

Batch: A1 **Roll No.:** 16010120015

Experiment / assignment / tutorial No.__1__

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of the Staff In-charge with date

Experiment No. 1

TITLE: Study of Networking devices (Hub,router,Gateway,Switch etc) and Transmission Media

AIM: To study different Networking devices used in day- to-day networks.

Expected Outcome of Experiment:

CO: Explain the fundamentals of the data communication networks, reference models, topologies, physical media, devices, simulators and identify their use in day-to-day networks.

Books/ Journals/ Websites referred:

1. A. S. Tanenbaum, "Computer Networks", Pearson Education, Fourth Edition
2. B. A. Forouzan, "Data Communications and Networking", TMH, Fourth Edition

Pre Lab/ Prior Concepts: Basics of LAN and Connecting devices

New Concepts to be learned: Layer wise connecting devices

Stepwise-Procedure:

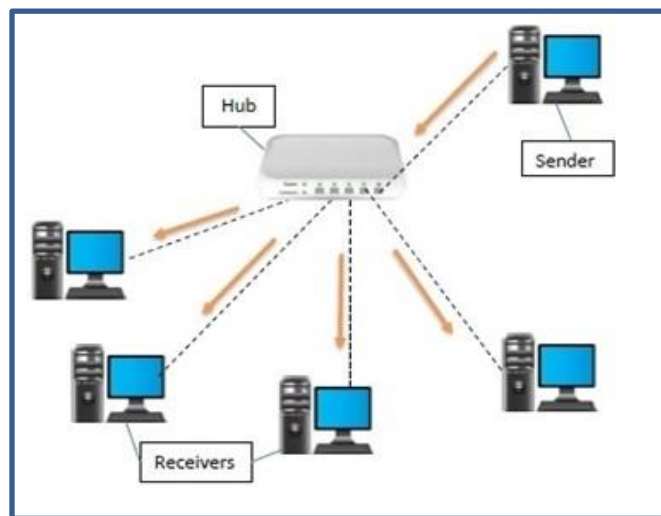
Study of Connecting Devices

Hub

A Hub is a physical layer networking device which is used to connect multiple devices in a network. Hub is used to connect computers in a LAN.

A Hub has many ports in it.

A computer which intends to be connected to the network is plugged in to one of these ports. When a data frame/packet arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination or not. On this network segment, all devices can communicate directly with each other.



Features

- A Hub is a non-intelligent network device that sends message to all ports.
- Hub is a passive device, and don't have any software associated with it.
- They generally have few ports of 4/12.

Hub broadcasts messages to all the devices connected to it Therefore they lack intelligence to compute transmission of data packets(Messages).

Types Of Hubs

- Passive Hubs.
- Active Hubs.
- Intelligent Hubs.

- **Passive Hubs** – A passive hub is just a connector. It connects the wires coming from different branches . Connect several networking cables together The signal pass through a passive hub without regeneration or amplification .
- **Active Hubs** – They regenerate or amplify the signal before they are retransmitted. They have their own power supply and serves both as a repeater as well as connecting centre.
- **Intelligent Hubs** – Intelligent hubs are active hubs that provide additional network management facilities. They can perform a variety of functions of more intelligent network devices like network management, switching, providing flexible data rates etc

Repeater

A Repeater is a network device that operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted and retransmit the refreshed signal.

Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data

When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength but they do not amplify the signal..
Digital repeaters can even reconstruct signals distorted by transmission loss.



Features Of Repeaters

- It is a 2-port device that reconstructs and regenerates weak signal and doesn't amplify the signal.
- Multiple LANs connected by a repeater can also be called as single LAN.

