Networking and Local Area Networks

Network Fundamentals

A **network** is a communication system with two or more stations that can communicate with one another. When it is desired to have each computer communicate with two or more additional computers, the interconnections can become complex. As Fig.(a) indicate, if four computers are to be interconnected, there must be three links to each PC. The number of links L required between N PCs (nodes) is determined by using the formula

$$L = \frac{N(N-1)}{2}$$

Assume,there are six PCs. The number of links is

$$L = \frac{6(6-1)}{2} = 15$$

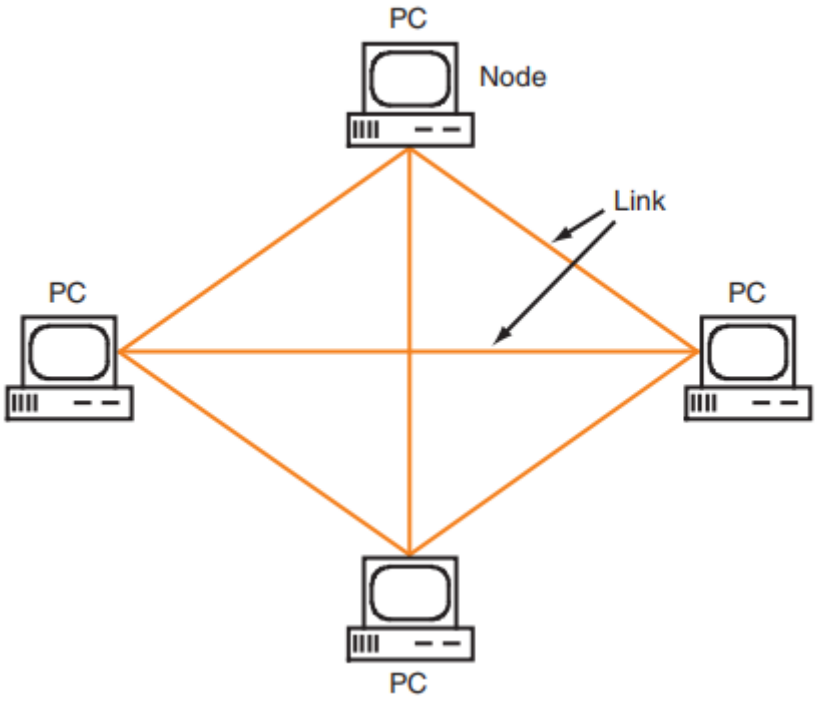


Fig (a): Network of Four PC's

The number of links or cables increases in proportion to the number of nodes involved. The type of arrangement shown in Fig.(a) is obviously expensive and impractical. Some special type of network wiring must be used, a combination of hardware and software that permits multiple

computers to be connected inexpensively and simply with the minimum number of links necessary for communication.

Types Of Network:

Each computer or user in a network is referred to as a node. The interconnection between the nodes is referred to as the communication link. There are five basic types of electronic networks in common use: wide-area networks (WANs), metropolitan-area networks (MANs), local-area networks (LANs), Storage Area Network(SAN) and personal-area networks (PANs).

Local-Area Networks (LANs):A LAN is the smallest type of network in general use. It consists primarily of personal computers interconnected within an office or building which is shown in fig(b) below.

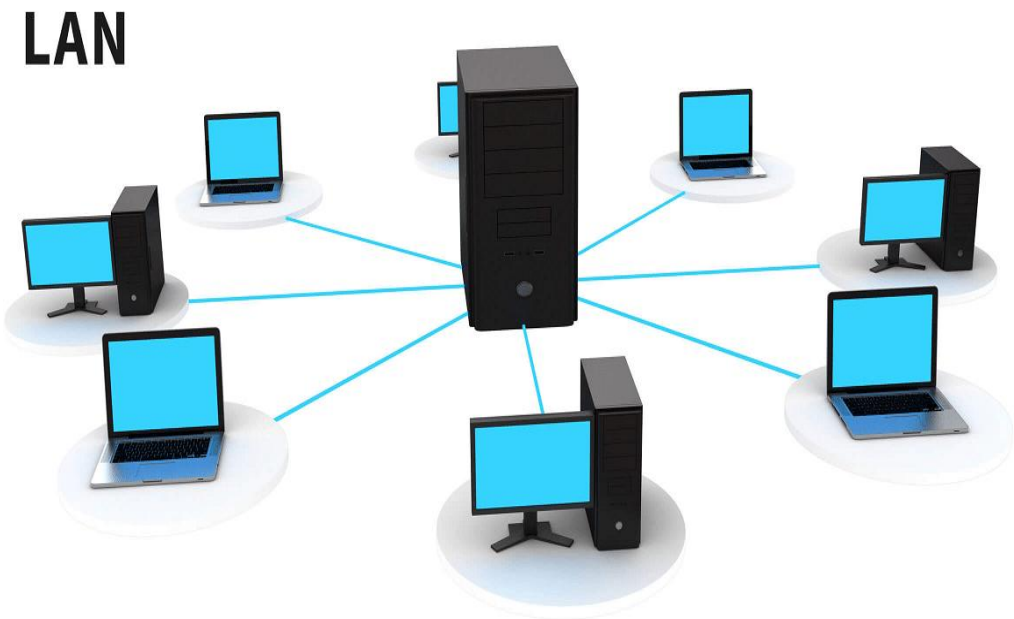


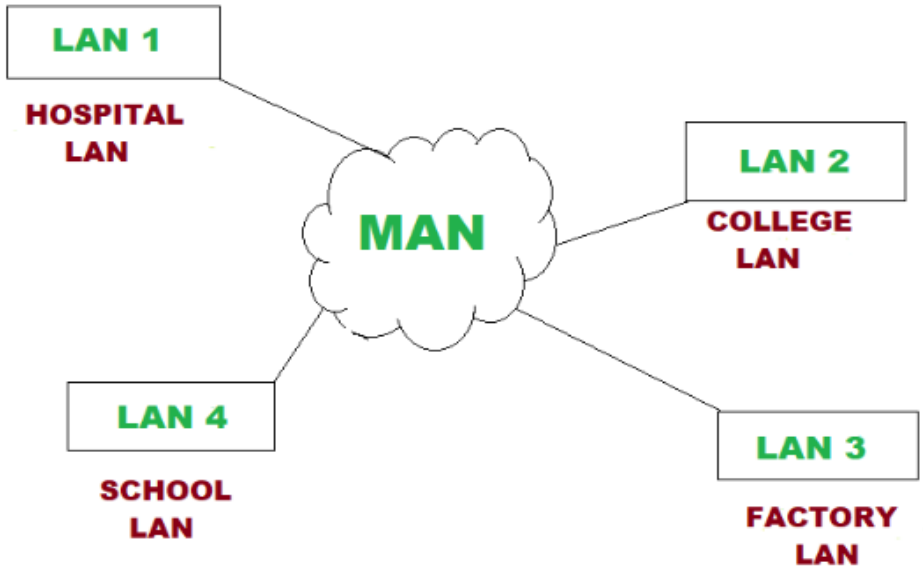
Fig (b): Local Area Network

LANs can have as few as 3 to 5 users, although most systems connect 10 to several thousand users. Small LANs can be used by a company to interconnect several offices in the same building; in such cases, wiring can be run between different floors of the building to make the connection. Larger LANs can interconnect several buildings within a complex, e.g., large companies with multiple buildings, military installations, and college campuses.

Some LANs consist of multiple PCs that are linked both to each other and to a minicomputer or mainframe. This allows each user on the LAN, to have access to the big computer as well as continue to operate independently. Home networks of two or more PCs are also LANs, and today most home LANs are fully wireless or incorporate wireless segments.

Metropolitan Area Network(MAN);

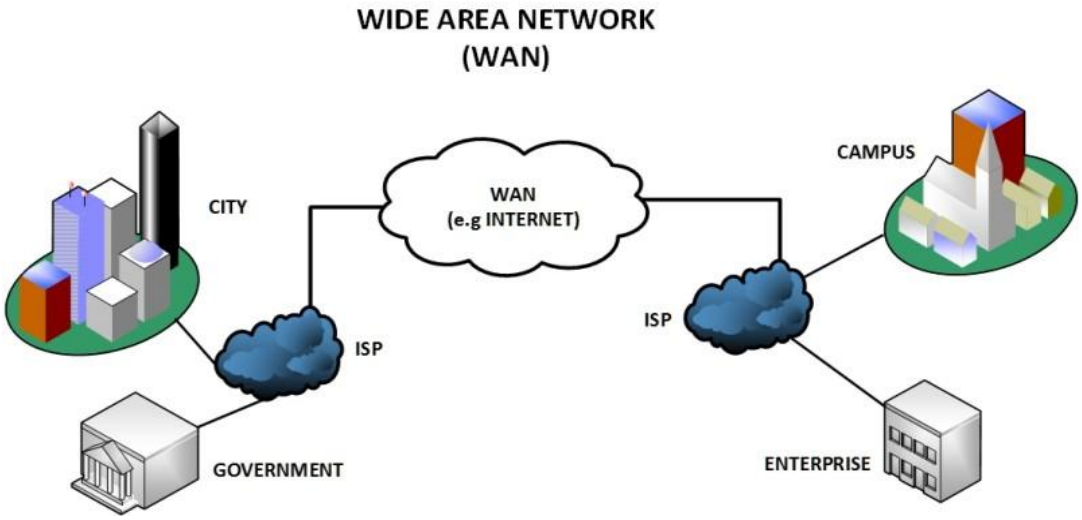
It is a computer network that connects number of LANs to form larger network, so that the computer resources can be shared. This type of network covers larger area than a LAN but smaller than the area covered by a WAN which is designed to extend over the entire city. MAN is specially designed to provide high-speed connectivity to the users in which the speed ranges in terms of Mbps. The architecture of MAN is quite complicated hence,it is hard to design and maintain.



Fig(c): Metropolitan Area Network

Wide Area Networks:

WAN stands for Wide Area Network, which is a network that covers a large geographical area, such as a country, a continent, or even the entire world. WANs are typically used to connect LANs that are separated by large distances, and enable communication and data transfer between different locations that may be hundreds or even thousands of kilometers apart. MANs are designed to cover a relatively small geographical area, while WANs are designed to cover much larger areas.



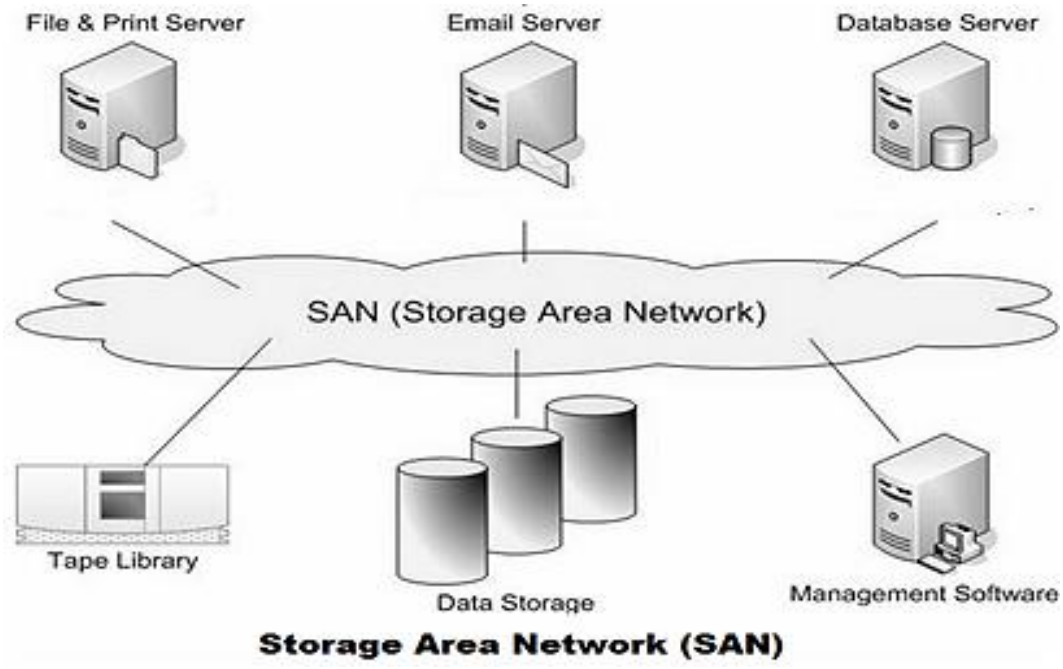
Fig(d): Wide Area Network

Personal-Area Networks (PANs): A PAN is a short-range wireless network that is set up automatically between two or more devices such as laptop computers, peripheral devices, or cell phones. The distance between the devices is very short, no more than about 10 m and usually much less. PANs are referred to as adhoc networks that are set up for a specific single purpose, such as the transfer of data between the devices as required by some application. For example, a laptop computer may link up with a printer, or a smartphone may need to download data from a PC. Most PANs just involve two nodes, but some have been set up to handle up to eight nodes and sometimes more.

