

Computer Networks and Security

Assignment No.- 01

Name :- Khushal Patil
Class :- TE-2 (R Batch)
Roll No. :- 64

1. What is a Computer Network?

A computer network is a system that connects two or more computing devices for transmitting and sharing information. Computing devices include everything from a mobile phone to a server. These devices are connected using physical wires such as optical fibre, but they can also be wireless.

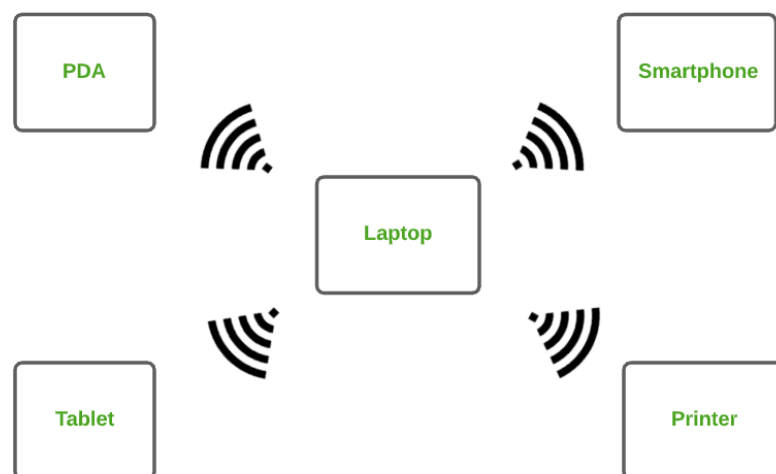


2. Types of Computer Networks

There are mainly five types of Computer Networks

1. Personal Area Network (PAN)

PAN is the most basic type of computer network. It is a type of network designed to connect devices within a short range, typically around one person. It allows your personal devices, like smartphones, tablets, laptops, and wearables, to communicate



and share data with each other. PAN offers a network range of 1 to 100 meters from person to device providing communication. Its transmission speed is very high with very easy maintenance and very low cost. This uses Bluetooth, IrDA, and Zigbee as technology. Examples of PAN are USB, computer, phone, tablet, printer, PDA, etc.

Types of PAN

- **Wireless Personal Area Networks:** Wireless Personal Area Networks are created by simply utilising wireless technologies such as WiFi and Bluetooth. It is a low-range network.
- **Wired Personal Area Network:** A wired personal area network is constructed using a USB.

Advantages of PAN

- PAN is relatively flexible and provides high efficiency for short network ranges.
- It needs easy setup and relatively low cost.
- It does not require frequent installations and maintenance
- It is easy and portable.
- Needs fewer technical skills to use.

Disadvantages of PAN

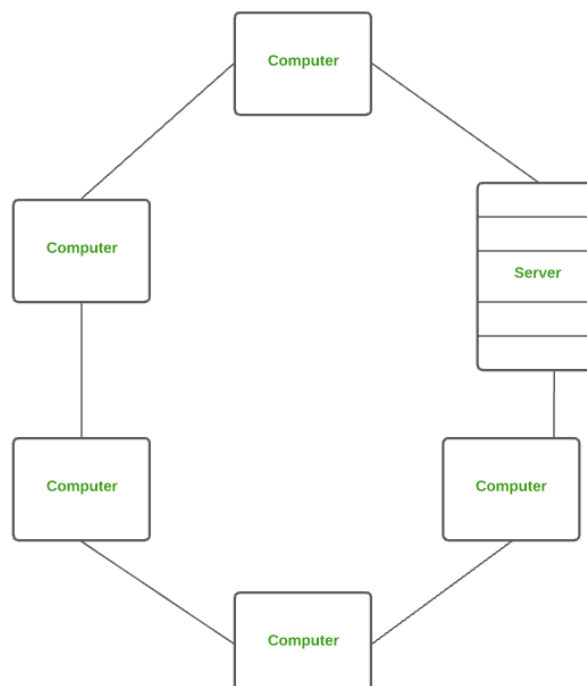
- Low network coverage area/range.
- Limited to relatively low data rates.
- Devices are not compatible with each other.
- Inbuilt WPAN devices are a little bit costly.