Types Of Repeaters

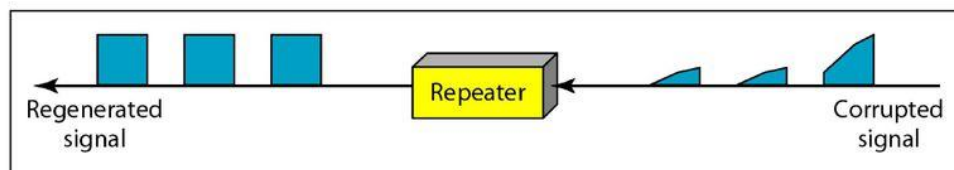
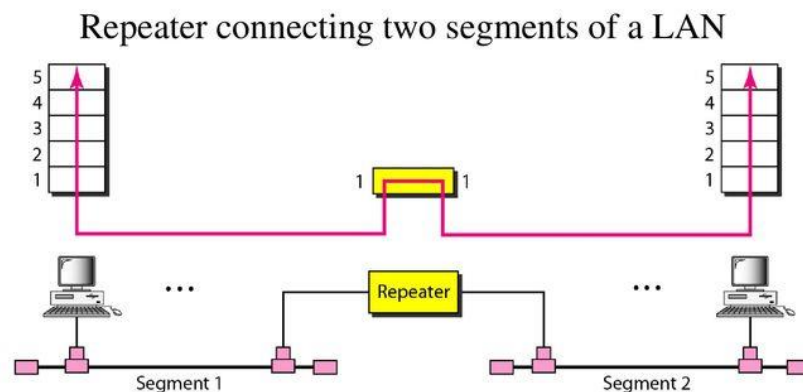
- Analog Repeaters – They only amplify the analog signal.
- Digital Repeaters – They reconstruct a distorted signal.
- Wired Repeaters – They are used in wired LANs.
- Wireless Repeaters – They are used in wireless LANs and cellular networks.
- Local Repeaters – They connect LAN segments separated by small distance.
- Remote Repeaters – They connect LANs that are far from each other.

Advantages of Repeaters

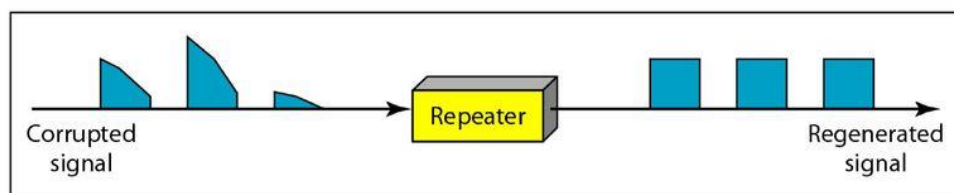
- Repeaters are simple to install
- They are cost effective.
- Repeaters don't require any processing overhead.
- They can connect signals using different types of cables.

Disadvantages of Repeaters

- Repeaters cannot connect dissimilar networks.
- They cannot differentiate between actual signal and noise.
- They cannot reduce network traffic or congestion.
- Most networks have limitations upon the number of repeaters that can be deployed.



a. Right-to-left transmission.



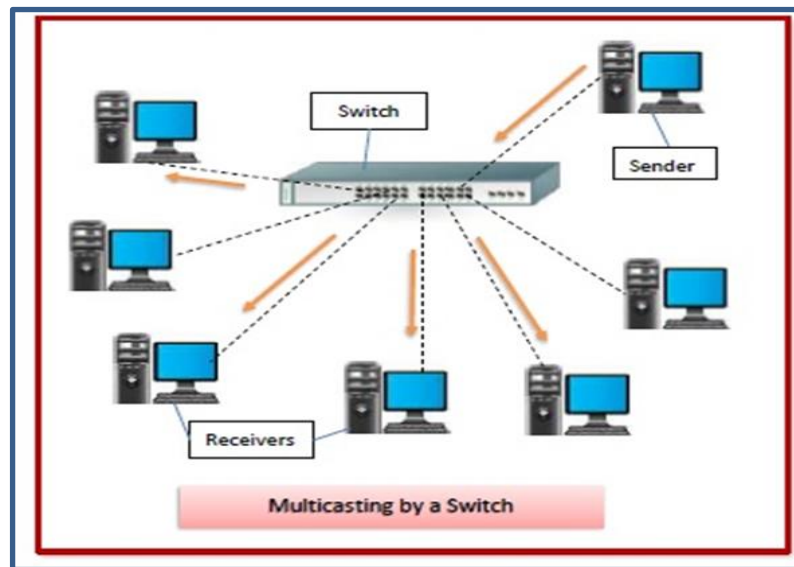
b. Left-to-right transmission.

