wi-Fi with SSID (Service Set Identifier) provided by the router or switch to configure the LAN network.

  - Wired LAN is set up using Ethernet cables while wireless LAN is set up using Wi-Fi that connects network devices without making any physical connection. A wired LAN network is more secure than a wireless LAN network but it is difficult to relocate.

Continue……

- **Network Security**:
  - Implement security measures such as firewalls, VLANs, and access control lists (ACLs).
  - Protect against unauthorized access and data breaches.
- **Testing the network and Validation**:
  - Conduct initial testing to verify connectivity, performance, and functionality.
  - Address any issues or bottlenecks.
  - Test each of the workstation connected to the network and ensure every workstation have access to network services.
- **Monitoring and Management**:
  - Set up network monitoring tools to track performance, detect anomalies, and troubleshoot.
  - Regularly review logs and manage network devices.
- **Documentation**:
  - Document the network design, including diagrams, IP assignments, and device configurations.
  - Maintain accurate records for future reference.
- Remember, a well-designed LAN ensures reliable communication and efficient resource utilization.

Advantages of LAN

1. It is an easy and cheap way of communication within a small geographical location.
2. It is easy to expand the network by connecting workstations to a central server.
3. It is easy to manage the resources and data from the central server.
4. It is more secure since data is stored on a central server which denies illegal access to data.
5. It has high data transmission rates.

Disadvantages of LAN

- It has a high initial setup cost.
- It violates the privacy of network users as administrators have access to all their data and files.
- It can face security issues if the central server is not properly secured.
- It needs regular maintenance to deal with issues such as software installations, hardware failures, cable disturbances, etc.
- It restricts the size of the network.

Steps to set up and configure LAN

- **1. Identify network services and resources**
- Start by listing all the services and resources that will be shared across the network. This could include file servers, printers, and internet access.
- Knowing what needs to be shared helps in selecting the right hardware and software, ensuring that all networking needs are met. You can use a spreadsheet to organize these resources, noting their locations and access requirements.

Continue…..

- **2. Select and prepare networking devices**
- Choosing the right switch and router is crucial. Make sure these devices have enough ports for all your workstations and other hardware. Update the firmware to the latest versions to ensure you’re getting the best performance and security features.
- **3. Plan your network architecture**
- Before you start connecting cables, you can either use network design software such as Cisco Packet Tracer or pen and paper to sketch out a network diagram. This will serve as your blueprint for device placement, cable lengths, and types. A well-planned architecture minimizes potential issues and simplifies troubleshooting down the line.