Applications of PAN

- Home and Offices
- Organizations and the Business sector
- Medical and Hospital
- School and College Education
- Military and Defense

2. Local Area Network (LAN)

LAN is the most frequently used network. A LAN is a computer network that connects computers through a common communication path, contained within a limited area, that is, locally. A LAN encompasses two or more computers connected over a server. The two important technologies involved in this network are Ethernet and Wi-fi. It ranges up to 2km & transmission speed is very high with easy maintenance and low cost. Examples of LAN are networking in a home, school, library, laboratory, college, office, etc.



Advantages of a LAN

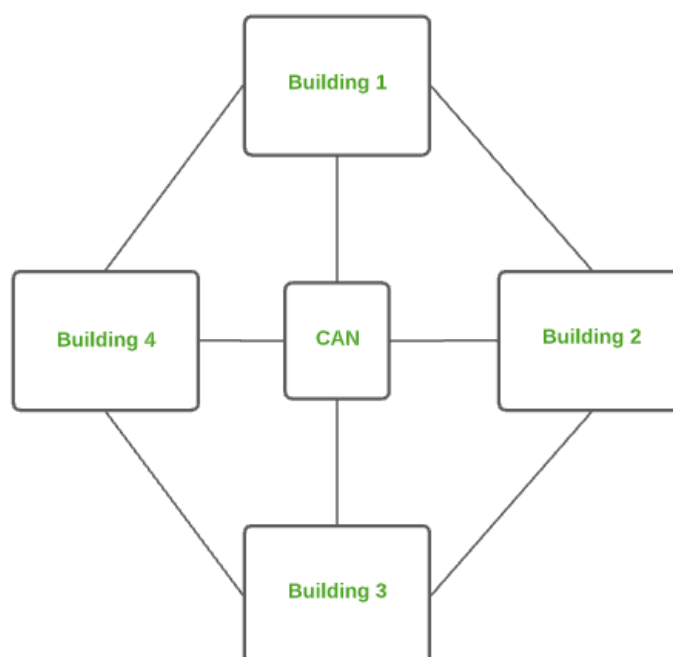
- Privacy: LAN is a private network, thus no outside regulatory body controls it, giving it a privacy.
- High Speed: LAN offers a much higher speed(around 100 mbps) and data transfer rate comparatively to WAN.
- Supports different transmission mediums: LAN support a variety of communications transmission medium such as an Ethernet cable (thin cable, thick cable, and twisted pair), fiber and wireless transmission.
- Inexpensive and Simple: A LAN usually has low cost, installation, expansion and maintenance and LAN installation is relatively easy to use, good scalability.

Disadvantages of LAN

- The initial setup costs of installing Local Area Networks is high because there is special software required to make a server.
- Communication devices like an ethernet cable, switches, hubs, routers, cables are costly.
- LAN administrator can see and check personal data files as well as Internet history of each and every LAN user. Hence, the privacy of the users are violated
- LANs are restricted in size and cover only a limited area
- Since all the data is stored in a single server computer, if it can be accessed by an unauthorized user, can cause a serious data security threat.

3. Campus Area Network (CAN)

CAN is bigger than a LAN but smaller than a MAN. This is a type of computer network that is usually used in places like a school or colleges. This network covers a limited geographical area that is, it spreads across several buildings within the campus. CAN mainly use Ethernet technology with a range from 1km to 5km. Its transmission speed is very high with a moderate maintenance cost and moderate cost. Examples of CAN are networks that cover schools, colleges, buildings, etc.

