K. J. Somaiya College of Engineering, Mumbai-77

(Autonomous College Affiliated to University of Mumbai)

Batch: B1 **Roll No.: 1711072**

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 Network topology and Connecting devices (Hub,router,Gateway,Switch etc)

AIM: To study different Network topologies and connecting devices used in day to day networks.

Expected Outcome of Experiment:
CO: Describe the network layer concepts and implement primitives related to addressing.

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 LAN

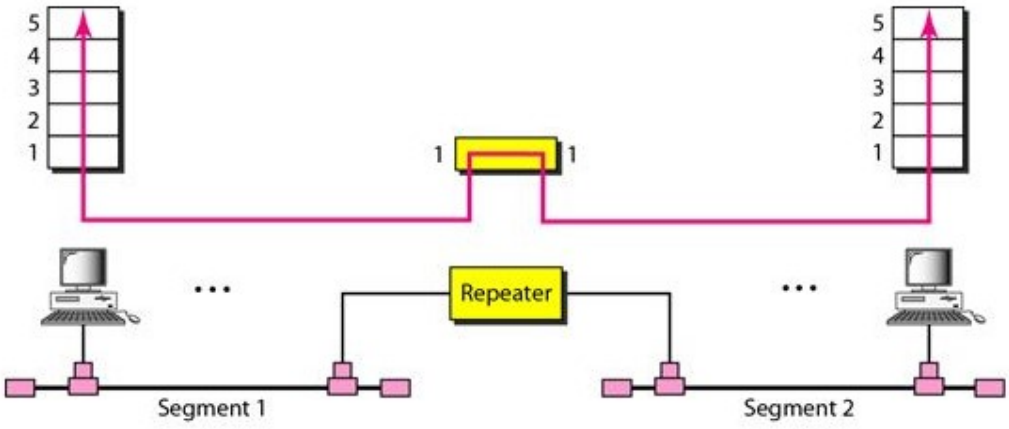
1. Define various basic attributes used in designing of a network.
2. Define LAN topology
3. Theoretical design of LAN using various topologies.

Study of Connecting Devices

Repeater

- A repeater is a device that operates only in the physical layer. Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data. A repeater receives a signal and, before it becomes too weak or corrupted, regenerates the original bit pattern. The repeater then sends the refreshed signal. Repeater amplifies the signal, which has got attenuated during the course of transmission because of the

physical conditions imposed by the transmission media. It also restores the signal to its original shape.A repeater can extend the physical length of a LAN, as shown in the following figure.



Characteristics:

- The specific characteristic of repeater is that whatever it receives it transmits to the other LAN segment. This does not understand the frame format and also physical addresses.
- It is a 2 port device.
- In other words, it is a transparent device. Therefore, multiple LANs connected by repeaters may be considered as a single LAN.

Advantages:

- The primary advantage of using a wireless repeater is that it can improve wireless signal strength without having to move a computer or router.
- The further a computer is from the wireless router it connects to, the weaker its wireless signal will tend to be. Weak signals can result in slow or intermittent connectivity.

Disadvantages:

- The main disadvantage associated with repeaters is their transparent nature because the signal received at one segment is truly transmitted to the other segment.
- Repeater does not understand the language of frame and therefore, cannot distinguish between noise and signal.
- When a collision occurs on one segment, the same along with noise produced by collision is reproduced on the other segment by repeater.

Hub

- A hub, also called a network hub, is a common connection point for devices in a network. Hubs are devices commonly used to connect segments of a LAN. The hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all

segments of the LAN can see all packets. The purpose of a hub is to join multiple computers or other network devices together to form a single network segment. On this network segment, all devices can communicate directly with each other.

Characteristics:

- The number of ports an Ethernet hub supports also varies. Four- and five-port Ethernet hubs are most common in home networks, but eight- and 16-port hubs can be found in some home and small office environments.
- **Types of Hub**
  - **Active Hub :-** These are the hubs which have their own power supply and can clean , boost and relay the signal along the network. It serves both as a repeater as well as wiring center. These are used to extend maximum distance between nodes.
  - **Passive Hub :-** These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend distance between nodes.