Fig(d): Personal Area Network

Storage Area Networks:

A SAN (storage area network) is a dedicated, independent high-speed network that interconnects and delivers shared pools of storage devices to multiple servers. Each server can access shared storage as if it were a drive directly attached to the server.The storage devices used in SAN Networks are Disk arrays, Tape libraries, Optical Storage devices like Archival Disc, M Disc Libraries,Optical Jukebox etc. SANs are typically composed of hosts, switches, storage elements, and storage devices that are interconnected using a variety of technologies, topologies, and protocols. SANs may also span multiple sites. A SAN is typically assembled with cabling, host bus adapters, and SAN switches attached to storage arrays and servers. Each switch and storage system on the SAN must be interconnected.



Fig(e): Storage Area Network

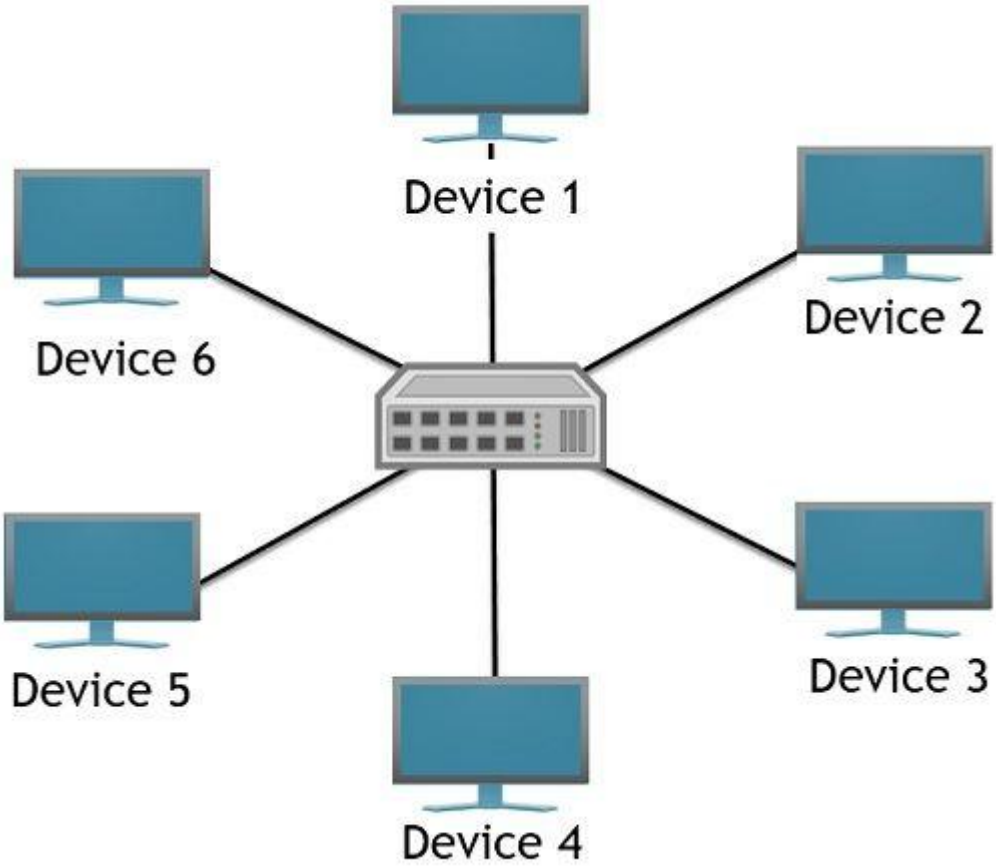
Network Topologies:

The topology of a network describes the basic communication paths between, and methods used to connect, the nodes on a network. The three most common topologies used are star, ring, and bus. These topologies apply to the LAN, MAN, and WAN.

Star Topology:

Star topology, often known as a star network, is one of the most typical network configurations. In this design, each node is linked to a hub, switch, or computer that serves as the hub for the whole network. The main network device serves as a server, and the other network nodes function as clients.
In star topology network configuration, a star-shaped icon represents every device connected to a central network device.Numerous star topology instances are found in real-world settings, including airports, hospitals, banks, and educational institutions.To link the clients to the central hub, co axial cables or twisted pair cables are utilized. In a star topology, every linked device is totally dependent on the central device; if the central device has any issues, communication throughout the whole computer network breaks down.

A basic star connection shown in fig(f) below.



Fig(f): A star LAN configuration.

From the above figure we observe that each device of the network is individually connected to the hub through separate cabling. Due to this connection whenever, a fault appears in any of the devices of the network, then its detection and solution becomes quite easy. But in this case, when the fault appears at the central hub of the network then it breaks down the

whole network completely, as all the devices are directly connected to this particular hub.

In this form of network structure, nodes can only connect with one another through a central device that is part of the network; direct communication between nodes is not possible. Both receiving and delivering messages from the sender are handled by this central device, which might be a Passive Hub, Active Hub, or Switch. In each situation, the method for operating the central device is different. As a result, Star Topology is divided into the following three groups based on its mode of operation:
1) Passive Star Topology
2) Active Star Topology
3) Star topology using Switch

In **passive star topology**, a passive hub is used as central controlling device.The hub will serve as the central device that accepts data messages from senders and distributes them to all associated nodes. All connected nodes accept destination address, checks after receiving the data message. If the destination address and the address of a node match, the matching node stores the message. If the destination address and the address of a node do not match, the node discards the data message.

In **active star topology**, an active hub is used as central controlling device.They have a power supply for regenerating, and amplifying the signals. When a port sends weak signaled data, the hub regenerates the signal and strengthens it, then send it further to all other ports. Active hubs are expensive as compared to passive hubs.

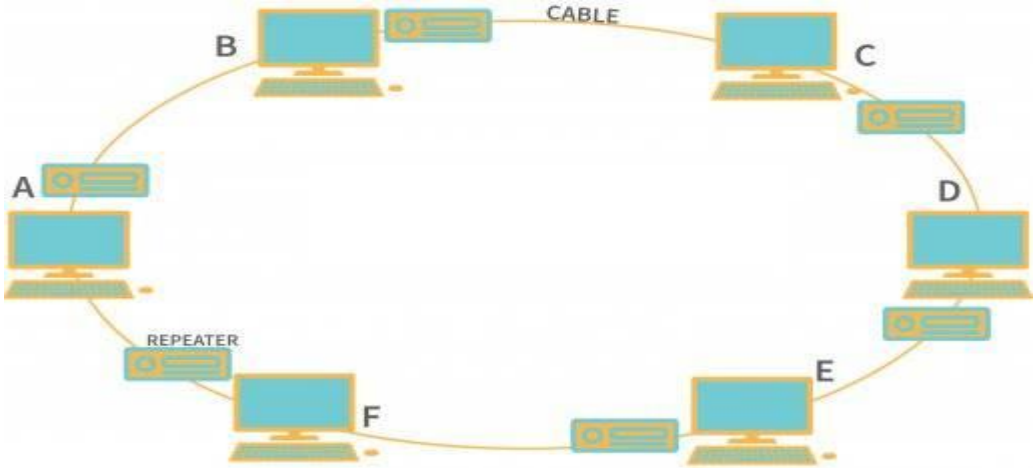
In **Star topology using switch**, hub is replaced with a switch as the central device in a star design. Switcher Star Network Topology is another name for the star network created with Switch. The central component in this kind of network is an intelligent device, Switch.
A switch is an intelligent device in terms of destination recognition, routing, and regeneration. A Switch receives the data message from the sender in a manner similar to what a Hub does. But instead of broadcasting the data message as soon as it is received, it first verifies the target address before sending the message to that specific location.
After reading the data message's destination address and carrying out a few further tasks, the switch sends the data message to the specified recipient.

Advantages of Star topology:

1) Star topology is relatively easy to install and configure. The central hub or switch acts as a central point of communication, making it easy to connect and disconnect devices. This makes it easy to add or remove devices from the network without affecting the rest of the network.
2) Star topology is also easy to troubleshoot. If a device on the network is not working properly, it is easy to isolate the problem by disconnecting the device from the central hub and testing it. This makes it easy to identify and fix problems on the network.
3) Star topology is highly scalable. If the network needs to be expanded, it is easy to add more devices by connecting them to the central hub. This makes it easy to expand the network as the number of devices on the network increases.

Disadvantages of Star topology:
1) If the central hub or switch fails, the entire network will be down. This can be a major problem for networks that require high availability.
2) Within the star topology implementation of a router or switch, it's very costly, especially when using a router or a switch as the central network device.
3) Within the star topology, more potential damage exposure is created by the cables a wires used in it.It needs to go behind under floors, walls, and through other obstacles to reach the intended peripherals or workstations.

Ring Topology:
Ring topology is a closed-loop network where all devices, such as computers and printers, are connected in a circular (ring) structure.
In this topology, each device is connected to two other devices, one on either side, forming a single continuous pathway for data transmission which is shown in fig (g) below.



Fig(g):A ring LAN configuration

In a ring topology network, data moves sequentially from one node to the next in a unidirectional manner. This topology commonly uses a token-passing control mechanism to ensure orderly data transmission and prevent collisions. In this mechanism, only the node holding the token has the right to transmit data.

When the node want to send data in this topology, it waits for the token to arrive at its position. Once the token is arrived,the node attach the data and send it to the next device. The device that receives the data becomes the new token holder, and the process repeats itself.

Each packet transmitted across the ring contains a destination address and the data. Each node checks the destination address as the packet circulates the ring. If the address matches the node's address, the node processes the packet. Otherwise, it passes the packet to the next node in the sequence.

If Node A wishes to send data to Node E, then the data travels from Node A to Node B to Node C to Node D to Node E

Ring topology can also be bi-directional, but implementing this requires additional hardware investment. However, the benefit of a bi-directional ring is that it can prevent data loss if a device in the ring fails. Whether the ring is unidirectional or bi-directional, the basic operation remains the same sequential data transmission.

Advantages of Ring topology:

1) Easy to manage due to its orderly structure.

2) Operates without a central server, simplifying node connectivity.

3) Guarantees equal access to resources for all devices.

4) The unidirectional flow of data minimizes the risk of packet collisions.

5) Token passing improves performance under heavy traffic, outperforming other topologies.

Disadavantages of Ring topology:

1) Troubleshooting the ring network is complex.

2) Adding or removing nodes can disrupt network activity.

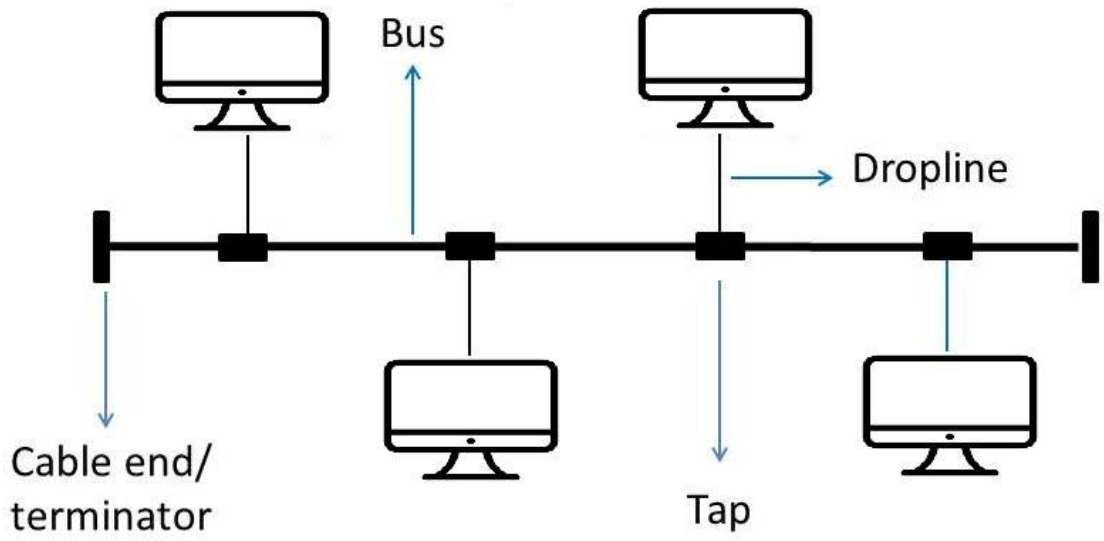
3) Performance lags behind bus topology in terms of speed.