Function of a repeater

Switch

A Switch is a multiport bridge with a buffer and a design that can boost its efficiency and performance. A switch is a data link layer device. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.

The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. It supports unicast, multicast as well as broadcast communications. In other words, the switch divides the collision domain of hosts, but broadcast domain remains the same.



Features of Switches

- Switch is an intelligent network device that can be conceived as a multiport network bridge. It uses packet switching technique to receive and forward data packets from the source to the destination device.
- It supports (unicast) one-to-one, (multicast) one-to-many and broadcast one-to-all communications.
- Switches are active devices, equipped with network software and network management capabilities.
- Switches can perform some error checking before forwarding data to the destined port.
- The number of ports is higher – 24/48.

Types Of Switch

- Unmanaged Switch
- Managed Switch
- LAN Switch

Advantages of Switches

- ➡ They increase the available bandwidth of the network.
- ➡ They help in reducing workload on individual host PCs.
- ➡ They increase the performance of the network.
- ➡ Networks which use switches will have less frame collisions. This is due to the fact that switches create collision domains for each connection.
- ➡ Switches can be connected directly to workstations.

Disadvantages of Switches

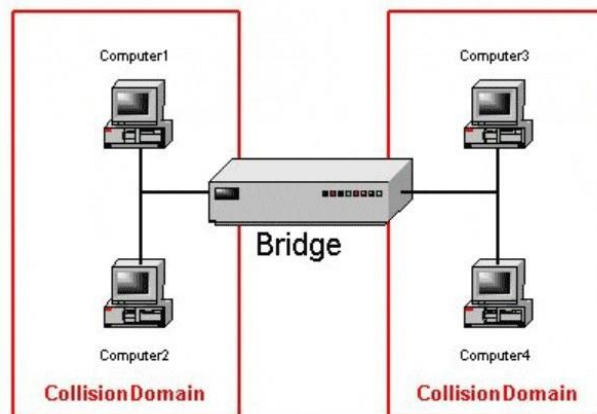
- ➡ They are more expensive compare to network bridges.
- ➡ Network connectivity issues are difficult to be traced through the network switch.
- ➡ Broadcast traffic may be troublesome.
- ➡ If switches are in promiscuous mode, they are vulnerable to security attacks e.g. spoofing IP address or capturing of ethernet frames.
- ➡ Proper design and configuration is needed in order to handle multicast packets.
- ➡ While limiting broadcasts, they are not as good as routers.

Bridge

A Bridge is a network device that connects multiple LANs (local area networks) together to form a larger LAN. The process of aggregating networks is called network bridging. A bridge connects the different components so that they appear as parts of a single network.

A network bridge is a device that divides a network into segments. Each segment represents a separate collision domain, so the number of collisions on the network is reduced. Each collision domain has its own separate bandwidth, so a bridge also improves the network performance.

Bridges operate at the data link layer of the OSI model and hence also referred as Layer 2 switches. The main function of this is to examine the incoming traffic and examine whether to filter it or forward it. If the bridge determines that the destination host is on another segment of the network, it forwards the frame to that segment.



Features Of Bridges

- Increases network reliability and makes the network easier to maintain by subdividing LAN into smaller segments which reduces congestion.
- It is a 2-port device.
- Improves network performance as each collision domain has separate bandwidth.
-