Advantages:

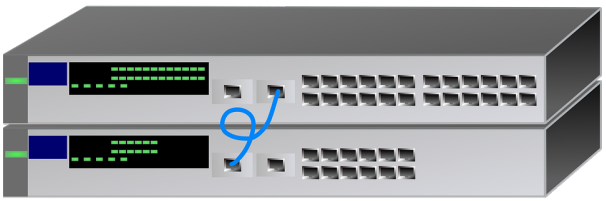
- They are more intelligent than repeaters.
- It can extend total distance of the network.
- It does not affect performance of the network seriously.
- It is cheaper.
- It can connect different media types.

Disadvantages:

- They do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.
- Hubs cannot filter data, so data packets are sent to all connected devices.In other words, collision domain of all hosts connected through Hub remains one.
- It does not operate in full duplex mode.
- It does not have mechanism to reduce the network traffic.
- It can not filter information i.e. it passes packets to all the connected segments.
- It does not have mechanisms such as collision detection and retransmission of packets.

Bridge

- A **network bridge** is a device that divides a network into segments. Each segment represent 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.
- A bridge works at the Data link layer (Layer 2) of the OSI model. It inspects incoming traffic and decide whether to forward it or filter it. Each incoming Ethernet frame is inspected for destination MAC address. If the bridge determines that the destination host is on another segment of the network, it forwards the frame to that segment.



Characteristics:

- **Network Expansion** – Increases the number of attached workstations and network segments
- **Frame Buffering** – Enables to interconnect different segments which use different MAC protocols as frames are buffered
- **Transparency** – Works at the MAC layer and hence are transparent to higher level protocols
- **Reliability** – Increases network reliability and makes the network easier to maintain by subdividing LAN into smaller segments which reduces congestion
- **Speed** – Is slow as compared to a repeater as it introduces delays due to buffering of frames.
- **Overload** – Overloads during periods of high traffic
- **Expensive** – More expensive than repeaters

- **No filtering** – Provides no filtering of the **broadcast** frames

Advantages:

- Bridges connect similar network types with different cabling
- Bridges increase the number of attached workstations and network segments

Disadvantages:

- Bridges is costly as compared to repeaters
- Bridges may affect performance as it buffers data frames

Switch

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

Characteristics:

- Switches are found in both unmanaged and managed forms.
- Unmanaged switches have no options and simply work out of box.
- Managed switches have advanced options that can be configured. Managed switches also contain software called firmware that should be updated as released by the switch manufacturer.
- Switches connect to other network devices via network cables only and thus do not require drivers to operate in Windows or other operating systems.

Advantages:

- 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:

- 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.

Router

- A **router** is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork until it reaches its destination node
- A router is connected to two or more data lines from different networks When a data packet comes in on one of the lines, the router reads the network address information in the packet to determine the ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey.

Characteristics:

1. Routers are multiport devices with high - speed backbones
2. Routers also support filtering and encapsulation like bridges
3. Like bridges routers are also self-learning, as they can communicate their existence. to other devices and can learn of the existence of new routers, nodes and LAN segments

4. As explained earlier, they route traffic by considering the network as a whole. It shows that they use a high level of intelligence to accomplish this task. This characteristic makes them superior than hubs and bridges because they simply view the network on a link-by-link basis
5. The packet handled by router may include destination address, packet priority level, least-cost route, minimum route delay, minimum route distance, and route congestion level
6. Routers constantly monitor the condition of the network, as a whole to dynamically adapt to changes in the condition of the network
7. They typically provide some level of redundancy so that they are less susceptible to catastrophic failure.

Advantages:

- It provides connection between different network architectures such as ethernet & token ring etc.
- It can choose best path across the internetwork using dynamic routing algorithms.
- It can reduce network traffic by creating collision domains and also by creating broadcast domains.
- It provides sophisticated routing, flow control and traffic isolation.
- They are configurable which allows network manager to make policy based on routing decisions.

Disadvantages:

- They operate based on routable network protocols.
- They are expensive compare to other network devices.
- Dynamic router communications can cause additional network overhead. This results into less bandwidth for user data.
- They are slower as they need to analyze data from layer-1 through layer-3.
- They require considerable amount of initial configurations.
- They are protocol dependent devices which must understand the protocol they are forwarding.