4) If one node or workstation fails, the entire network is affected.

5) Due to the unidirectional ring, a token must pass through every node, impacting speed and efficiency.

Bus Topology:

Bus topology, alternatively known as line topology, is a type of network topology where all devices on a network are connected to a single cable, called a bus or backbone. This cable serves as a shared communication line, allowing all devices (computers, printers, etc.) to receive the same signal simultaneously.Fig.(h) shows the bus configuration.



Fig(h):A bus LAN configuration.

Bus topology is bi-directional, i.e., data is transmitted in both directions on the backbone cable to ensure it reaches the recipient, regardless of its position on the bus.A twisted-pair cable or a coaxial cable is utilized as a

bus (backbone cable) to link network devices, computers or nodes together.

Bus topology has a single central cable that serves as the shared communication medium for all network devices. Each device is connected to this cable via a tap or a connector. This structure allows all devices to communicate with each other.

Terminators are used at each end of the cable to absorb signals once they reach the end of the cable. This prevents these signals' reflection down the line, which could cause interference.

When a device wants to send data to another device, it broadcasts the data onto the cable. However, only the device with the matching destination address will process the data. Other devices will ignore the data.

Before sending data, a device checks the bus to see if it is free. If the bus is free, the data is transmitted,but if the bus is not free, the device will wait for a random amount of time before attempting to transmit the data again. This helps avoid collisions, which occur when two devices try to transmit data simultaneously.

But if a collision does occur, the devices involved will stop transmitting and again wait for a random amount of time before attempting to transmit again. This process is repeated until the data is successfully transmitted.

Bus topology is primarily used in small-to-medium-sized local area networks, such as small offices or home setups. It's also suitable for temporary or ad-hoc networks that require quick setup and tear down.

Advantages of Bus Topology:

1) A single cable connects all nodes in a bus topology.

2) This topology is easy to install and requires minimal configuration.

3) Bus topology is cheaper because it uses a common cable for data transmission.

4) This topology provides high-speed data transfer as there are no intermediary devices between the nodes.

5) Since all the nodes are connected to a single wire, the network remains operational even if one node fails.

Disadvantages of Bus Topology:

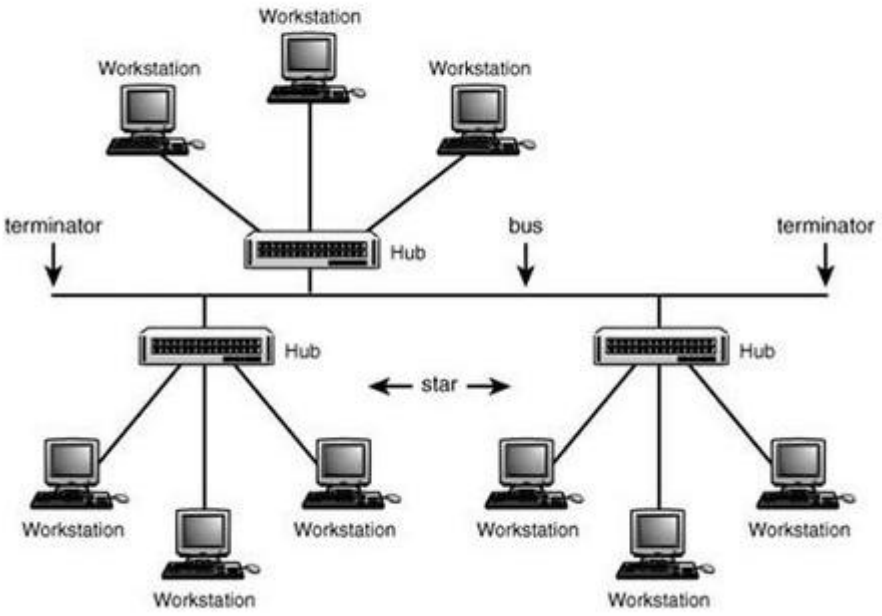
1) The entire network will fail if the central cable (bus or backbone) gets damaged or faulty.

2) The network's performance decreases as the number of devices connected increases, as all devices share the same bandwidth.

3) Due to cable length limitations, bus topology is unsuitable for large networks.

Tree Topology:

It is a type of network topology in which nodes are connected in such a way that it looks like a tree which is shown in fig(i) below.



Fig(i): A LAN Tree topology

Tree topology is a combination of bus topology and star topology. In a bus topology ,nodes i.e, hubs are connected to the central bus. While in a star topology nodes are connected to hubs. Tree topology is an expansion of star and bus topology. It is also known as an extended star topology.

In tree topology hubs are connected to the central bus. There is a point to point connection between every node meaning every node is

connected to a hub. To expand a tree network you just need to attach another hub and cables

Tree topology is flexible and reliable. Tree network can be connected to large network also. This network is connected in such a way that it reduces network traffic also. You can connect as many servers to the network as you want. The information is shared among all the computers in the network. If any computer wants to send a message then it will broadcast the message through hub and the hub will redirect the message to the destination computer.

Advantages of Tree topology:

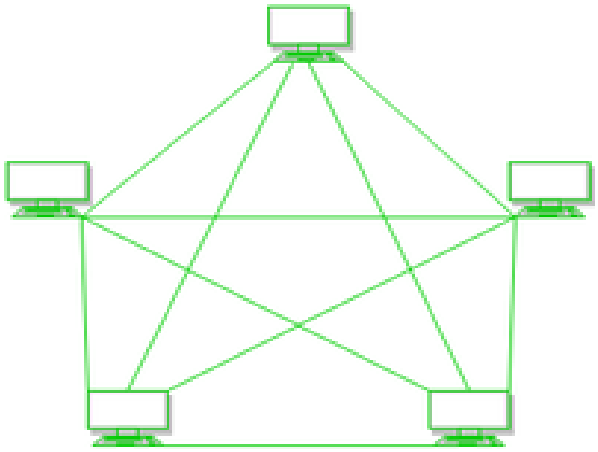
1) Tree topology is a combination of bus and star topology. So the features of both bus and star topologies are added to the tree topology.
2) It is easy to expand the network. We just need an extra hub and cables. More star networks are added to the main cable or bus without any issue.
3) If any node gets disconnected from the tree network then other nodes will function regularly. The performance of the network is not affected by removing any node.

Disadvantages of Tree topology:

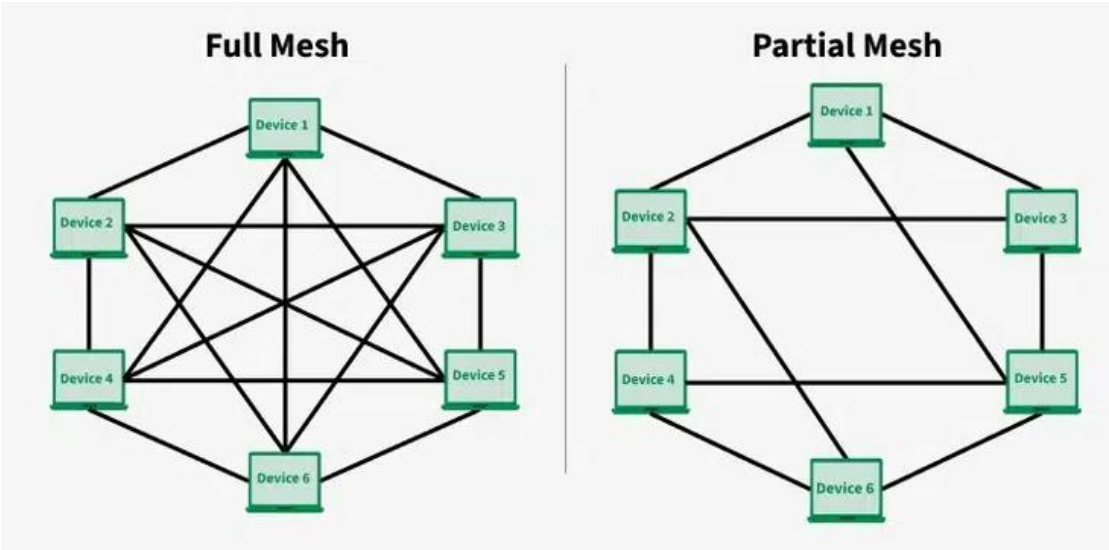
1) Tree topology is dependent on the main bus cable. If the main bus gets any problem the whole network will fail to perform.
2) If more and more segments/nodes are added to the network then it becomes a problem to manage the network.
3) If any hub stops working then some nodes in the network become disconnected from the network.

Mesh Topology:

In mesh, all the computers are interconnected to every other in a network as shown in Fig.(j).Each computer not only sends its own signals but also receives data from other computers. The nodes are connected to every other completely via a dedicated link during which information is travel from nodes to nodes and there are N(N-1)/2 links in mesh if there are N nodes. Every node features a point-to-point connection to the opposite node.



Fig(j): A LAN Mesh topology



There are two types of Mesh topologies

1. Fully-connected Mesh Topology
2. Partially-connected Mesh Topology

In wired full-mesh topology, each device on the network is connected together, creating connections between all device on the network. Full-Mesh topology provide an extreme level of redundancy when compared with other network topologies. The main advantage in full-mesh topology is, if any connection between two devices failed, there is always an alternate path exists to reach the destination.Full-mesh topology works well in a small network. Example; less than five devices. But as the number of devices in the network increases, Full-Mesh topology based networks become complex.

A partial-mesh topology is also a mesh topology similar to full-mesh topology. In partial-mesh topology, all the devices are not connected to each other as in full-mesh topology. In partial-mesh topology, some of the devices are connected to many devices together, but other devices are connected only to one or two devices.

Advantages of Mesh Topology:

1) Failure during a single device won't break the network.
2) There is no traffic problem as there is a dedicated point to point links
3) for every computer.
3)This topology provides multiple paths to succeed in the destination and provides redundancy.
4) Data transmission is more consistent because failure doesn't disrupt its processes.
5) Adding new devices won't disrupt data transmissions.

Disadvantages of Mesh Topology:

1) It is costly as compared to the opposite network topologies i.e. star, bus, point to point topology.
2) Installation is extremely difficult in the mesh.
3) Power requirement is higher as all the nodes will need to remain active all the time and share the load.
4) Maintenance needs are challenging with a mesh.

Hybrid Network Topologies:

Hybrid topology is an interconnection of two or more basic network topologies, each of which contains its own nodes. The resulting interconnection allows the nodes in a given basic topology to communicate with other nodes in the same basic topology as well as those in other basic topologies within the hybrid topology.

There are different types of hybrid network topologies depending on the basic topologies that make up the hybrid and the adjoining topology that interconnects the basic topologies.

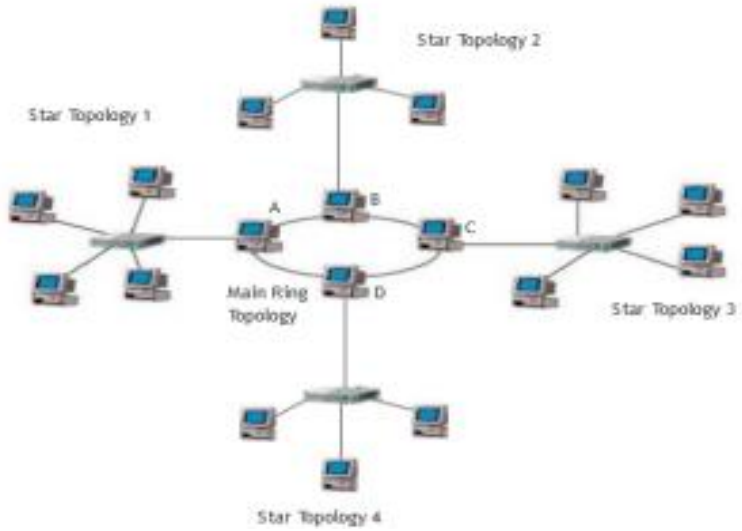
The following are some of the hybrid network topologies:
1. Star-Wired Ring Network Topology

2. Star-Wired Bus Network Topology

3. Hierarchical Network Topology

In a star-wired ring hybrid topology, a set of star topologies are connected by a ring topology as the adjoining topology. Joining each star topology to the ring topology is a wired connection.