Types Of Bridge

- Transparent Bridges
- Source Routing Bridges

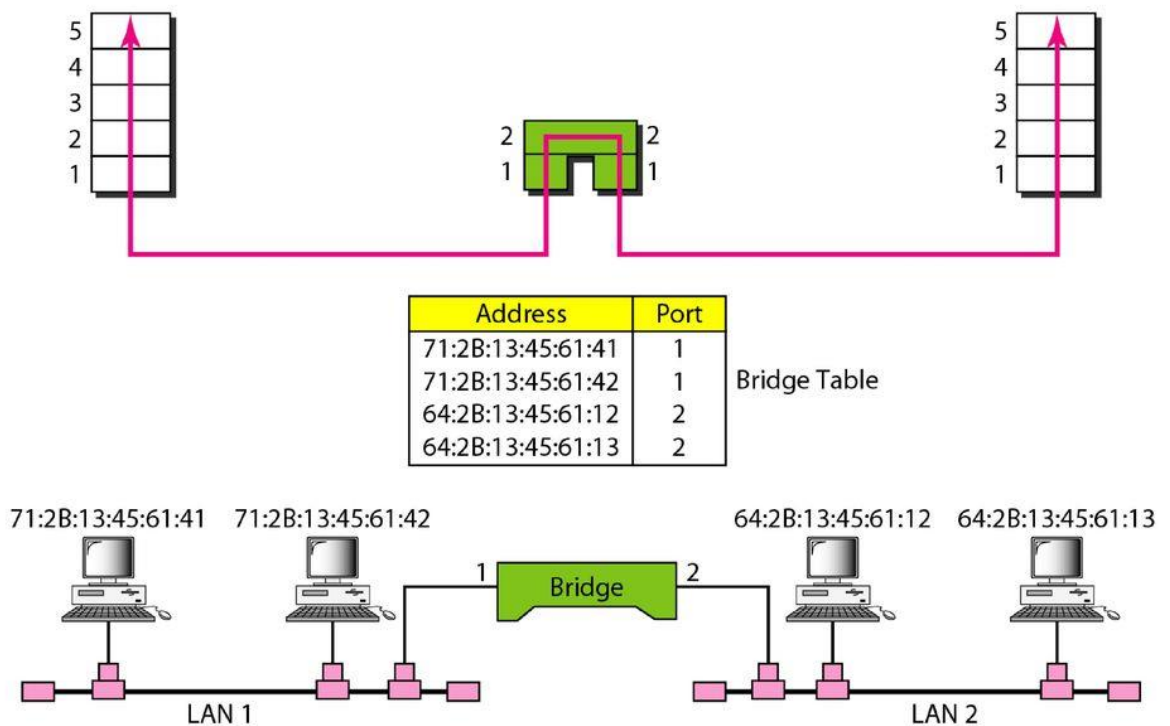
Advantages of using a bridge

- Extend physical network
- Reduce network traffic with minor segmentation
- Creates separate collision domains
- Reduce collisions
- Connect different architecture

Disadvantages of using bridges

- Slower than repeaters due to filtering
- Do not filter broadcasts
- More expensive than repeaters

A bridge connecting two LANs



A bridge does not change the physical (MAC) addresses in a frame.

Router

Routers are networking devices operating at layer 3 or a network layer of the OSI model. They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.

It is also known as an **intelligent device** as it can calculate the best route to pass the network packets from source to the destination automatically. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.



Characteristics

- Routers constantly monitor the condition of the network.
- Routers connects different networks together and sends data packets from one network to another .They typically provide some level of redundancy so that they are less susceptible to catastrophic failure.
- Routers are multiport devices with high - speed backbones.
- Routers also support filtering and encapsulation like bridges.