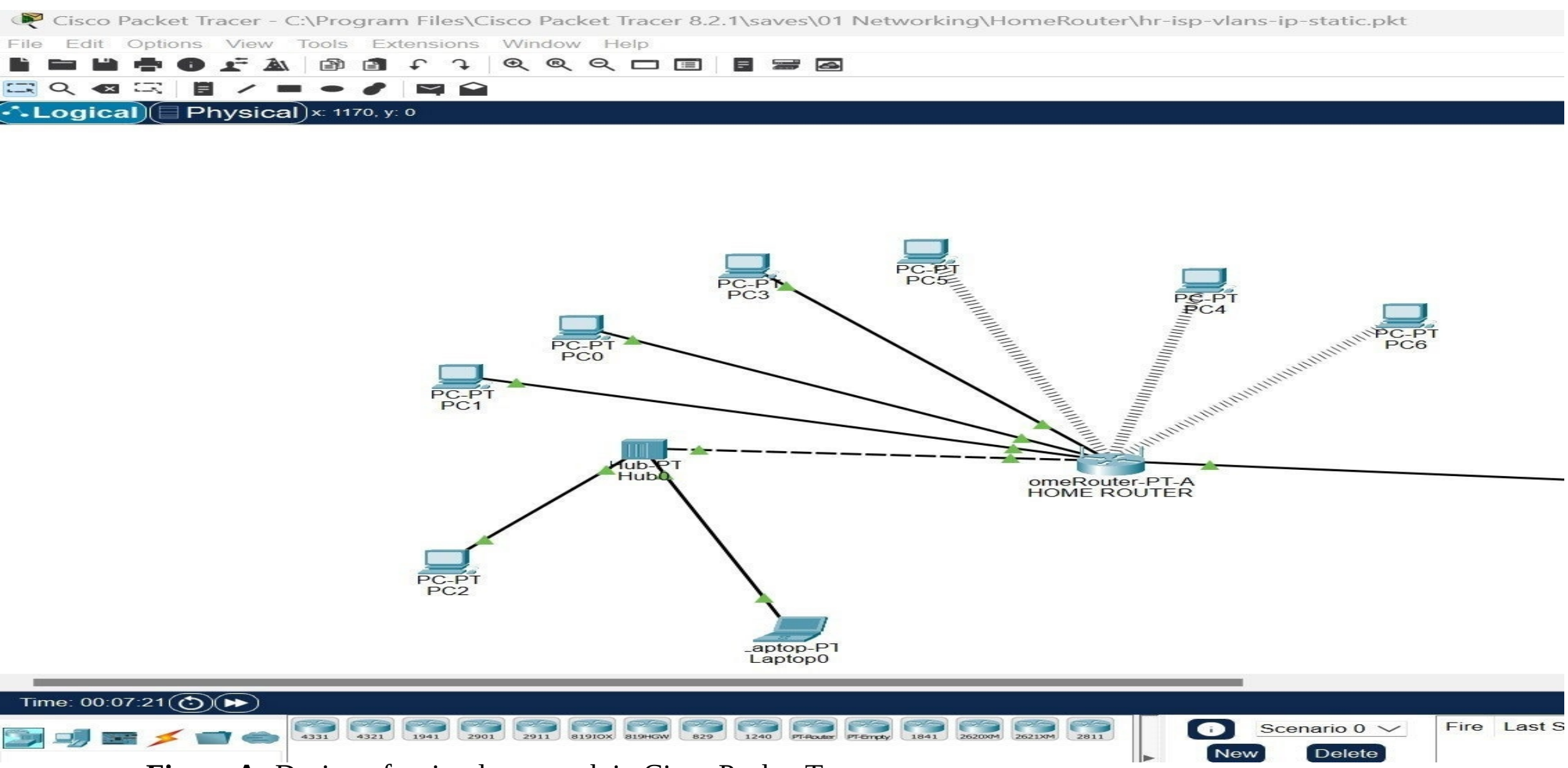


Figure A: Design of a simple network in Cisco Packet Tracer.

Continue……

- **4. Configure IP addressing**
- IP addressing is a critical aspect of network setup. Decide whether to use static or dynamic IP addresses. Static IPs are often used for servers and network devices, while dynamic IPs can be assigned to workstations through DHCP.
- For static IPs, you'll need to manually enter IP addresses for each device. This is often done through each device's settings menu. It's also possible to enable DHCP for dynamic IPs on your router via its admin panel to automatically assign IPs to connected devices.
- **5. Cable and connect devices**
- Based on your network diagram, start connecting devices using the appropriate cables. Remember to keep the process neat. Make sure to use quality cables and connectors to minimize signal loss and potential issues. Test each connection as you go along to ensure it's secure and functional.
- **6. Initial testing**
- Once all devices are connected, perform an initial round of tests. Check if all devices can communicate with each other, access the internet, and use shared resources. Resolve any issues before moving to the next step.

Continue….

- **7. Monitor and manage**
- While you could stop after Step 6, it will serve you better in the long run to ensure that your LAN is not just up and running, but that it stays that way. This is done by keeping an eye on your network's performance after confirming that it's functional.
- Use network monitoring and management tools like Wireshark and SolarWinds Network Performance Monitor to monitor traffic, bandwidth usage, and any unauthorized access attempts.
- **8. Document your network**
- Documentation is often overlooked, but is crucial for effective network management. Keep a record of all configurations, IP addresses, and device placements. This documentation will be invaluable for troubleshooting and future network expansions

Testing the established LAN

- Testing an established **Local Area Network (LAN)** ensures its reliability and performance. Testing an already installed LAN means checking whether all devices, connections, and services are working correctly. Here are some methods to test your LAN:

1. Check Physical Connections

Start with the basics because many network issues come from simple faults.

- ❖ Ensure all Ethernet cables (UTP) are properly connected
- ❖ Check switch/router power status
- ❖ Look at LED indicators (blinking lights = active connection)
- ❖ Replace any damaged cables

2. Verify IP Configuration

Check whether devices are correctly configured.

• On Windows: use ipconfig

• On Linux: use ifconfig or ip addr

Confirm:

a. IP address

b. Subnet mask

c. Default gateway

If the IP starts with 169.254.x.x, it indicates a problem (no DHCP).

3. Test Connectivity (Ping Test)

Use ping to check communication between devices.

- ❖ Ping localhost (127.0.0.1) for tests your own system
- ❖ Ping another computer in the LAN
- ❖ Ping the default gateway (router)

Results:

- Reply → connection is OK
- Request timed out → problem exists

4. Check Network Services

Ensure important services are working:

- ❖DHCP server can assigns IP addresses
- ❖DNS server can resolves domain names
- ❖File sharing and printer services

Continue…….