Figure (k) is a diagrammatic representation of the star-wired ring topology:



In the above fig, individual nodes of a given star topology like Star Topology 1 are interconnected by a central switch which in turn provide an external connection to other star topologies through a node A in the main ring topology.
Information from a given star topology reaching a connecting node in the main ring topology like A flows either in a bidirectional or unidirectional manner. A bidirectional flow will ensure that a failure in one node of the main ring topology doesn't lead to the complete breakdown of information flow in the main ring topology.

Advantages of Hybrid Topology:
1) This type of topology combines the benefits of different types of topologies in one topology.
2) It is easily scalable as Hybrid networks are built in a fashion which enables easy integration of new hardware component
3) Handles a large volume of traffic.
4) It is used to create large networks.
5)The speed of the topology becomes fast when two topologies are put together.

Disdvantages of Hybrid Topology:

1) It is a type of expensive network.
2) The design of a hybrid network is very complex.
3) Usually, hybrid architectures are larger in scale so they require a lot of cables in the installation process.
4) Installation is a difficult process.

LAN HARDWARE:

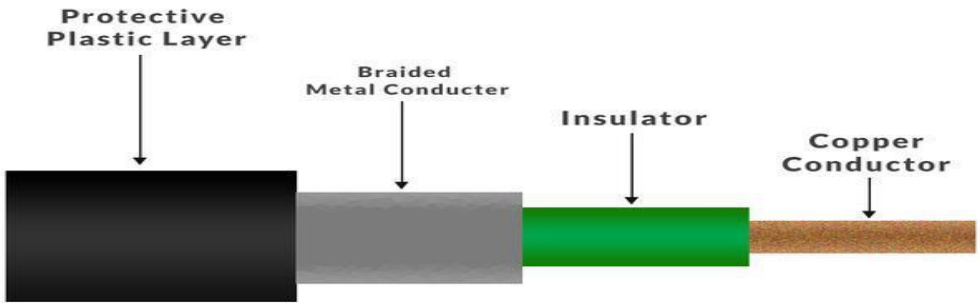
All LANs are a combination of hardware and software. The primary hardware devices are the computers themselves and the cables and connectors that link them. Additional pieces of hardware unique to networks include network interface cards, repeaters, hubs and concentrators, bridges, routers, gateways, and many other special interfacing devices.

Cables:

The three basic cable types used in LANs are coaxial cable, twisted-pair, and fiber-optic cable. Most local-area networks started with usage of coaxial cable, but today twisted-pair cable dominates. Fiber- optic cable is used in higher-speed, secure networks, which are now widespread.

1.Coaxial cable: It is a superior medium because its extremely wide band width permits very high-speed bit rates. Although loss is generally high, attenuation is usually offset by using repeaters that boost the signal level and regenerate the signal waveshape. The major benefit of coaxial cable is that it is completely shielded, so that external noise has little or no effect on it. Coax was once widely used in LAN cabling but today has been primarily replaced with twisted-pair cable.

It is a type of guided media made of plastics, and copper wires which transmit the signal in electrical form rather than light form which is shown in fig(l) below.



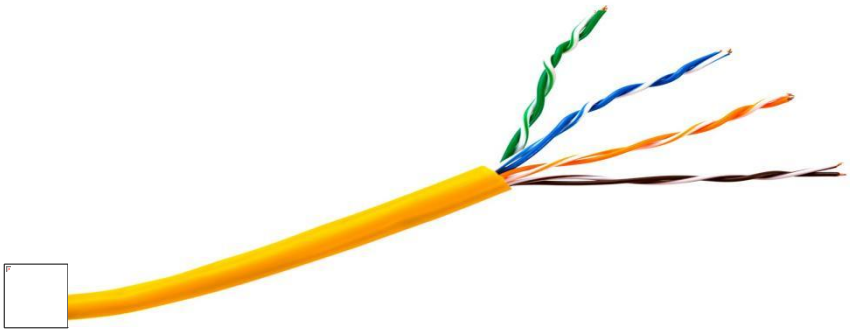
Fig(l):Coaxial Cable

The core copper conductor is used for the transmission of signals and the insulator is used to provide insulation to the copper conductor.The insulator is surrounded by a braided metal conductor which helps to prevent the interference of electrical signals and prevent cross talk. This entire setup is again covered with a protective plastic layer to provide extra safety to the cable.

2.Twisted Pair cable:

Twisted pair cables have been around for a long time. They were mainly invented for voice transmissions. Twisted pair is a widely used medium in networking because it's lighter, cheaper, more flexible, easy to install, and provides greater speeds than coaxial cables. There are two types of twisted pair cables: the unshielded twisted pair (UTP) and the shielded twisted pair (STP).

The unshielded twisted pair cable has 4 pairs of copper wires that are present inside a plastic sheath. These wires are twisted to protect them from interference. The only protection available for a UTP cable is a plastic sheath that is thin in size which is shown in fig(m) below:



Fig(m): Unshielded Twisted Pair Cable

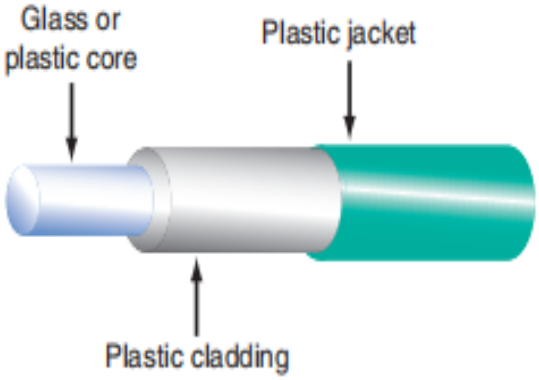
The shielded twisted pair cable is widely used in high-speed networks. The major difference between UTP and shielded twisted pair is that STP makes use of a metallic shield to wrap the wires which is shown in fig(n) below

Fig(m): Shielded Twisted Pair Cable

This metallic shield prevents interference to a better extent than UTP. These STP cables come with numbering; the higher the numbering, the better the interference prevention. Most computer networks must go with CAT 3(Category 3) or CAT 5, and nothing less than this.

Fiber Optic Cables:

Fiber optics refers to the technology and method of transmitting data as light pulses along a glass or plastic strand or fiber which is shown in fig(n) below.



Fig(n): Fiber Optic Cable

Fiber optic cables are used for long-distance and high-performance data networking. They are capable of transmitting data over longer distances and at higher bandwidths (data rates) than electrical cables, making them a critical component in modern telecommunications, internet, and computer networking.

The two basic types of fiber cables are multimode fiber (MMF) and single-mode fiber (SMF). MMF is usually the plastic type and used in shorter cables because it has greater loss than glass. SMF is glass, more fragile, and thinner, and offers less loss over longer distances. Special fiber optic connectors are required to attach the cables to the network

equipment. Speeds of up to 1 Tbps (terabits per second) are achievable by using fiber optics.

CONNECTORS:

All cables used in networks have special terminating connectors that provide a fast and easy way to connect and disconnect the equipment from the cabling and maintain the characteristics of the cable through the connection.

Co axial cable connectors:

Coaxial cable requires special connectors that will maintain the characteristics of the cable.Coaxial connectors are designed not only to provide a convenient way to attach and disconnect equipment and cables but also to maintain the physical integrity and electrical properties of the cable.The choice of a coaxial connector depends on the type and size of cable, the frequency of operation, and the application. The most common types are the PL-259 or UHF, BNC, F, SMA, and N-type connectors.

Twisted-Pair Connectors:

A larger modular connector known as the RJ-45 connector is widely used in twisted pairs . The RJ-45 contains eight connectors, so it can be used to terminate four twisted pairs. Matching jacks on the equipment or wall outlets are used with these connectors. Most LANs today use RJ-45 connectors.

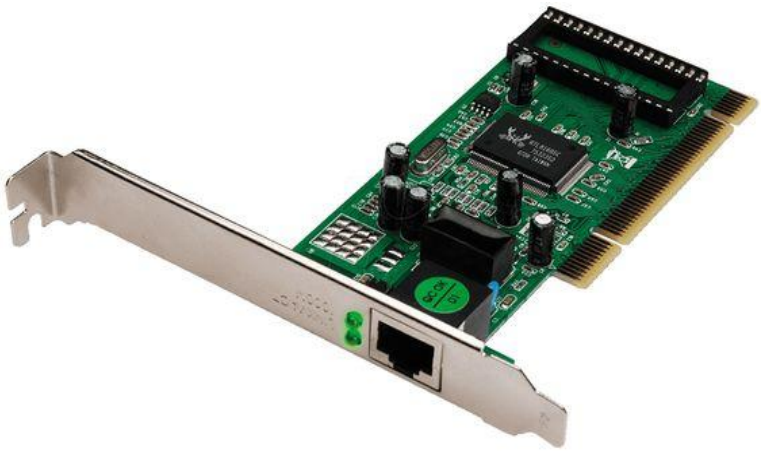
Fiber Optic Connectors:

An optical fiber connector is a device used to link optical fibers, facilitating the efficient transmission of light signals. An optical fiber connector enables quicker connection and disconnection. They come in various types like SC, LC, ST, and MTP, each designed for specific applications. In all, about 100 different types of fiber optic connectors have been introduced to the market but SC and LC connectors are the most common types of connectors on the market.

NETWORK INTERFACE CARD(NIC):

A network interface card (NIC) is a hardware component, typically a circuit board or chip, installed on a computer so it can connect to a network.A network interface card is also known as a network interface controller,network adapter, LAN adapter and physical network interface. It enables data to be sent and received between the computer and other network-connected devices, such as routers or switches. The

NIC can use either wired or wireless technologies to connect the computer to the rest of the network.

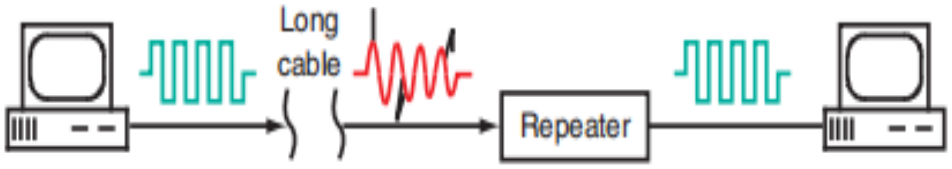


Fig(o): Network Interface Card(NIC)

A NIC acts as an interface between the physical layer, which manages the physical connection with the cable or wireless antenna, and the data link layer, which provides a reliable communication channel. There are two main types of Network Interface Cards-wired and wireless. Wired networks require an Ethernet cable, while Wireless networks rely on radio frequencies provided by an antenna to send and receive data over larger distances with less interference than wired connections.Wireless adapters usually contain several components including an antenna, transceiver chip and amplifier chip in order to communicate with other wireless devices within close range or even across long distances depending on its frequency range capacity.

REPEATERS:

When signals from a NIC must travel a long distance over coaxial cables or twisted-pair cables, the binary signal is greatly attenuated by the resistance of the wires and distorted by the capacitance of the cable. In addition, the cable can pick up noise along the way. As a result, the signal can be too distorted and noisy to be received reliably.
A common solution to this problem is to use one or more repeaters along which is shown in fig(p) below:



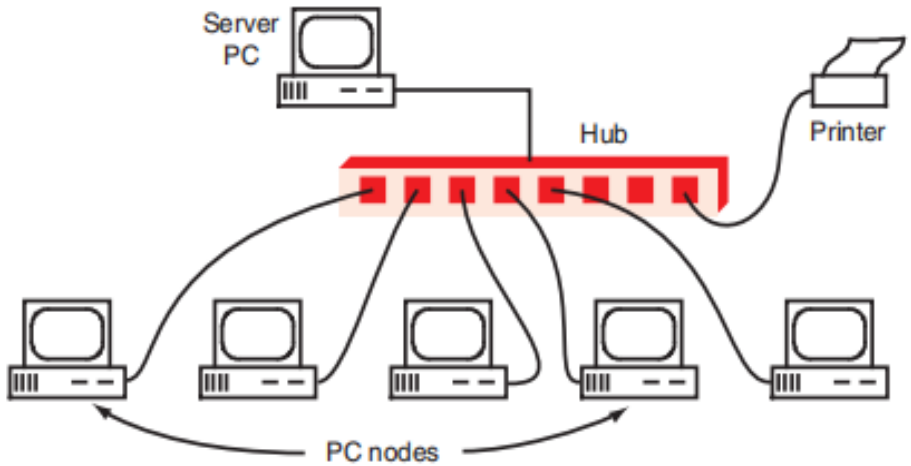
Fig(p) Repeater

A repeater is an electronic circuit that takes a partially degraded signal, boosts its level, shapes it up, and sends it on its way. Over long transmission distances, several repeaters may be required.
Repeaters are small, inexpensive devices that can be inserted into a line with appropriate connectors or built into other LAN equipment. Most repeaters are really transceivers i.e,bidirectional circuits that can both send and receive data. Transceiver repeaters can receive signals from either direction and transmit them in the opposite direction.