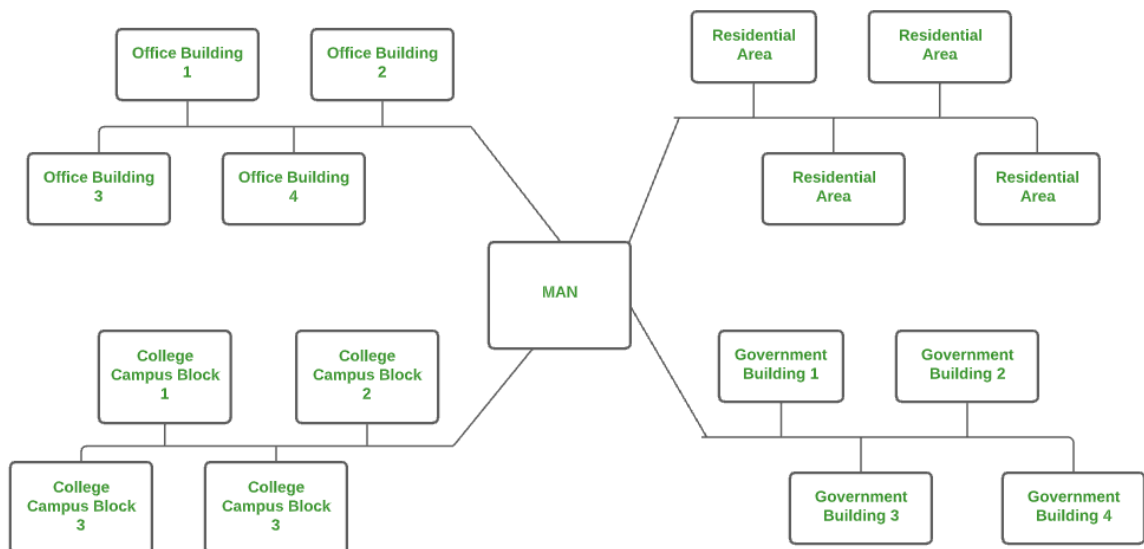


Advantages of CAN

- Speed: Communication within a CAN takes place over Local Area Network (LAN) so data transfer rate between systems is little bit fast than Internet.
- Security: Network administrators of campus take care of network by continuous monitoring, tracking and limiting access. To protect network from unauthorized access firewall is placed between network and internet.
- Cost effective: With a little effort and maintenance, network works well by providing fast data transfer rate with multi-departmental network access. It can be enabled wirelessly, where wiring and cabling costs can be managed. So to work with in a campus using CAN is cost-effective in view of performance

4. Metropolitan Area Network (MAN)

A MAN is larger than a LAN but smaller than a WAN. This is the type of computer network that connects computers over a geographical distance through a shared communication path over a city, town, or metropolitan area. This network mainly uses FDDI, CDDI, and ATM as the technology with a range from 5km to 50km. Its transmission speed is average. It is difficult to maintain and it comes with a high cost. Examples of MAN are networking in towns, cities, a single large city, a large area within multiple buildings, etc.



Advantages of MAN

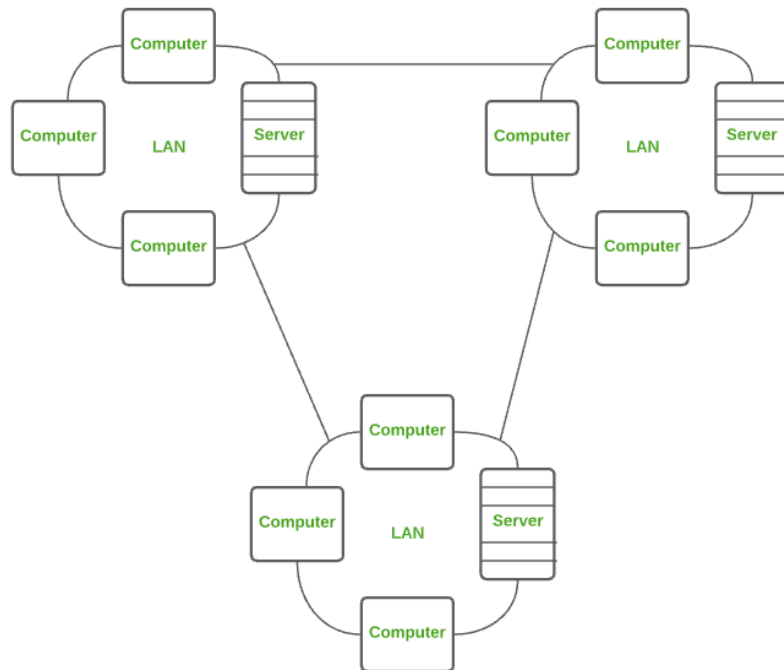
- MAN offers high-speed connectivity in which the speed ranges from 10-100 Mbps.
- The security level in MAN is high and strict as compared to WAN.
- It supports to transmit data in both directions concurrently because of dual bus architecture.
- MAN can serve multiple users at a time with the same high-speed internet to all the users.
- MAN allows for centralized management and control of the network, making it easier to monitor and manage network resources and security.