5.Use Advanced Diagnostic Tools

a. tracert / traceroute for checks path of data
b. netstat for shows active connections
c. Wireshark for analyzes network traffic

6. Check Network Performance

- Monitor speed and latency
- Identify bottlenecks or congestion

Those are some steps you can use for testing established LAN.

Application of LAN

- **Resource sharing:** LAN network allows workstations connected to the network to share resources such as printers, scanners, CD drives, etc. which reduces the cost of the set up of the network.
- **Software sharing:** LAN network allows to share a single copy of licensed software among workstations connected to the network instead of purchasing separate software for each computer.
- **Internet sharing:** LAN network facilitates sharing of internet connection among all the devices connected to the network.

Continue……

- **Data sharing:** LAN network allows different workstations to share the data and files with each other. It also allows access to data stored on the central server.
- **Communication:** Devices connected to a LAN network can communicate with each other.

All these application can be done at home network,education institution, Entertainment and media etc.

NETWORK INTERFACE CARD (NIC),

- A **Network Interface Card (NIC)**, also known as a **network adapter** or **LAN adapter**, is a vital hardware component that enables computers and servers to connect to networks.
- A NIC is typically a **circuit board** installed in a computer.
- Its primary purpose is to provide a dedicated network connection for the device.

- NICs allow computers to communicate with other devices on the network, whether through wired (Ethernet) or wireless connections.

- **Types of NICs**
  1. **Wired NICs**:

     These include traditional Ethernet cards that connect via cables.

  2. **Wireless NICs (Wi-Fi)**:

     They use antennas to transmit data to Wi-Fi routers using radio frequency signals. You'll find these in laptops and desktops alike.

- **Components of a NIC**:
  - **Controller**: Functions like a mini CPU, processing received data.
  - **Boot ROM socket**: Enables boot ROM capability, allowing diskless workstations to connect to the network securely.
  - **NIC port**: Connects directly to Ethernet cables or transceivers, transmitting and receiving electronic signals.
  - **Bus interface**: Plugged into the computer or server’s expansion slot.
  - **LED indicators**: Help users identify the network card’s working status.

- **NIC Location**:
  - NICs were initially connected to computers via an **expansion card** that plugged into the computer bus.
  - Nowadays, motherboard manufacturers often integrate the NIC directly into the motherboard, either in the chipset or with a dedicated Ethernet chip.
  - Some computers still have NICs installed in separate slots, especially when connecting to non-Ethernet networks.
  - Portable NICs can also connect via **USB**.

- **Function**:

At the **TCP/IP layer**, a NIC acts as an interface:

1. It **transmits signals** at the **physical layer**, converting digital data into electrical signals.
2. It **delivers data packets** at the **network layer**, ensuring seamless communication . When you request a web page, the NIC:
   - Retrieves data from your device.
   - Sends the data to the internet server.
   - Receives the required data back from the internet for display

- **The NIC Driver**:
  - The NIC’s driver is **essential** for its functioning.
  - **Interface**: It acts as the interface between software running on the computer and the NIC hardware.
  - **Installation**: The driver software is installed in the computer’s operating system, and the operating system’s **kernel** controls access to the driver and the NIC

DIAGNOSING EQUIPMENTS IN COMPUTER NETWORKS

- When it comes to diagnosing and troubleshooting issues in computer networks, there are several tools available. These tools help network administrators and technicians identify problems, analyze network performance, and ensure smooth functioning.
- Remember that these tools serve different purposes, and using them collectively can help you diagnose and resolve network problems effectively. Let's explore some of the essential diagnostic tools:

1. Software Diagnostic Tools

These are command-line or application-based tools used to test network connectivity and performance.

A. Ping

Ping is a basic command-line utility used to test the reachability of a host (computer or server) on a network. Tests if one device can communicate with another. It sends an ICMP (Internet Control Message Protocol) echo request to the target host and waits for an echo reply. Helps detect if a host is reachable.

Useful for checking network connectivity and response times.

Example usage: ping google.com

B. Traceroute (Tracert)

Shows the path data takes from source to destination.

It lists the probable hops (intermediate routers) between your computer and the target address.

Helps identify network latency and routing issues.

Example usage: traceroute google.com

Helps identify where a connection fails.

C. Ipconfig / Ifconfig

Ipconfig (Windows) and Ifconfig (Linux) display network adapter information.

They report IPv4 and IPv6 addresses, subnets, default gateways, and other network configuration details.

Useful for checking IP settings

Displays IP address and network configuration.

Helps diagnose incorrect settings.

D. Wireshark:

Wireshark is a powerful free packet sniffer.

It captures and analyzes network traffic, allowing you to inspect packets in detail.

Useful for diagnosing complex issues, security analysis, and troubleshooting.