Gateway

- A gateway is a node (router) in a computer network, a key *stopping point* for data on its way to or from other networks. Thanks to gateways, we are able to communicate and send data back and forth. The Internet wouldn't be any use to us without gateways (as well as a lot of other hardware and software).

- In a workplace, the gateway is the computer that routes traffic from a workstation to the outside network that is serving up the Web pages. For basic Internet connections at home, the gateway is the Internet Service Provider that gives you access to the entire Internet.

Characteristics:

- Gateway servers are often stackable or rack-mounted for use in computer rooms. These devices may include LED indicators for monitoring purposes.
- Other features for gateways include integrated firewalls for security and support for tunneling, a technique where packets are transmitted across a public routed network in a private "tunnel" that simulates a point-to-point connection and allows network protocols to traverse incompatible infrastructures.

Advantages:

Direct connections between internal and external hosts are disallowed.

- User-level authentication is supported.

- The application commands are analyzed inside the payload portion of the data packets.

Disadvantages:

Slower than packet filters

- Needs the internal client to know about them.

- Every possible type of connection can not be supported

NIC

- To connect to a network, a computer uses a network interface card (NIC). A NIC controls the wired and wireless connections of a computer to exchange information with other computers and the Internet.

- NICs were commonly included in desktop computers in the 1990s and early 2000s. In the 1980s and early 1990s, many computers did not include networking capabilities, so a NIC could be added as an expansion card. Most NICs were installed in a PCI slot on the motherboard. Early NICs included a BNC connector for coax network connections, though

Ethernet ports soon became the standard. Therefore most NICs include one or more Ethernet ports.

- As wireless networking became more popular, wireless NICs also grew in popularity. Instead of an Ethernet port, wireless NICs are designed for Wi-Fi connections and often have an antenna to provide better wireless reception for the computer. Older wireless cards have PCI connections while most modern wireless NICs connect to a PCI Express slot.

Characteristics:

A network card functions as a middleman between your computer and the data network. For example, when you log in to a website, the PC passes the site information to the network card, which converts the address into electrical impulses.

Network cables carry these impulses to a Web server somewhere on the Internet, which responds by sending a Web page back to you, once again in the form of electronic signals. The card receives these signals and turns them into data that your PC displays.

Advantages:

- Newer NICs can reach speed upto 2000 Mbps.
- NICs are very cheap to buy and easy to install.
- Stable connection between device and cable.

Disadvantages:

- Proper configuration is needed in order for device to work properly.
- NICs can be unsafe and data is not secured.

Connecting Cables

While connecting different networks, we come across different connecting cables, which are as follows:

RJ45/ RJ 11 Connectors: The RJ45 (Registered Jack 45) cable or the Cat 5 cable, is used to connect the two different LAN's together. This is normally confused with the RJ11 cable, which is used in the interconnections in the telephone network.

Twisted pair cable

In balanced pair operation, the two wires carry equal and opposite signals and the destination detects the difference between the two. This is known as differential mode transmission. Noise sources introduce signals into the wires by coupling of electric or magnetic fields and tend to couple to both wires equally.

The noise thus produces a common-mode signal which is canceled at the receiver when the difference signal is taken.

This method starts to fail when the noise source is close to the signal wires; the closer wire will couple with the noise more strongly and the common-mode rejection of the receiver will fail to eliminate it. This problem is especially apparent in telecommunication cables where pairs in the same cable lie next to each other for many miles. One pair can induce crosstalk in another and it is additive along the length of the cable. Twisting the pairs counters this effect as on each half twist the wire nearest to the noise-source is exchanged.

Providing the interfering source remains uniform, or nearly so, over the distance of a single twist, the induced noise will remain common-mode. Differential signaling also reduces electromagnetic radiation from the cable, along with the associated attenuation allowing for greater distance between exchanges.