Hubs

A Hub is a networking device which receives signal from the source, amplifies it and send it to multiple destinations or computers.Hubs are also called Ethernet Hub, Repeater Hub, Active Hub and Network Hub. Basically it is a networking device which is used in multiple devices like Computers, Servers etc to communicate each other and make them work as a single network segment. Hubs are used in 'Physical Layer' of OSI Model.

Hubs is a small box in rectangular shape which have multiple ports for connecting various devices to it shown in fig(q).

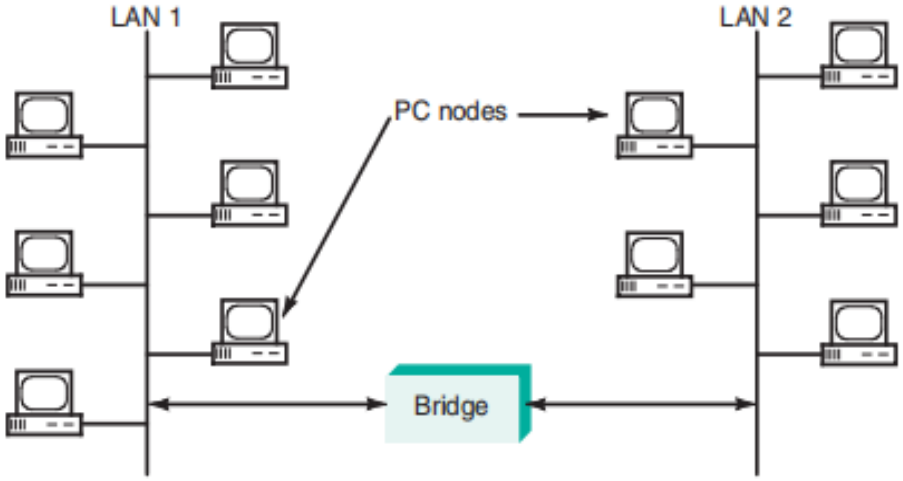


Fig(q) Hub

It receives its power supply from auxiliary power sources. The main work of Hub is to receive incoming data signals, amplify them in the form of electrical signals and then send them to each connected device. A Hub may contain a number of ports. Minimum amount of ports that a hub can have is 8 and it can have up to 48 ports for connecting various devices and peripherals to it.

Bridges:

A bridge is a network device that is connected as a node on the network and performs bidirectional communication between two LANs shown in fig(r) below:



Fig(r)A bridge connects two LANs

A bridge can also be used when one LAN becomes too big. Most LANs are designed for a maximum upper limit of nodes. The reason for this is that the greater the number of nodes, the longer and more complex the wiring. Furthermore, when many individuals attempt to use a LAN simultaneously, performance deteriorates greatly, leading to net work delays. One way to deal with this problem is to break a large LAN into two or more smaller LANs. First it is determined which nodes communicate with other nodes the most, and then a logical breakdown into individual LANs is made. Communication between all users is maintained by interconnecting the separate LANs with bridges. The result is improved overall performance.

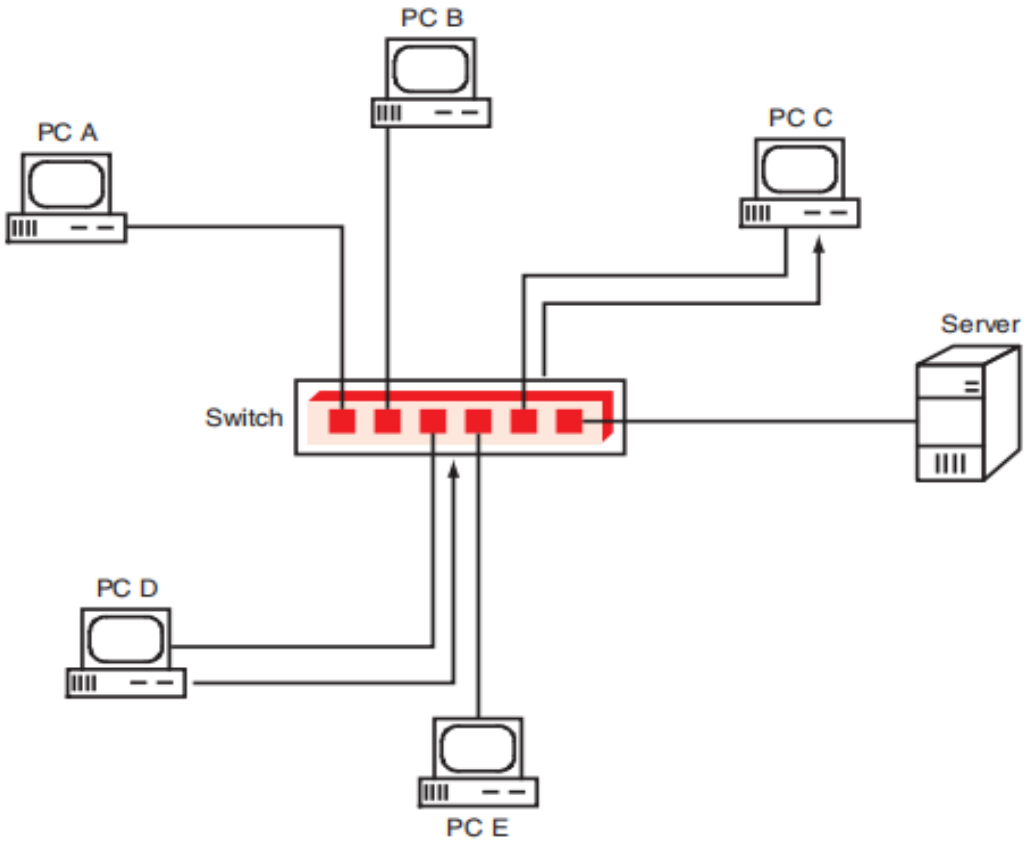
A bridge is generally designed to interconnect two LANs with the same protocol, e.g., two Ethernet networks. However, there are bridges that are able to accomplish protocol conversion so that two LANs with different protocols can converse.

Switches:

A switch is a hub like device used to connect individual PC nodes to the network wiring. Unlike a hub, a switch provides a means to connect or disconnect a PC from the network wiring. Switches have largely replaced hubs in most large LANs because switches greatly expand the number of possible nodes and improve performance.

As a network grows, more and more nodes are connected to the wiring. This has the effect of slowing down data transfers as all nodes must share the media. The longer cables restrict the data rate. And the greater number of users vying for the cable makes access times longer. These problems are overcome with a switch. The switch can be used to divide the LAN into smaller segments. This immediately improves performance. LAN switches recognize individual node addresses. When transmitting data from one PC to another, the switch detects the address of the receiving PC and connects it to the wiring. Otherwise, a PC is disconnected from the wiring by the switch until it is ready to send or receive data. By reducing the loads imposed by all the unused PCs, the switch allows the network to be significantly faster.

Ethernet switches have become the key component in most LANs. They implement the interconnection between servers, PCs, and other nodes but also speed up the entire network by reducing the number of collisions and allowing one PC to speak directly to another. This arrangement also provides increased network security by preventing intrusions from one node to the others.
Fig. (s) shows how a switch works.



Fig(s) Ethernet Switch

If PC D wants to send data to PC C, it does so directly by connecting the two PCs together. The other computers on the network are not involved, so their connections do not load the network circuitry. No collisions occur, so the data transfer is as fast as the network allows. The switch is usually provided with software that allows it to be configured in different ways. For example, a broadcast mode is available where one PC can transmit the same message to all computers on the network.

The switch identifies each PC by its media access control (MAC) address. The MAC address is a 48-bit number unique to each PC. The MAC address is made up of 6 bytes or octets identified by its hexadecimal code in the following format:

00:A0:C9:14:D3:29

The first 3 bytes identify the manufacturer of the NIC or PC, such as Intel, Dell, or Cisco; the last 3 bytes are special to the PC or other device. The MAC address is hardwired into each NIC or PC when it is built and is used as the source or destination address in the Ethernet protocol frame. Ethernet switches use the MAC address to route the data from the source to the desired destination. The switch actually "learns" the addresses as the network is used and creates a MAC address lookup table in its memory. It also learns which ports each PC is connected to. The lookup table is updated each time a message is sent or received.

Routers:

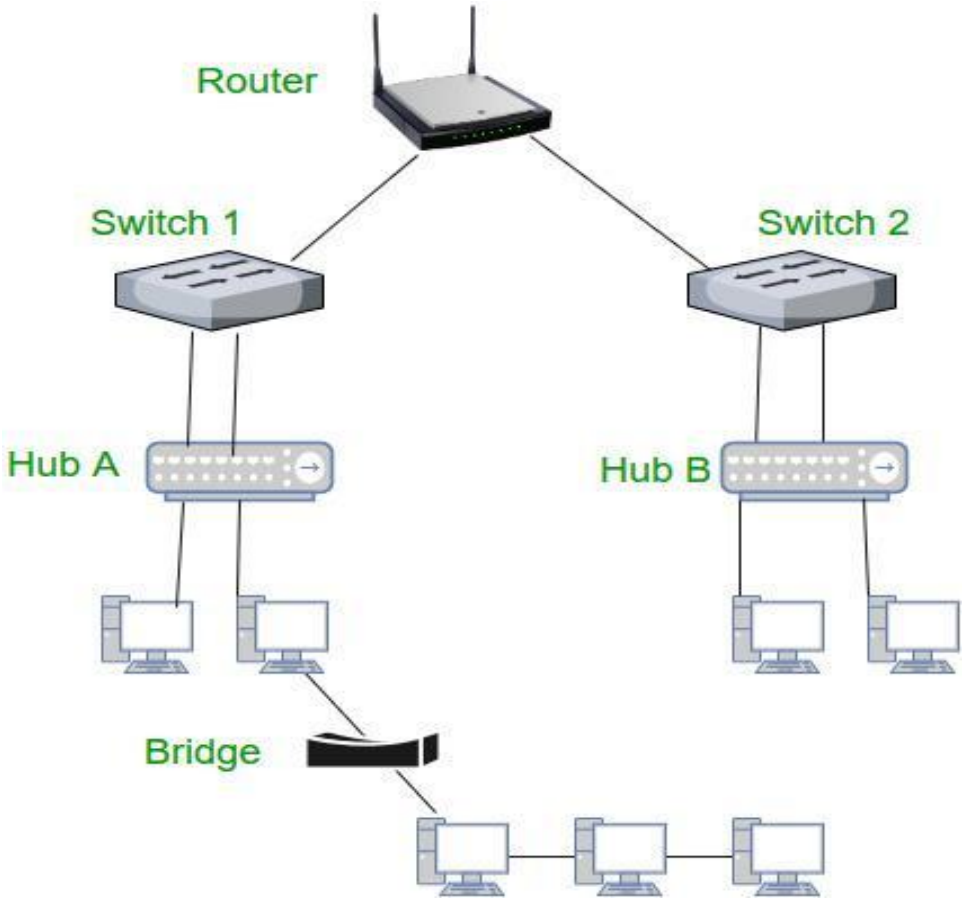
Like bridges, routers are designed to connect two networks. The main difference between bridges and routers is that routers are intelligent devices that have decision-making and switching capabilities.

Fig(g): Router

A Router is a networking device that forwards data packets between computer networks. By sending data packets to their intended IP

addresses, it manages traffic between different networks and permits several devices to share an Internet connection.