Example usage: Install Wireshark and start capturing packets

E. Netstat

Shows active connections and ports. Useful for detecting unauthorized connections.
It shows information about open ports, established connections, and listening services.

Useful for monitoring network activity.

Example usage: netstat –a

F. Nslookup

Nslookup available for Windows, Unix, Linux, and macOS) provides DNS server diagnostics.

It helps resolve domain names to IP addresses and vice versa.

Useful for troubleshooting DNS-related problems.

Example usage: nslookup google.com

2. Hardware Diagnostic Tools

These are physical devices used to test cables and network equipment.

I. Cable Tester

Checks if network cables are working properly.

Detects broken or mis wired cables.

II. Tone Generator and Probe

Used to trace cables in walls or panels.

III. Multimeter

Measures electrical signals in cables and devices.

IV. Loopback Plug

Tests network ports (NIC or switch ports).

Network operating system(NOS)

- The basic definition of an **operating system** is that the operating system is the interface between the computer hardware and the user.
- In daily life, we use the operating system on our devices which provides a good GUI, and many more features.
- Similarly, a network operating system(NOS) is specialized software that facilitates communication and resource sharing among multiple devices and computers within a network.

A **Network Operating System** is software installed on a server (or sometimes on client machines) that enables:

- Communication between computers
- Sharing of resources (files, printers, internet)
- Centralized management of users, security, and data
- Unlike a normal OS (like Windows 10), a NOS is built specifically to **support networking functions**.

Examples of NOS include:

- Windows Server
- Linux (e.g., Ubuntu Server, Red Hat)
- UNIX

Types of Network Operating Systems

There are mainly two types of networks;

1. Peer to Peer:

Peer-to-peer network operating systems allow the sharing of resources and files with small-sized networks and having fewer resources. In general, peer-to-peer network operating systems are used on LAN. Example: Small office network

2. Client/server:

Client-server network operating systems provide users access to resources through the central server. This NOS is too expensive to implement and maintain. This operating system is good for the big networks which provide many services.

Central server controls the network. Clients request services from the server

- Example: School, bank, or company network

- **Features of NOS**:

  1. Resource Sharing: NOS allows printers, applications, and file systems to be shared across the network.

  2. Security: It provides features like user authentication and access control.

  3. Data Backup: NOS facilitates data backups.

  4. Inter-Networking: Enables communication between different networks.

- **Functions of NOS**:

1. User Account Management:

NOS creates and manages user accounts on the network.

2. Resource Access Control:

It controls access to resources (such as files, printers, and databases) on the network.

3. Communication Services:

NOS enables communication between devices on the network.

4. Monitoring and Troubleshooting:

It monitors and troubleshoots network issues.

5. Resource Configuration and Management:

NOS configures and manages network resources

Advantages of NOS:

1. **Stability**:

Centralized servers enhance stability.

2. Security:

Provide Good security features.

3. Technology Upgrades:

Easy implementation of new technology and hardware.

4. Remote Access:

Provides remote access to servers from different locations.

Disadvantages of Network Operating Systems

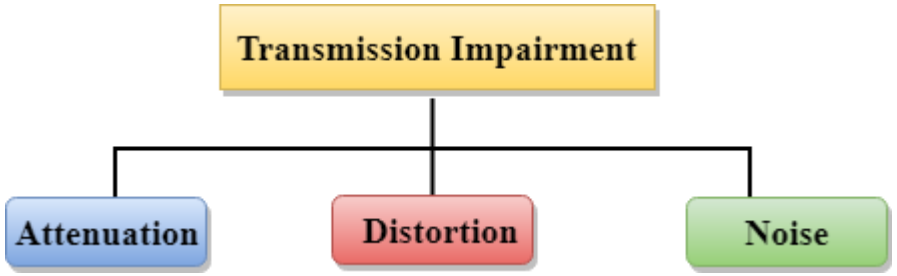
1. Depend on the central location to perform the operations.
2. High cost to buying server.
3. Regular updating and maintenance are required.

- **Examples of NOS**:
  - Microsoft Windows Server
  - UNIX/Linux
  - Artisoft’s LANtastic
  - Banyan’s VINEs

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).
- In a copper-based network, the bits in the form of electrical signals.
- In a fiber 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, fiber optics, atmosphere, water, and vacuum.
- The characteristics and quality of data transmission are determined by the characteristics of medium and signal.