Types Of Router

- Wireless Router
- Broadband Routers
- Core Routers

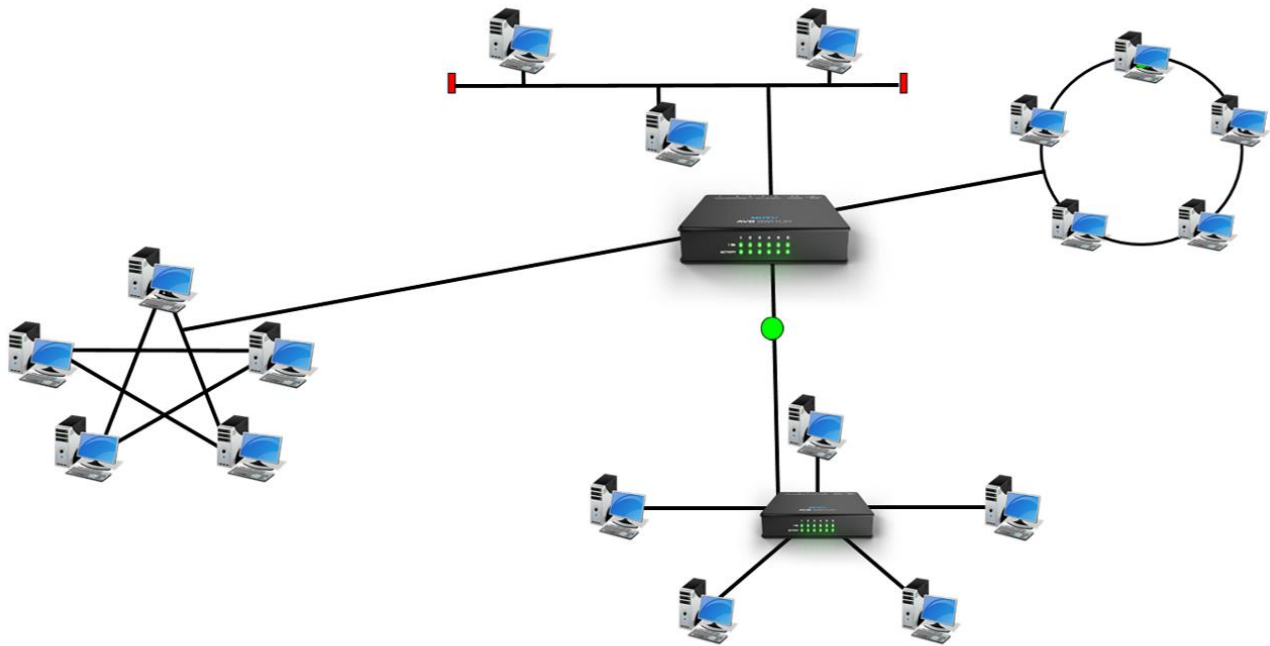
Advantages and Disadvantages of Routers

Advantages

- provide sophisticated routing, flow control, and traffic isolation
- are configurable, which allows network manager to make policy based on routing decisions
- allow active loops so that redundant paths are available

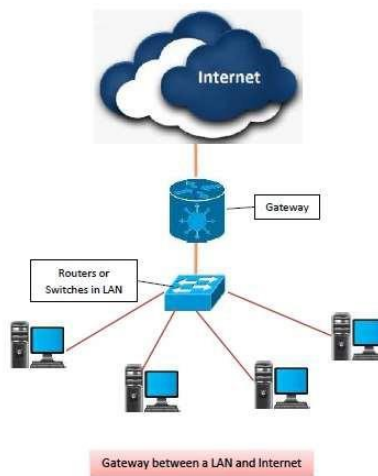
Disadvantages

- are protocol-dependent devices that must understand the protocol they are forwarding.
- can require a considerable amount of initial configuration.
- are relatively complex devices, and generally are more expensive than bridges.



Gateway

A Gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models/transmission protocols. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway.



Features of Gateway

- A gateway operates as a protocol converter, providing compatibility between the different protocols used in the two different networks.
- It uses packet switching technique to transmit data across the networks.
- Gateway is located at the boundary of a network and manages all data that inflows or outflows from that network.
- It forms a passage between two different networks operating with different transmission protocols.