The twist rate (also called pitch of the twist, usually defined in twists per meter) makes up part of the specification for a given type of cable. Where nearby pairs have equal twist rates, the same conductors of the different pairs may repeatedly lie next to each other, partially undoing the benefits of differential mode. For this reason it is commonly specified that, at least for cables containing small numbers of pairs, the twist rates must differ.[

UTP cables are found in many Ethernet networks and telephone systems. For indoor telephone applications, UTP is often grouped into sets of 25 pairs according to a standard 25-pair color code originally developed by AT&T Corporation. A typical subset of these colors (white/blue, blue/white, white/orange, orange/white) shows up in most UTP cables. The cables are typically made with copper wires measured at 22 or 24 American Wire Gauge (AWG),[3] with the colored insulation typically made from an insulator such as polyurethane and the total package covered in a polyurethane jacket.

For urban outdoor telephone cables containing hundreds or thousands of pairs, the cable is divided into smaller but identical bundles. Each bundle consists of twisted pairs that have different twist rates. The bundles are in turn twisted together to make up the cable. Pairs having the same twist rate within the cable can still experience some degree of crosstalk. Wire pairs are selected carefully to minimize crosstalk within a large cable.

Unshielded twisted pair cable with different twist rates

UTP cable is also the most common cable used in computer networking. Modern Ethernet, the most common data networking standard, can use UTP cables. Twisted pair cabling is often used in data networks for short and medium length connections because of its relatively lower costs compared to optical fiber and coaxial cable.

UTP is also finding increasing use in video applications, primarily in security cameras. Many cameras include a UTP output with screw terminals; UTP cable bandwidth has improved to match the baseband of television signals. As UTP is a balanced transmission line, a balun is needed to connect to unbalanced equipment, for example any using BNC connectors and designed for coaxial cable.

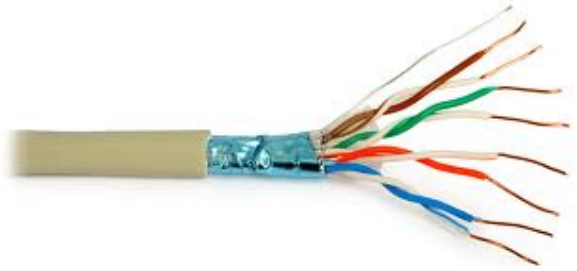


Fig 7.Twisted Pair Cable

Coaxial cable

Coaxial cable is the kind of copper cable used by cable TV companies between the community antenna and user homes and businesses. Coaxial cable is sometimes used by telephone companies from their central office to the telephone poles near users. It is also widely installed for use in business and corporation Ethernet and other types of local area network.

Coaxial cable is called "coaxial" because it includes one physicalchannel that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both running along the same axis. The outer channel serves as a ground. Many of these cables or pairs of coaxial tubes can be placed in a single outer sheathing and, with repeaters, can carry information for a great distance.

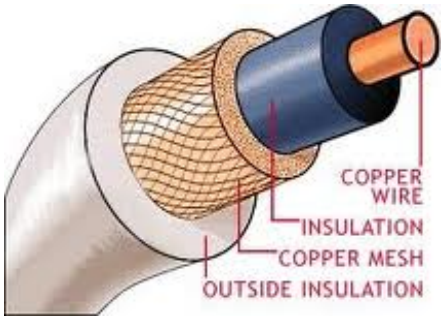


Fig 8.Coaxial Cable

Optical Fiber

Fiber-optic communication is a method of transmitting information from one place to another by sending pulses of light through an optical fiber. The light forms an electromagnetic carrier wave that is modulated to carry information. First developed in the 1970s, fiber-optic communication systems have revolutionized the telecommunications industry and have played a major role in the advent of the Information Age. Because of its advantages over electrical transmission, optical fibers have largely replaced copper wire communications in core networks in the developed world.

The process of communicating using fiber-optics involves the following basic steps: Creating the optical signal involving the use of a transmitter, relaying the signal along the fiber, ensuring that the signal does not become too distorted or weak, receiving the optical signal, and converting it into an electrical signal.