Causes Of Transmission Impairment:

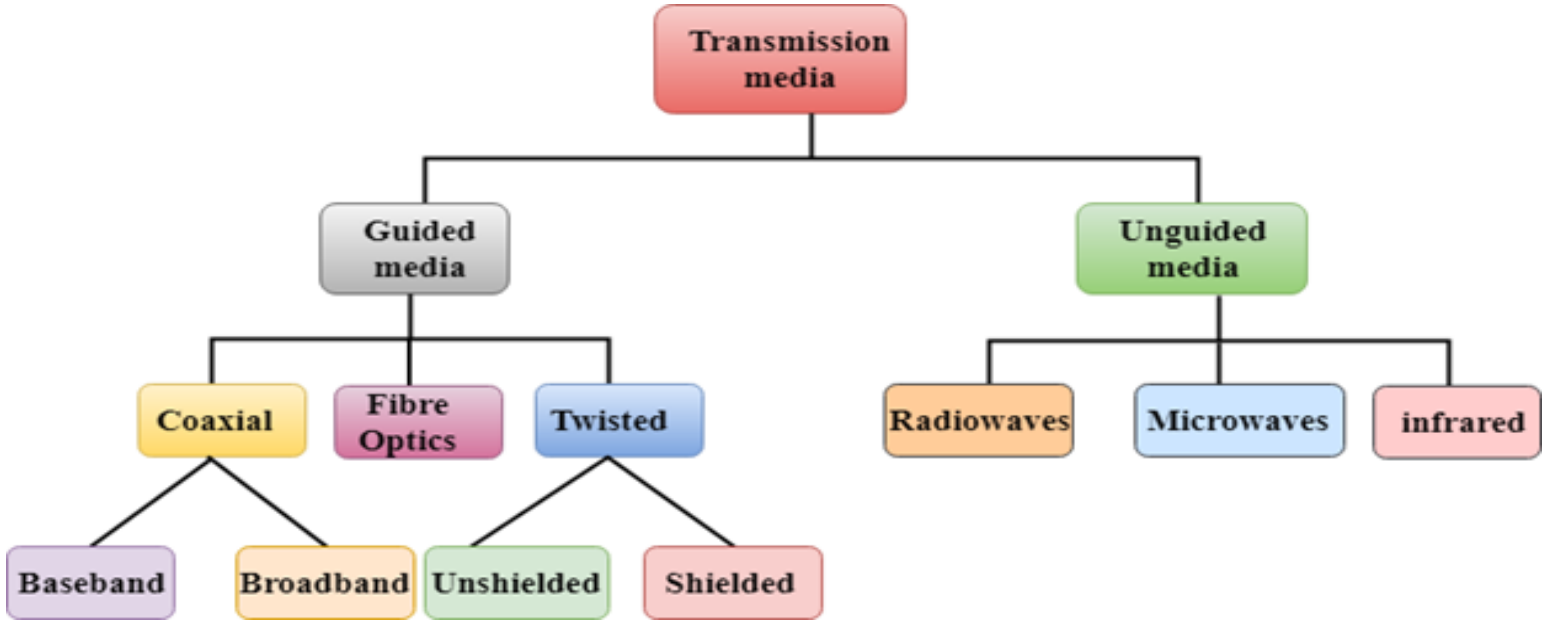


•**Attenuation:** Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.

•**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

Classification Of Transmission Media



GUIDED MEDIA

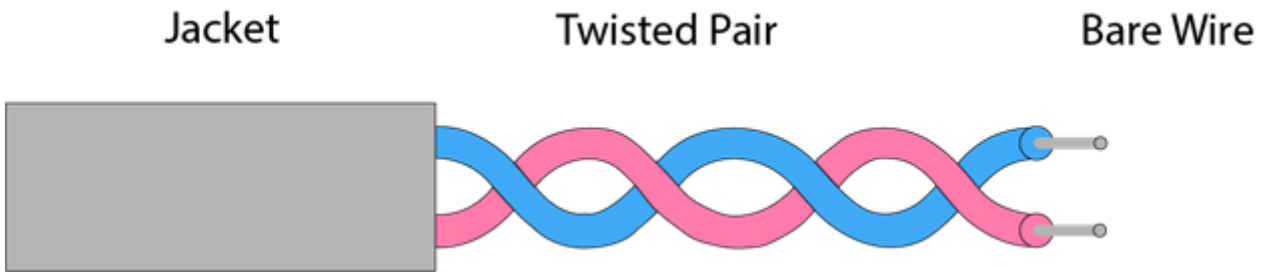
It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