Types Of Gateways

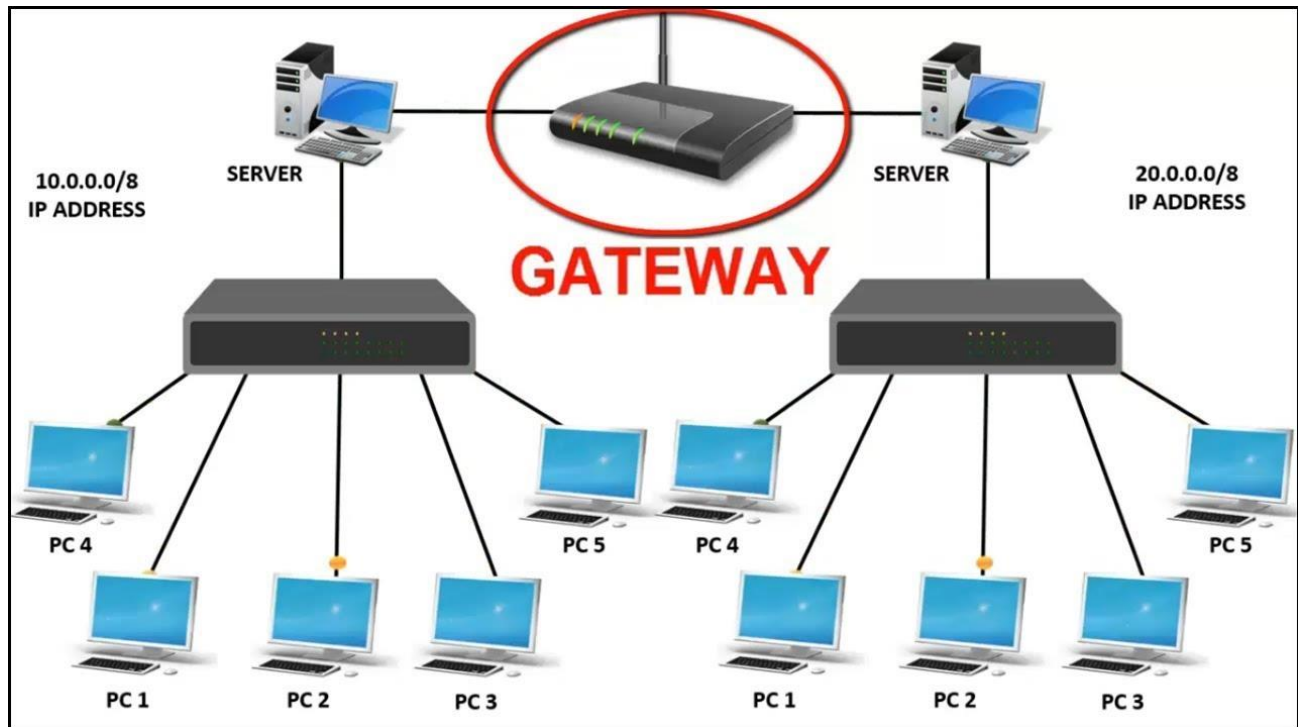
- Unidirectional Gateways
- Bidirectional Gateways

Unidirectional gateways

Unidirectional gateways allow alerts to flow in only one direction. Changes made in the source ObjectServer are replicated in the destination ObjectServer or application, but changes made in the destination ObjectServer or application are not replicated in the source ObjectServer. Unidirectional gateways can be considered as *archiving* tools.

Bidirectional gateways

Bidirectional gateways allow alerts to flow from the source ObjectServer to the target ObjectServer. In a bidirectional gateway configuration, changes made to the contents of a source ObjectServer are replicated in a destination ObjectServer or application, and the destination ObjectServer or application replicates its alerts in the source ObjectServer. Bidirectional gateways can be considered as *synchronization* tools.



Transmission Media

A communication channel that is used to carry the data from the transmitter to the receiver through the electromagnetic signals. The main function of transmission media is to carry the data in bits from sender to receiver in a network.

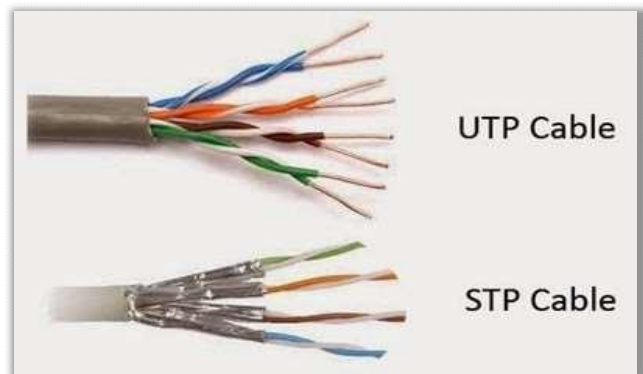
Twisted pair cable

Twisted-pair cable is a type of cabling that is used for telephone communications and most modern Ethernet networks. A pair of wires forms a circuit that can transmit data. The pairs are twisted to provide protection against crosstalk, the noise generated by adjacent pairs. When electrical current flows through a wire, it creates a small, circular magnetic field around the wire. When two wires in an electrical circuit are placed close together, their magnetic fields are the exact opposite of each other. Thus, the two magnetic fields cancel each other out. They also cancel out any outside magnetic fields. Twisting the wires can enhance this cancellation effect. Using cancellation together with twisting the wires, cable designers can effectively provide self-shielding for wire pairs within the network media.

Two basic types of twisted-pair cable exist: unshielded twisted pair (UTP) and shielded twisted pair (STP).