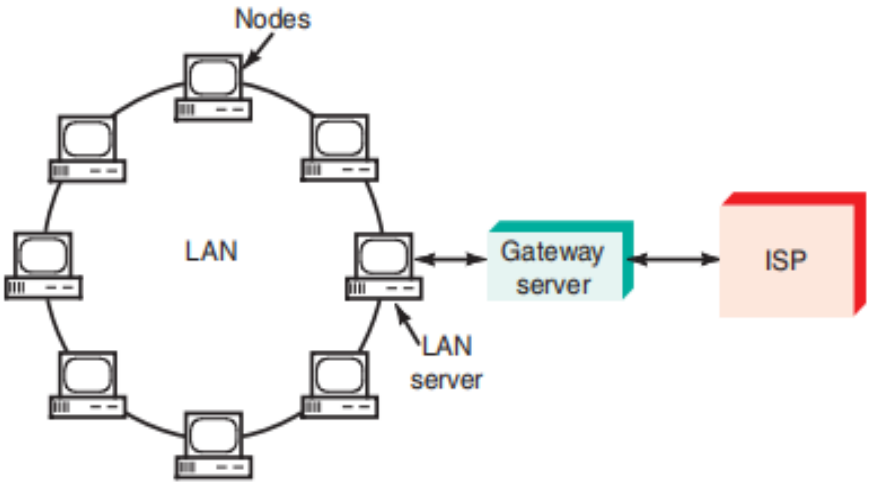
A router determines a packet's future path by examining the destination IP address of the header and comparing it to the routing database. The list of routing tables outlines how to send the data to a specific network location. They use a set of rules to determine the most effective way to transmit the data to the specified IP address.
To enable communication between other devices and the internet, routers utilize a modem, such as a cable, fiber, or DSL modem. Most routers include many ports that can connect a variety of devices to the internet simultaneously. In order to decide where to deliver data and where traffic is coming from, it needs routing tables.



Fig(t) Router Network

Gateways:

A gateway is another inter network device that acts as an interface between two LAN s or between a LAN and a larger computer system which is shown in fig(u) below.



Fig(u):Gateway

The primary benefit of a gateway is that it can connect networks with incompatible protocols and configurations
There are two main types of gateways: unidirectional gateways and bidirectional gateways.

Unidirectional gateways also known as one way gateway allow data to flow in only one direction. The information is transmitted from one network to another but in the opposite direction it is not possible to send or receive data. This type of gateway is used in situations where it is important to limit the flow of information to one direction only for security or other reasons.

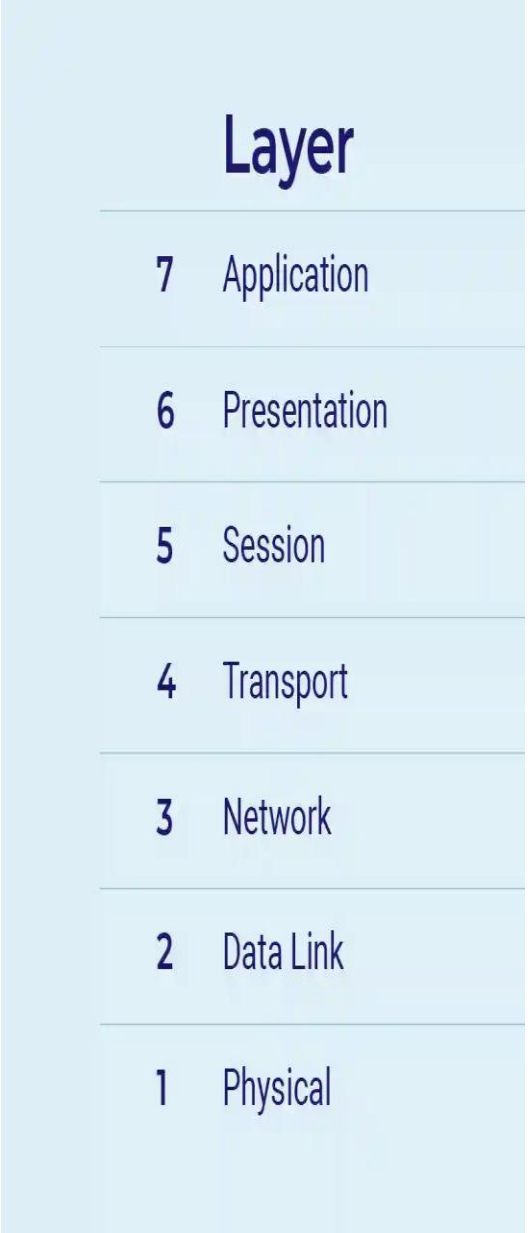
Bidirectional gateways allow data to flow in both directions. They can be used as synchronization tools.

The three criteria necessary for an effective and efficient network are **performance, reliability and security.**
1) Performance of the network depends on number of users, type of transmission medium, and the capabilities of the connected hardware and the efficiency of the software.
2) Reliability is measured by frequency of failure, the time it takes a link to recover from the failure and the network's robustness(network's ability to remain connected and functional even when it's attacked randomly or deliberately)
3) Security issues include protecting data from unauthorized access and viruses.

Computer networks communicate using protocols, which define the procedures that the systems involved in the communications process will use. Numerous protocols are used today to provide networking capabilities, such as how much data can be sent, how it will be sent, how it will be addressed, and what procedure will be used to ensure that there are no undetected errors. **Data communications protocols** are sets of rules governing the orderly exchange of data within the network or portion of network.The list of protocols used by a system is called a protocol stack which generally includes only one protocol per layer.

OSI SEVEN LAYER PROTOCOL

Open Systems Interconnection(OSI) is the name for a set of standards for communicating among computers. The primary purpose of OSI standards is to serve as a structural guide for exchanging the information between computers, workstations and networks.In 1983, the ISO adopted a seven layer communication architecture reference model which is shown in fig(v) below:The OSI model uses an approach called layering to illustrate and explain the message exchange process. This approach divides the various functions and services provided by a network into discrete groupings called layers, as illustrated in figure .



Fig(v): OSI seven layer protocol hierarchy

7.Application Layer:

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

6.Presentation Layer:

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

5.Session Layer:

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

4.Transport Layer:

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

3.Network Layer:

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

2.Data Link Layer:

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

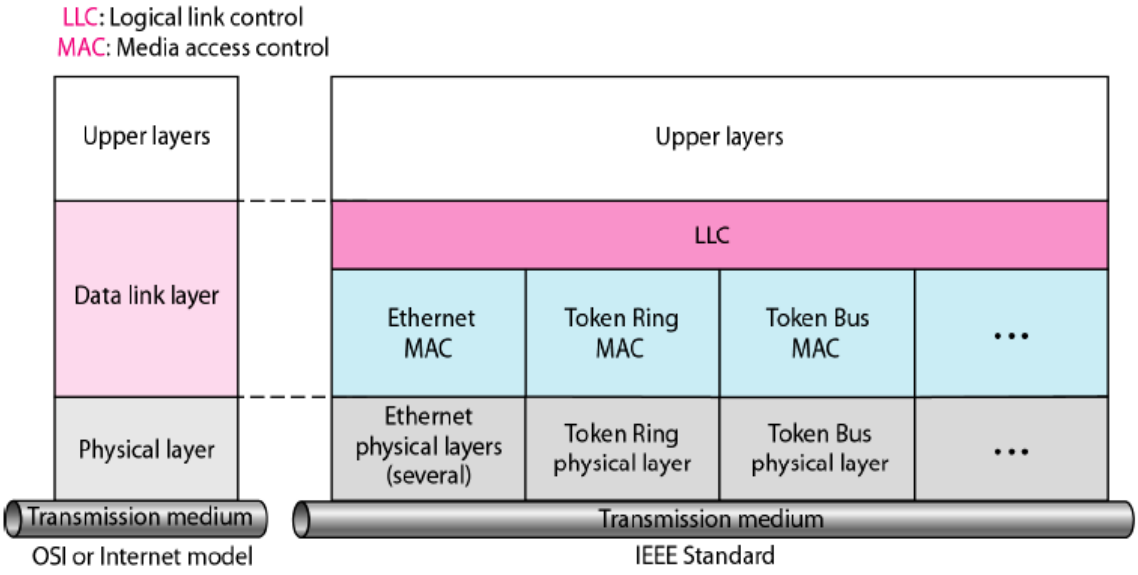
Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.

1.Physical Layer:

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

IEEE STANDARDS:

In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards and to enable inter communication among equipment from a variety of manufacturers. Project 802 is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.
Figure (w) gives relationship of 802 standard to the traditional OSI Model:



IEEE 802 standard split data link layer into two sublayers
• LLC(Logical Link Control) and MAC (Media Access control)

In addition to this IEEE 802 created several physical layer standards for different LAN protocols
• Ethernet Physical layer

• Token ring Physical layer
• Token bus physical layer

LLC(Logical Link Control)

▪ In IEEE 802 standard LLC sub layer carries out flow control, error control and framing.
▪ LLC provides one single Data link protocol for all LANS whereas MAC provides different protocols for different LANS as shown in figure (w).
• The intent of LLC is to provide flow control and error control for upper layers.

MAC (Media Access Control)

IEEE 802 has created a sublayer called MAC that defines specific access method for each LAN for example it defines CSMA/CD as Media access method for Ethernet LAN's and token passing method for token ring and token bus LAN.

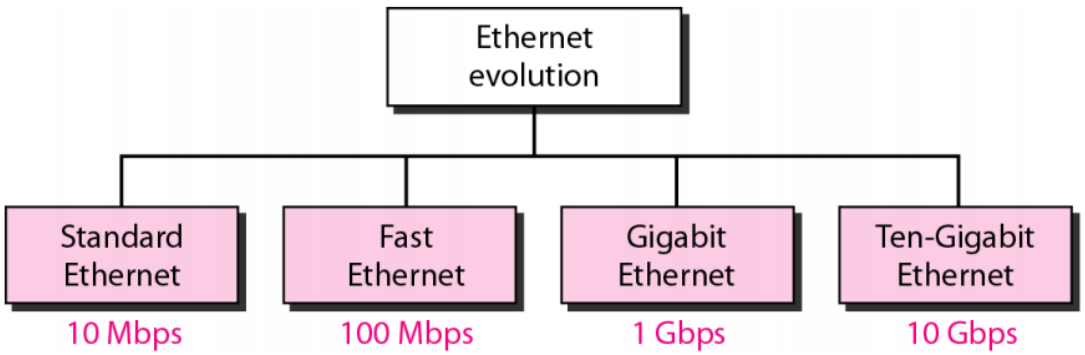
SNo	IEEE Standards in computer networks	Description
1	IEEE 802	Overview and architecture of LAN/MAN.
2	IEEE 802.1	Bridging and management of LAN/MAN.
3	IEEE 802.1s	Multiple spanning trees.
4	IEEE 802.1w	Rapid reconfiguration of spanning trees.
5	IEEE 802.1x	Network access control of ports.
6	IEEE 802.2	Logical Link Control (LLC).
7	IEEE 802.3	Ethernet(CSMA/CD)
8	IEEE 802.4	Token Bus
9	IEEE 802.5	Defined MAC Layer for token ring
10	IEEE 802.6	Metropolitan Area Networks
11	IEEE 802.7	Broadband LAN using co axial cable
12	IEEE 802.8	Fiber Optic practices
13	IEEE 802.9	Integrated services LAN
14	IEEE 802.10	Interoperable LAN security
15	IEEE 802.11	Wireless LAN and mesh
16	IEEE 802.12	Demand Priority

17	IEEE 802.13	Not Used
18	IEEE 802.14	Cable Modems
19	IEEE 802.15	Wireless PAN
20	IEEE 802.15.1	Bluetooth Certification
21	IEEE 802.15.4	ZigBee Certification
22	IEEE 802.16	BroadBandWireless Access(WiFi)
23	IEEE 802.16e	BroadBandWireless Access(Mobile)
24	IEEE 802.17	Resilient Packet Ring

ETHERNET LAN

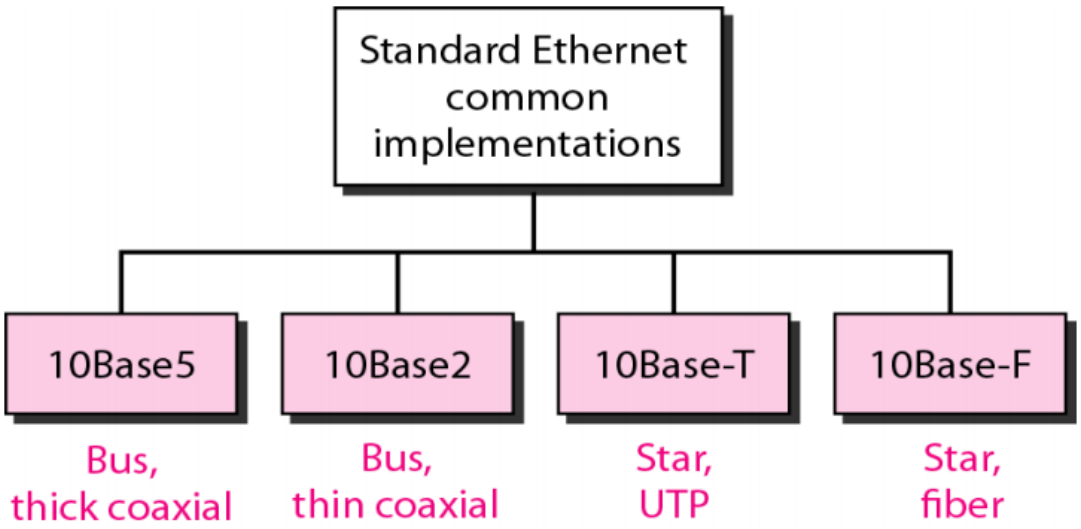
Ethernet has been a relatively inexpensive, reasonably fast, and very popular LAN technology for several decades. Two individuals at Xerox PARC -- Bob Metcalfe and D.R. Boggs developed Ethernet beginning in 1972 and specifications based on this work appeared in IEEE 802.3 in 1980. Ethernet has since become the most popular and most widely deployed network technology in the world. Many of the issues involved with Ethernet are common to many network technologies, and understanding how Ethernet addressed these issues can provide a foundation that will improve your understanding of networking in general.