TYPES OF GUIDED MEDIA

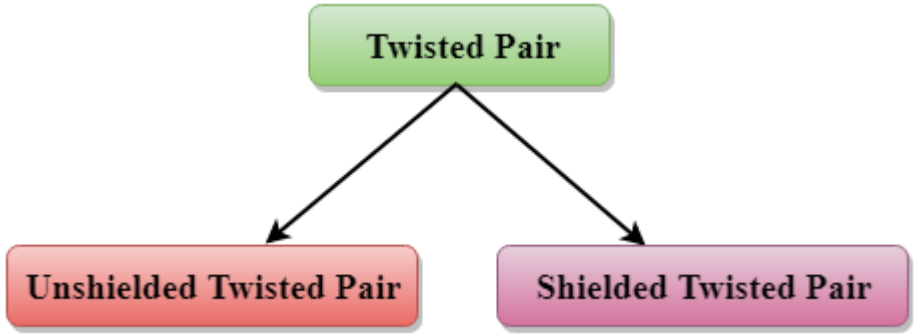
1. Twisted pair
2. Coaxial
3. Optical fibre

TWISTED PAIR

- Twisted pair is a physical media made up of a pair of cables twisted with each other. 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.
- A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.
- The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.



Types of Twisted pair



UNSHIELDED TWISTED PAIR

An unshielded twisted pair is widely used in telecommunication.

- **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.

Advantages Of Shielded Twisted Pair:

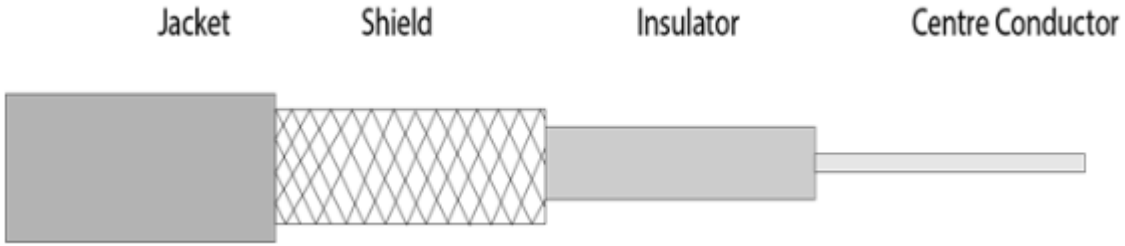
- The cost of the shielded twisted pair cable is not very high and not very low.
- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.
- It is shielded that provides the higher data transmission rate.

Disadvantages Shielded Twisted Pair

- 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.

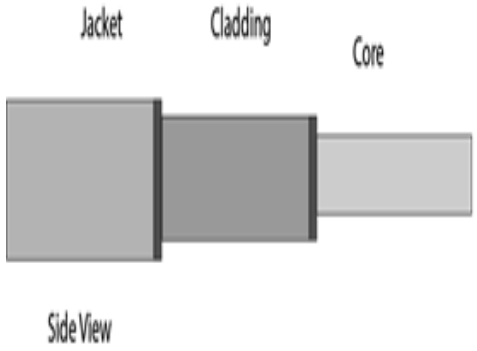
Disadvantages Of Coaxial cable:

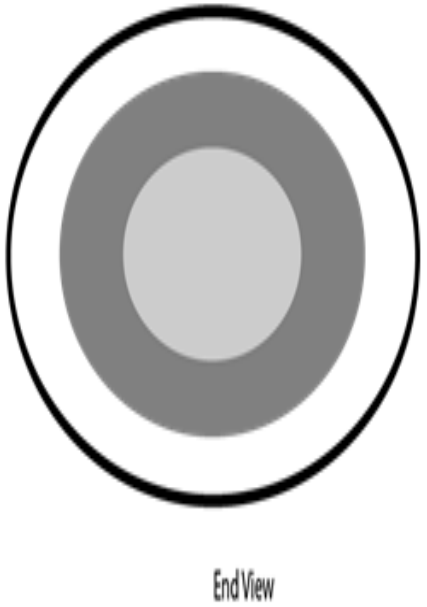
- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

FIBER OPTIC

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

- **Diagrammatic representation of fiber optic cable:**





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

•**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 fiber.

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

Advantages of fiber optic cable

- **Greater Bandwidth:** The fiber optic cable provides more bandwidth as compared copper. Therefore, the fiber optic carries more data as compared to copper cable.
- **Faster speed:** Fiber optic cable carries the data in the form of light. This allows the fiber optic cable to carry the signals at a higher speed.
- **Longer distances:** The fiber optic cable carries the data at a longer distance as compared to copper cable.
- **Better reliability:** The fiber 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:** Fiber optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

UNGUIDED TRANSMISSION

- An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.
- In unguided media, air is the media through which the electromagnetic energy can flow easily.