UTP cable is a medium that is composed of pairs of wires. UTP cable is used in a variety of networks. Each of the eight individual copper wires in UTP cable is covered by an insulating material. In addition, the wires in each pair are twisted around each other. UTP cable relies solely on the cancellation effect produced by the twisted wire pairs to limit signal degradation caused by electromagnetic interference (EMI) and radio frequency interference (RFI). To further reduce crosstalk between the pairs in UTP cable, the number of twists in the wire pairs varies.

STP cable combines the techniques of shielding, cancellation, and wire twisting. Each pair of wires is wrapped in a metallic foil. The four pairs of wires then are wrapped in an overall metallic braid or foil. As specified for use in Ethernet network installations, STP reduces electrical noise both within the cable (pair-to-pair coupling, or crosstalk) and from outside the cable (EMI and RFI). Although STP prevents



interference better than UTP, it is more expensive and difficult to install. In addition, the metallic shielding must be grounded at both ends. If it is improperly grounded, the shield acts like an antenna and picks up unwanted signals. Because of its cost and difficulty with termination, STP is rarely used in Ethernet networks.

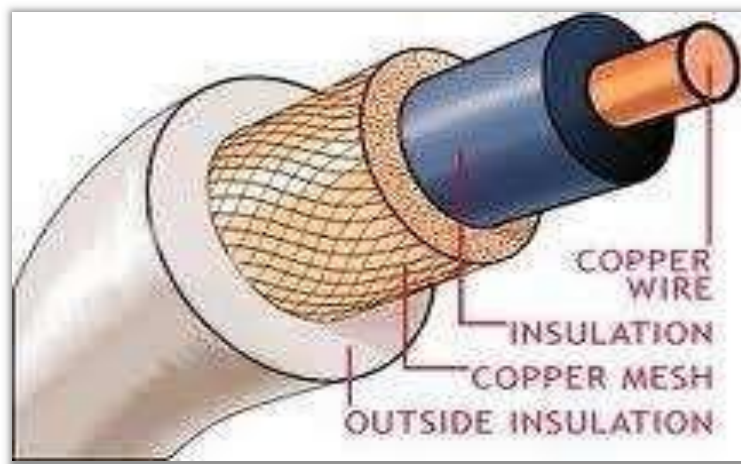
Coaxial cable

A coaxial cable is a type of shielded and insulated copper cable that is used in computer networks and to deliver cable TV services to end users. Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently.

Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.

Coaxial cables are categorized by their Radio Government ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and type of the inner insulator, the construction of the shield and the size and type of outer casing. Each cable defined by an RG rating is adapted for a specialized function.

As far as performance is concerned the attenuation is much higher in coaxial cable as compared to twisted pair cable and thus requires frequent use of repeaters.

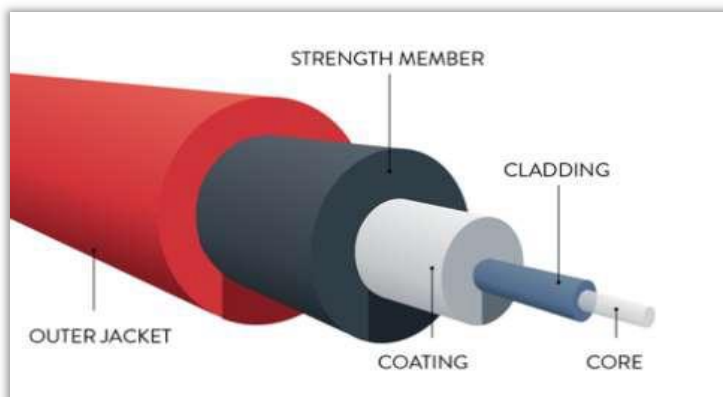
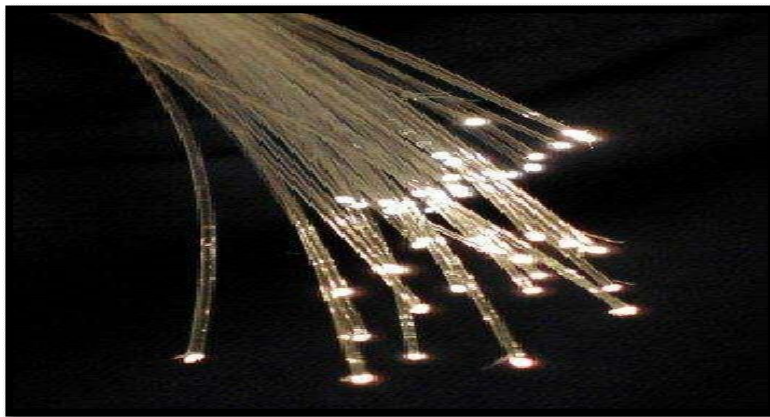