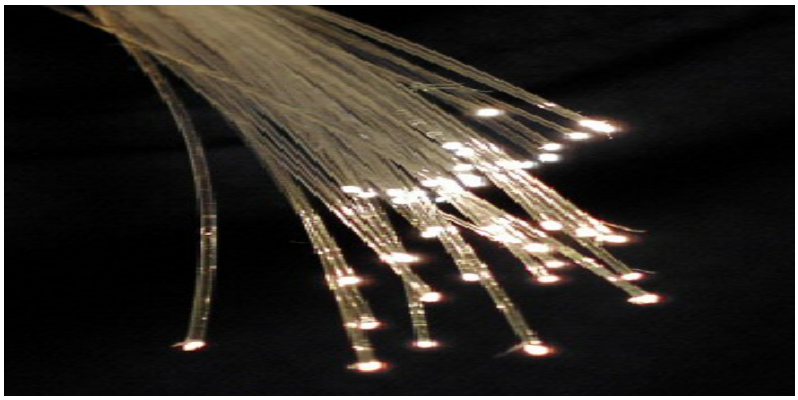


Fig 9.Fiber Optics Cable

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 but much more primitive and has lesser ports.
- Router-Connects all computers from a LAN to internet using same IP.
- IEEE 802.11- WiFi standard- 802.11 b has speed of 11 Mbps, 802.11 g has a speed of 54 Mbps and 802.11 N uses multiple wireless signals and antennas and has speeds of over 100Mbps.
- Gateway-Needed when 2 different network technologies are being used. Acts as translator.

CONCLUSION: Various network components were studied successfully.

Post Lab Questions

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

Ans.

1. Hubs:

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.

Common types of hubs used in networking are network hubs, passive hubs, intelligent and switching hubs.

- Network Hubs: These are common connection points for network devices, which connect segments of a LAN (local area network) and may contain multiple ports – an interface for connecting network devices such as printers, storage devices, workstations and servers. A data packet arriving at one hub's port may be copied to other ports allowing all segments of the network to have access to the data packet.
- Passive Hubs: These only serve as paths or conduits for data passing from one device, or network segment, to another.
- Intelligent Hubs: Also known as manageable hubs, these hubs allow system administrators to monitor data passing through and to configure each port, meaning to determine which devices or network segments are plugged into the port. Some ports may even be left open with no connection.
- Switching Hubs: These hubs actually read the attributes of each unit of data. The data is then forwarded to the correct or intended

port.

2. Switches:

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 LAN switch operates at the data link layer (Layer 2) or the network layer of the OSI Model and, as such it can support all types of packet protocols. Essentially, switches are the traffic cops of a simple local area network.

A switch in an Ethernet-based LAN reads incoming TCP/IP data packets/frames containing destination information as they pass into one or more input ports. The destination information in the packets is used to determine which output ports will be used to send the data on to its intended destination. Switches are similar to hubs, only smarter. A hub simply connects all the nodes on the network -- communication is essentially in a haphazard manner with any device trying to communicate at any time, resulting in many collisions. A switch, on the other hand, creates an electronic tunnel between source and destination ports for a split second that no other traffic can enter. This results in communication without collisions.

Switches are similar to routers as well, but a router has the additional ability to forward packets between different networks, whereas a switch is limited to node-to-node communication on the same network.

3. Bridge:

A bridge is a type of computer network device that provides interconnection with other bridge networks that use the same protocol.

Bridge devices work at the data link layer of the Open System Interconnect (OSI) model, connecting two different networks together and providing communication between them. Bridges are similar to repeaters and hubs in that they broadcast data to every node. However, bridges maintain the media access control (MAC) address table as soon as they discover new segments, so subsequent transmissions are sent to only to the desired recipient.

Bridges are also known as Layer 2 switches.

A network bridge device is primarily used in local area networks because they can potentially flood and clog a large network thanks to their ability to broadcast data to all the nodes if they don't know the destination node's MAC address.

A bridge uses a database to ascertain where to pass, transmit or discard the data frame.

If the frame received by the bridge is meant for a segment that resides on the same host network, it will pass the frame to that node and the receiving bridge will then discard it.

If the bridge receives a frame whose node MAC address is of the connected network, it will forward the frame toward it.

4. Gateway:

A gateway is a data communication device that provides a remote network with connectivity to a host network.

A gateway device provides communication to a remote network or an autonomous system that is out of bounds for the host network nodes. Gateways serve as the entry and exit point of a network; all data routed inward or outward must first pass through and communicate with the gateway in order to use routing paths. Generally, a router is configured to work as a gateway device in computer networks.

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. C. Gateway

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

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

Ans. B. Bridge