Unguided transmission is broadly classified into three categories:

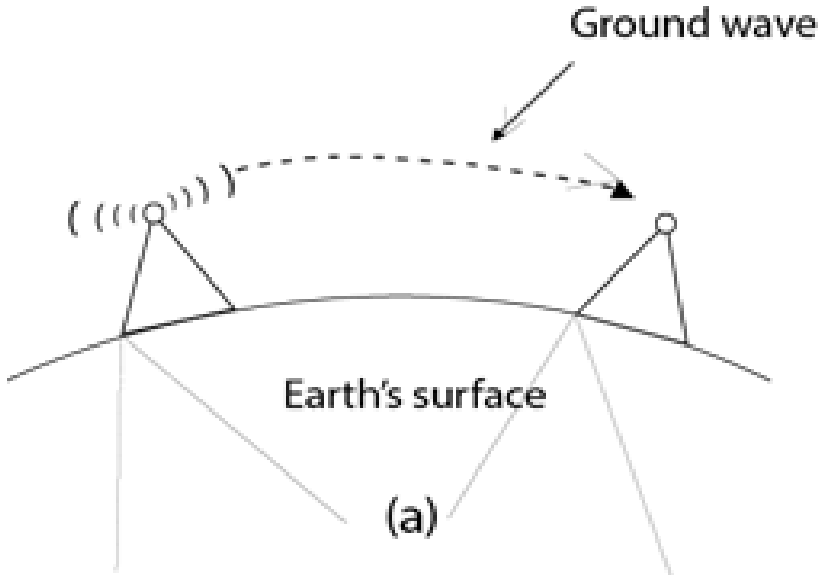
1.Radio waves

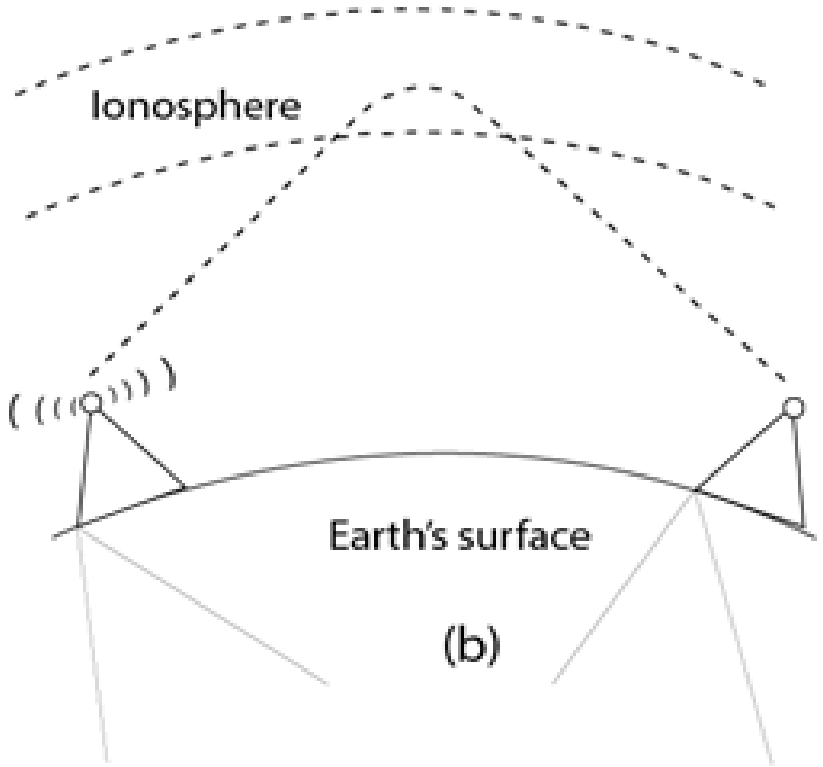
2. Microwaves

3. Infared

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

- Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.
- Microwaves are unidirectional; when an antenna transmits microwaves they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.
- **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.

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 Of Infrared:

- 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.

TRANSMISSION MODES

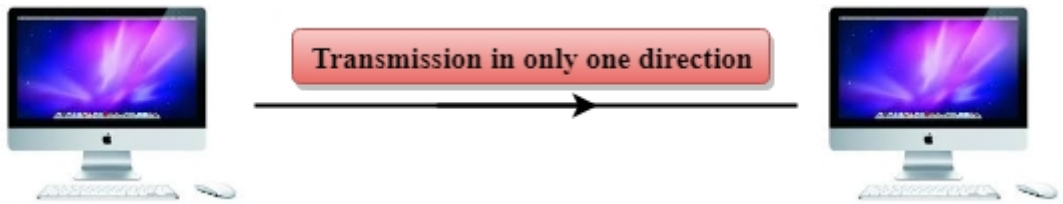
- The way in which data is transmitted from one device to another device is known as **transmission mode**.
- The transmission mode is also known as the communication mode.
- Each communication channel has a direction associated with it, and transmission media provide the direction. Therefore, the transmission mode is also known as a directional mode.
- The transmission mode is defined in the physical layer.