Optical Fiber

Optical fibers make use of light to send information through the optical medium by sending pulses of light. It consists of **thin glass fibers** or plastic or any dielectric medium which can carry light signals from one end to the other. Optical fiber refers to the medium and the technology which is related, or you can say that it is connected with the transmission of information in the form of light impulses and this transmission is done along with a glass or plastic wire or fiber. The wires of fiber optic cable can carry much more information than any other conventional copper wire. The typical optical fiber consists of a very **narrow strand of glass called the core**. Around the core is a **concentric layer of glass called the cladding**.

In such a system a pulse of light indicates bit 1 and the absence of light indicates bit 0. Light source can be an LED or a laser beam. **A detector generates an electrical pulse when the light falls on it.**

Optical fibers work on the principle that the core refracts the light and the cladding reflects the light. The core refracts the light and guides the light along its path. The cladding reflects any light back into the core and stops light from escaping through it – it bounds the medium! **Fast data transmission rate is an advantage to using fiber optics data transmission.**



Summary

The features of the connecting devices can be explained in brief as follows:

- **Hub**- Broadcasts data from one port to all other ports in the network.
- **Repeater**- Regenerates the input data which is subjected to attenuation.
- **Switch**- Intelligent device which sends data to particular port.
- **Bridge**-Same function as switch, connects multiple LANs but much more primitive and has only 2 ports.
- **Router**-Connects all computers from a LAN to internet using same IP.
- **Gateway**-Needed when 2 different network technologies are being used. Acts as translator.

CONCLUSION:

In this experiment various network components usage and working was studied and understood successfully.

Post Lab Questions

1. Compare Hub, switch, bridge, and gateway and specify the use in different cases.

HUB	SWITCH	BRIDGE	GATEWAY
A Hub, in the context of networking, is a hardware device that relays communication data. A hub sends data packets (frames) to all devices on a network, regardless of any MAC addresses contained in the data packet.	A Switch, in the context of networking is a high-speed device that receives incoming data packets and redirects them to their destination on a local area network (LAN).	A Bridge is a network device that connects multiple LANs (local area networks) together to form a larger LAN.	A Gateway is a passage to connect two networks together that may work upon different networking models/transmission protocols. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system.

Operates at layer 1 of the OSI model. (Physical Layer)	Operates at layer2 of the OSI model. (Data Link Layer)	Operates at layer2 of the OSI model. (Data Link Layer)	Operates at layer3 of the OSI model. (Network Layer)
Doesn't work with MAC address.	Work with MAC address.	Work with MAC address.	Works with MAC address.
Broadcasts incoming traffic on all ports.	Sends data packets to destination node only.	Routes traffic towards their addressed destinations only.	It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway.
Number of ports range from 4-12.	Number of ports range from 5-52.	2 port-device.	2 port-device.
It is a passive device.	It is an active device.	It is an active device.	It is an active device.
Used to connect multiple devices over the network.It is commonly used to connect segments of a LAN (Local Area Network).	A switch is a hardware device that filters and forwards network packets from one networking device (switch, router, computer, server, etc.) to another.	Bridges connects two or more different LANs that has a similar protocol and provides communication between the devices (nodes) in them.	The gateway converts information, data or other communications from one protocol or format to another.

2. Which of the following device is used to connect two systems, especially if the systems use different protocols?

- A.hub
- B.bridge
- C.gateway**
- D.repeater
- E.None of the above

Ans. Gateway

3. Frames from one LAN can be transmitted to another LAN via the device

- A. Router
- B. Bridge**
- C. Repeater
- D. Modem

Ans. Bridge