Ethernet Evolution through four generations:



1.Standard Ethernet

The Standard Ethernet defines several physical layer implementations; four of the most common are shown below



1.10Base5 (Thick Ethernet):

a) **Cable**:Thick coaxial cable ("yellow cable")
b) **Topology**: Bus Topology
c) **Maximum segment length**: 500m
d) **Nicknamed**: Thicknet

Used in the **earliest Ethernet networks**

2. 10Base2 (Thin Ethernet):

a)**Cable**:Thin coaxial cable
b)**Topology:** Bus Topology
c)**Maximum segment length:** 185m
d)**Nicknamed:** Thinnet or Cheapernet

Cheaper and easier to install compared to 10Base5, but still used bus topology (single cable backbone)

3. 10Base-T (Twisted Pair Ethernet)

a)**Cable**: Unshielded Twisted Pair (UTP), typically Cat3 or better
b)**Topology:** Star topology (devices connect to a central hub/switch)
c)**Maximum segment length:** 100 meters per cable run

Much more reliable and scalable than coaxial-based Ethernet

4. 10Base-F (Fiber Ethernet)

a)**Cable**: Fiber optic cable
b)**Topology:** Star topology
c)**Maximum segment length:** Up to 2000 meters (depending on type)

Provided higher resistance to electromagnetic interference, suitable for long-distance and backbone connections

2.Fast Ethernet:

Fast Ethernet is a networking standard that increased the data transfer speed of Ethernet from 10 Mbps to 100 Mbps. Introduced in 1995 as the IEEE 802.3u standard, it was a major improvement over the original Ethernet and became a foundation for later, faster standards like Gigabit Ethernet.

Key features

1.Speed: Offers a maximum data rate of 100 megabits per second (Mbps).

2.Backward compatibility: Works seamlessly with older 10 Mbps Ethernet networks, making upgrades relatively simple.

3.Cost-effectiveness: Provided a significant performance boost over older networks without requiring a complete and expensive overhaul of the existing cabling infrastructure.

4.Media flexibility: Operates over both twisted-pair copper cables and fiber-optic cables.

5.Duplex modes: Supports both half-duplex (sending or receiving data at one time) and full-duplex (simultaneous sending and receiving) operation.

Common Fast Ethernet variants

1.100BASE-TX: The most widespread Fast Ethernet standard, it runs over two pairs of Category 5 (Cat5) or better copper twisted-pair cable. It is used in most home and office Local Area Networks (LANs) for distances up to 100 meters.

2.100BASE-FX: This standard uses fiber-optic cable for data transmission, allowing for much longer distances up to 2 kilometers with multimode fiber. This makes it ideal for backbone connections in larger networks or in environments with high electromagnetic interference.

3.100BASE-T4: A less common and now obsolete standard, this variant was designed to achieve 100 Mbps over four pairs of older Category 3 cabling. It was created to offer an upgrade path for older generation networks but became unnecessary as Cat5 cabling became standard.

3.Gigabit Ethernet:

Gigabit Ethernet (GbE) is a networking standard that transmits data at a rate of 1 gigabit per second (Gbps), or 1,000 Mbps. It is a significant upgrade from Fast Ethernet, which operates at 100 Mbps, making it ten times faster. Since its introduction in 1999, GbE has become the standard for most wired local area networks (LANs) due to its superior speed and compatibility with older Ethernet technology.

Key features of Gigabit Ethernet

1.High speed: With a maximum speed of 1 Gbps, it provides ample bandwidth for modern applications, such as 4K video streaming, online gaming, and transferring large files.

2.Widespread compatibility: GbE uses the same framing structure and protocols as previous versions of Ethernet (IEEE 802.3), allowing it to integrate easily into existing networks.

3.Uses common cabling: While early GbE standards relied on fiber optics, the popular 1000BASE-T standard can run over common twisted-pair copper cables, like Category 5e (Cat 5e) or Cat 6, making upgrades more affordable for many organizations.

4.Full-duplex operation: GbE operates in full-duplex mode when connected via switches, allowing data to be sent and received simultaneously. This eliminates collisions and doubles the potential bandwidth for point-to-point links.

Common Gigabit Ethernet variants:

Gigabit Ethernet is implemented in several physical layer standards for different media and distances:

1.1000BASE-T: The most common GbE standard for local networks, it uses all four pairs of a Cat 5e, Cat 6, or Cat 7 copper cable to achieve 1 Gbps speeds over distances up to 100 meters.

2.1000BASE-SX: This standard uses fiber-optic cable and a short-wavelength laser for connections over multimode fiber. It is popular for intra-building links in large office buildings and data centers, with a maximum reach of up to 550 meters.

3.1000BASE-LX: Using a long-wavelength laser and fiber-optic cable, this standard can transmit GbE over longer distances—up to 10 kilometers using single-mode fiber.

4.1000BASE-CX: An older standard that is now largely obsolete, this version used shielded twisted-pair copper cable for connections up to 25 meters.

4.10 Gigabit Ethernet:

10 Gigabit Ethernet (10GbE) is a networking standard that transmits data at 10 gigabits per second (Gbps)—ten times the speed of standard Gigabit Ethernet (1GbE). First standardized by the IEEE in 2002, 10GbE was initially adopted in data centers and high-performance networks, but is now becoming more common in enterprise and high-end home networks.

Key features

1.Speed: Provides data transfer rates up to 10 Gbps, enabling faster backups, reduced latency, and support for bandwidth-intensive applications like 4K video editing, virtualization, and cloud computing.

2.Full-duplex only: Unlike older Ethernet standards, 10GbE only operates in full-duplex mode, allowing data to be sent and received simultaneously. This eliminates collisions and makes repeaters obsolete.

3.Media options: 10GbE can operate over both fiber optic and copper twisted-pair cables, with different standards for varying distances and performance needs.

4.Backward compatibility: It maintains the same Ethernet frame format as previous versions, ensuring compatibility with existing Ethernet networks.

Common 10 Gigabit Ethernet variants

Different physical layer standards exist for 10GbE, each designed for specific media and distances

1.10GBASE-T: The most common copper standard, it delivers 10 Gbps speeds over standard twisted-pair cabling. Requires Category 6a (Cat6a) or higher for runs up to 100 meters.

2.10GBASE-SR: The most common and lowest-cost fiber standard for short distances.Uses multimode fiber using short-wavelength (850nm) lasers.The cable length is up to 300 meters on OM3 fiber and 400 meters on OM4 fiber.

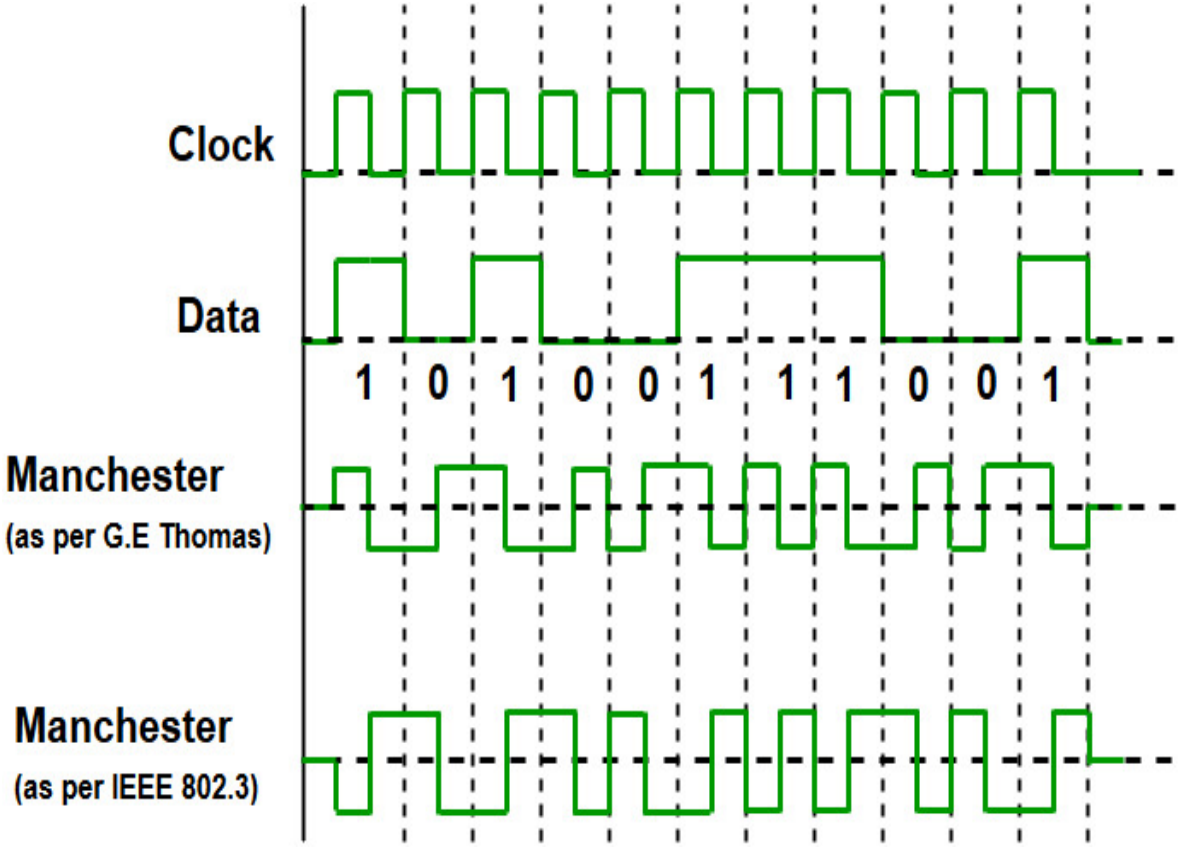
3.10GBASE-LR: A fiber standard designed for long-distance connections. Uses single-mode fiber with a long-wavelength (1310nm) laser. Supports distances up to 10 kilometers.

4.10GBASE-ER: An "extended range" fiber standard for very long distances.Uses single-mode fiber with a long-wavelength (1550nm) laser.Supports distances up to 40 kilometers.

5.10GBASE-CX4: An older, now-legacy standard for very short copper links, typically within data center racks.Uses shielded twinaxial copper cabling.Distance is limited to 15 meters

Encoding:

Ethernet uses baseband data transmission methods. This means that the serial data to be transmitted is placed directly on the bus media. Before transmission, however, the binary data is encoded into a unique variation of the binary code known as the Manchester code shown in fig(x) below



Fig(x): Manchestar Encoding

Topology:

Topology is the shape of a local-area network (LAN) or other communications system. In other words, a topology describes pictorially the configuration or arrangement of a (usually conceptual) network, including its nodes and connecting lines.Ethernet uses topology to transfer the data.There are four principal topologies used in LANs.