The Transmission mode is divided into three categories;

1. Simplex mode
2. Half-duplex mode
3. Full-duplex mode

SIMPLEX MODE

- In Simplex mode, the communication is unidirectional, i.e., the data flow in one direction.
- A device can only send the data but cannot receive it or it can receive the data but cannot send the data.
- The radio station is a simplex channel as it transmits the signal to the listeners but never allows them to transmit back.
- Keyboard and Monitor are the examples of the simplex mode as a keyboard can only accept the data from the user and monitor can only be used to display the data on the screen.
- The main advantage of the simplex mode is that the full capacity of the communication channel can be utilized during transmission.



Advantage of Simplex mode

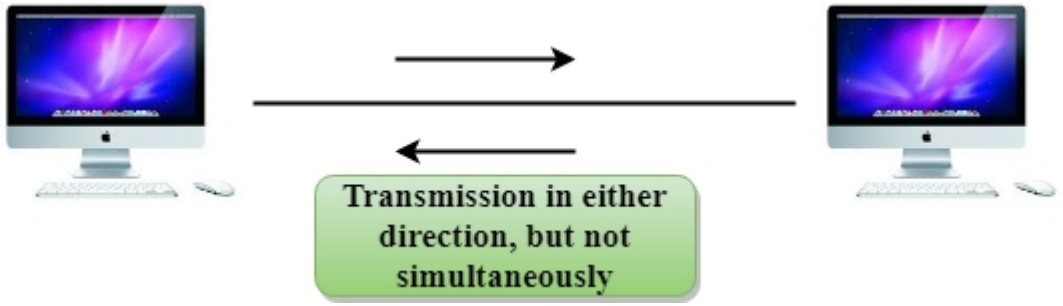
- In simplex mode, the station can utilize the entire bandwidth of the communication channel, so that more data can be transmitted at a time.

Disadvantage of Simplex mode

- Communication is unidirectional, so it has no inter-communication between devices.

HALF-DUPLEX MODE

- In a Half-duplex channel, direction can be reversed, i.e., the station can transmit and receive the data as well.
- Messages flow in both the directions, but not at the same time.
- The entire bandwidth of the communication channel is utilized in one direction at a time.
- In half-duplex mode, it is possible to perform the error detection, and if any error occurs, then the receiver requests the sender to retransmit the data.
- A **Walkie-talkie** is an example of the Half-duplex mode. In Walkie-talkie, one party speaks, and another party listens. After a pause, the other speaks and first party listens. Speaking simultaneously will create the distorted sound which cannot be understood.



Advantage of Half-duplex mode:

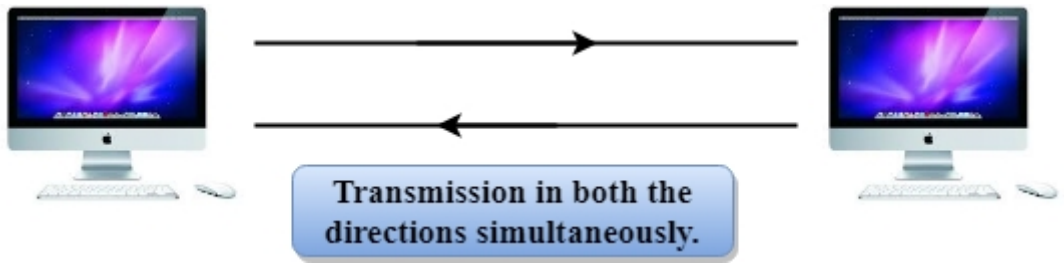
•In half-duplex mode, both the devices can send and receive the data and also can utilize the entire bandwidth of the communication channel during the transmission of data.

Disadvantage of Half-Duplex mode:

•In half-duplex mode, when one device is sending the data, then another has to wait, this causes

FULL-DUPLEX MODE

- In Full duplex mode, the communication is bi-directional, i.e., the data flow in both the directions.
- Both the stations can send and receive the message simultaneously.
- Full-duplex mode has two simplex channels. One channel has traffic moving in one direction, and another channel has traffic flowing in the opposite direction.
- The Full-duplex mode is the fastest mode of communication between devices.
- The most common example of the full-duplex mode is a telephone network. When two people are communicating with each other by a telephone line, both can talk and listen at the same time.



Advantage of Full-duplex mode:

•Both the stations can send and receive the data at the same time.

Disadvantage of Full-duplex mode:

•If there is no dedicated path exists between the devices, then the capacity of the communication channel is divided into two parts.