- **Bus topology:** All devices are connected to a central cable, called the bus or backbone. Bus networks are relatively inexpensive and easy to install for small networks. Ethernet LAN and Token bus LAN uses bus topology.
- **Ring topology:** All devices are connected to one another in the shape of a closed loop, so that each device is connected directly to two other devices, one on either side of it. Ring topologies are relatively expensive and difficult to install, but they offer high bandwidth and can span large distances.Token Ring LAN uses ring topology
- **Star topology:** All devices are connected to a central hub. Star networks are relatively easy to install and manage, but bottlenecks can occur because all data must pass through the hub.Ethernet LAN uses star topology
- **Tree topology**: A tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured

workstations connected to a linear bus backbone cable.Ethernet LAN uses tree topology

CSMA/CD:

CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) is a media access control method that was widely used in Early Ethernet LANs when there used to be shared Bus Topology and each node (Computers) was connected by Coaxial Cables. Nowadays Ethernet is Full Duplex and Topology is either Star (connected via Switch or Router) or point-to-point (Direct Connection). Hence CSMA/CD is not used but they are still supported though.
Consider a scenario where there are 'n' stations on a link and all are waiting to transfer data through that channel. In this case, all 'n' stations would want to access the link/channel to transfer their own data. The problem arises when more than one station transmits the data at the moment. In this case, there will be collisions in the data from different stations.This protocol decides which station will transmit when so that data reaches the destination without collisions.

How Does CSMA/CD Work?
Step 1: Check if the sender is ready to transmit data packets.

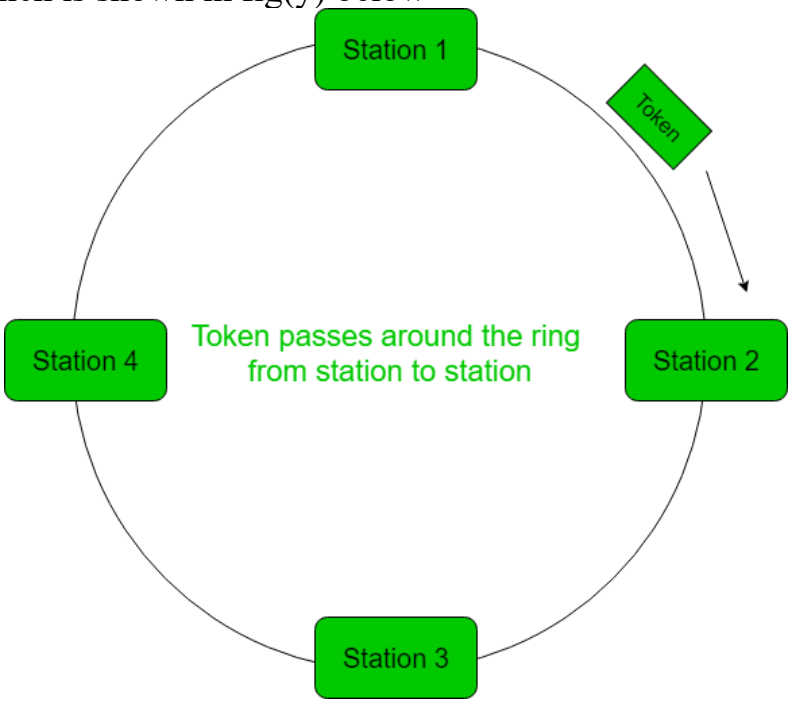
Step 2: Check if the transmission link is idle.
The sender has to keep on checking if the transmission link/medium is idle. For this, it continuously senses transmissions from other nodes. The sender sends dummy data on the link. If it does not receive any collision signal, this means the link is idle at the moment. If it senses that the carrier is free and there are no collisions, it sends the data. Otherwise, it refrains from sending data.

Step 3: Transmit the data & check for collisions.
The sender transmits its data on the link. CSMA/CD does not use an 'acknowledgment' system. It checks for successful and unsuccessful transmissions through collision signals. During transmission, if a collision signal is received by the node, transmission is stopped. The station then transmits a jam signal onto the link and waits for random time intervals before it resends the frame. After some random time, it again attempts to transfer the data and repeats the above process.

Step 4: If no collision was detected in propagation, the sender completes its frame transmission and resets the counters.

TOKEN RING LAN:

A token-ring network is a local area network (LAN) topology that sends data in one direction throughout a specified number of locations by using a token which is shown in fig(y) below



Fig(x): Token Ring LAN

Token ring networks are generally considered either Type 1 or Type 3 configurations. Type 1 networks can support up to 255 stations per network ring and use shielded twisted pair wires

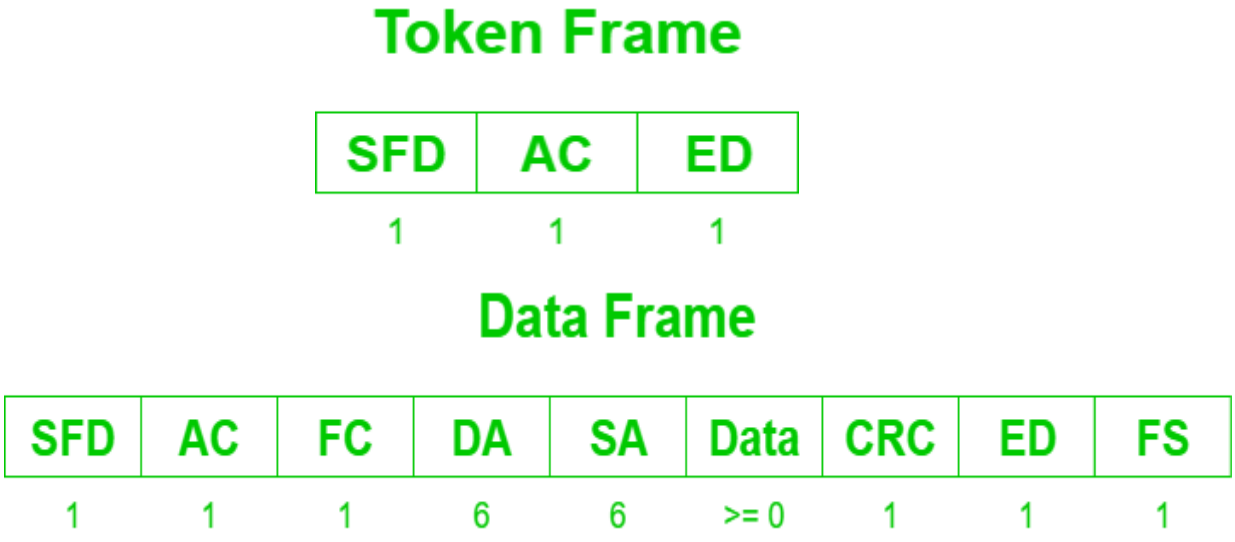
Type 3 networks can support up to 72 stations per network and use unshielded twisted pair wires with Cat3, Cat4 or Cat5 with RJ-45 connectors. Like Ethernet, the token ring functions at Layers 1 and 2 of the Open Systems Interconnection (OSI) model.

The token is the symbol of authority for control of the transmission line. This token allows any sending station in the network ring to send data when the token arrives at that location.A token is a special frame of 3 bytes that circulates along the ring of stations. A station can send data frames only if it holds a token. The tokens are released on successful transfer of the data frames.Whenever a station wants to transmit a frame it inverts a single bit of the 3-byte token which instantaneously changes it into a normal data packet. Because there is only one token, there can atmost be one transmission at a time.

Working of Token Ring:

1. The frame or packet reaches the next station according to the sequence of the ring.
2. Whether the frame contains a message addressed to them is determined by the current node. If yes, then the message is removed by the node from the frame.Then there is an empty frame(an empty frame is called the token frame).If no, the node passes the frame to its adjacent node.
3. A Station that has the token frame, only has the access to transfer the data. If it has data then insert that data into the token frame otherwise release that token for the next station. The next station picks up that token frame for further transmission.

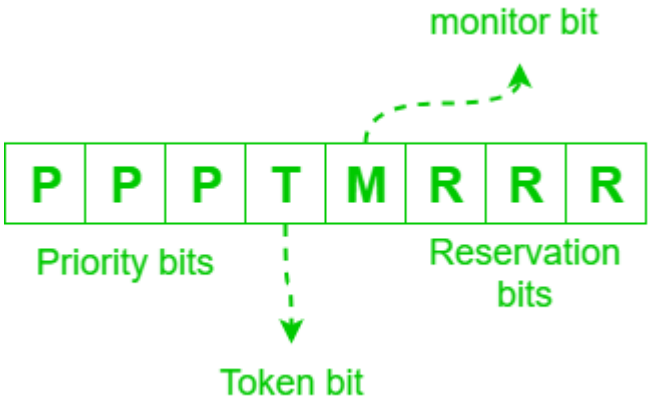
A station may hold the token for the token-holding time which is 10 ms unless the installation sets a different value. If there is enough time left after the first frame has been transmitted to send more frames, then these frames may be sent as well. After all pending frames have been transmitted or the transmission frame would exceed the token-holding time, the station regenerates the 3-byte token frame and puts it back on the ring. The format of Token ring is shown in fig(y) below



Fig(y): Token Frame Format

Start frame delimiter (SFD) –It is a one byte field that marks the beginning of frame.It contains a unique non data bit pattern that a receiving station can easily recognize when a new frame is starting.

Access control (AC)



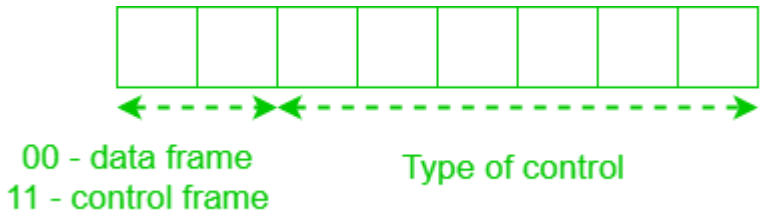
Priority bits and **reservation bits** help in implementing priority. Priority bits = reservation bits = 3 bits each.The priority value(0-7) expresses the minimum priority level required for a station to capture the token.The higher the number is the highest the priority the node gets.The reservation bits are a request mechanism for future token access at higher priorities.

Token bit is used to indicate presence of token frame. If token bit = 1 –> token frame and if token bit = 0 –> not a token frame(i.e, it's a data frame).

Monitor bit helps in solving orphan packet problem(data frames sent by the source node and then it went to shut down are known as orphan packets) . Every station in a token ring network is either an active monitor or a standby monitor. There can be only one active monitor on a ring at a time. The active monitor performs several ring administration functions.. Whenever the Monitor encounter the packet, it changes the monitor bit to 1 which was initially 0 and after that if the Monitor encounter the packet whose monitor bit is 1, it will discard them.

Frame control (FC) – First 2 bits indicates whether the frame contains data or control information. In control frames, this byte specifies the

type of control information.



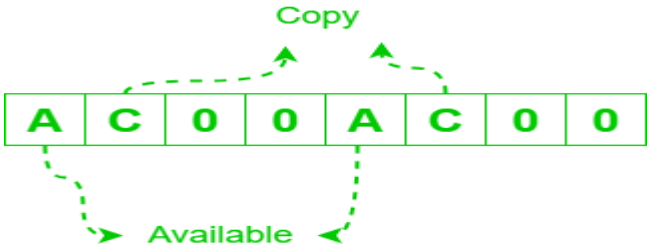
Destination address (DA) and Source address (SA) – consist of two 6-byte fields which is used to indicate MAC address of source and destination.

Data – Data length can vary from 0 to maximum token holding time (THT) according to token reservation strategy adopted. Token ring imposes no lower bound on size of data i.e. an advantage over Ethernet.

Cyclic redundancy check (CRC) – 32 bit CRC which is used to check for errors in the frame, i.e., whether the frame is corrupted or not. If the frame is corrupted, then its discarded.

End delimiter (ED) – It is used to mark the end of frame. It contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.

Frame status (FS) – It Is a 1-byte field terminating a data frame.A one-byte field used as a primitive acknowledgment scheme on whether the frame was recognized and copied by its intended receiver.



Advantages of token rings:
1) Token rings reduce the chances of data collision.
2) Token passing performs better than bus topology under heavy traffic.
3) A server is not needed to control connectivity among the nodes.

Disdvantages of token rings:

1) If the token fails, it can cause the entire network to stop functioning because the whole communication depends on it.
2) Token ring networks generally deliver lower data transmission speeds than Ethernet networks, making them unsuitable for high-bandwidth applications.
3) Token ring networks are more expensive to set up and maintain than Ethernet networks in terms of hardware and support costs.