Disadvantages of MAN

- The architecture of MAN is quite complicated hence, it is hard to design and maintain.
- This network is highly expensive because it required the high cost to set up Fiber optics.
- It provides less fault tolerance.
- The Data transfer rate in MAN is low when compare to LANs.

5. Wide Area Network (WAN)

WAN is a type of computer network that connects computers over a large geographical distance through a shared communication path. It is not restrained to a single location but extends over many locations. WAN can also be defined as a group of local area networks that communicate with each other with a range above 50km. Here we use Leased-Line & Dial-up technology. Its transmission speed is very low and it comes with very high maintenance and very high cost. The most common example of WAN is the Internet.



Advantages of WAN

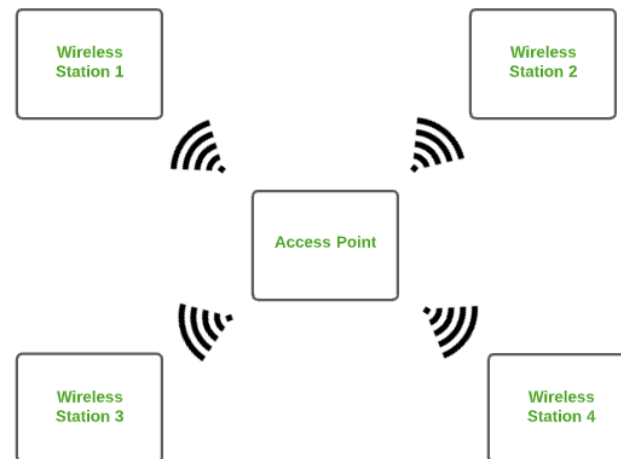
- It covers large geographical area which enhances the reach of organisation to transmit data quickly and cheaply.
- The data can be stored in centralised manner because of remote access to data provided by WAN.
- The travel charges that are needed to cover the geographical area of work can be minimised.
- WAN enables a user or organisation to connect with the world very easily and allows to exchange data and do business at global level.

Disadvantages of WAN

- Traffic congestion in Wide Area Network is very high.
- The fault tolerance ability of WAN is very less.
- Noise and error are present in large amount due to multiple connection point.
- The data transfer rate is slow in comparison to LAN because of large distances and high number of connected systems within the network.

6. Wireless Local Area Network (WLAN)

WLAN is a type of computer network that acts as a local area network but makes use of wireless network technology like Wi-Fi. This network doesn't allow devices to communicate over physical cables like in LAN but allows devices to communicate wirelessly. The most common example of WLAN is Wi-Fi.



3. What is a LAN card?

A LAN card also known as NIC is a hardware component, where network controllers are integrated on to a circuit board that uses standard OSI model of 7 layers to communicate and it acts like a trans-receiver, where it can transmit and receives at the same time while communicating with other devices. Suppose if we want to communicate with another device, let us assume the case of client and server, where the communication between them takes place by firstly sending signals to the physical layer, and then transmitting data packets to the network layer which is an interface at TCP/IP. Connection to the motherboard is made using any one of the following via PCI connector, ISA connector, PCI-E, FireWire, USB, Thunderbolt.

The connection to the network is made via any one of the following: Ethernet, Wi-Fi, Token –Ring, ATM

Functions of NIC

- It acts like a translator, which converts data into a digital signal.
- Communication can be either by using cable wire or by the router which is wireless over the server network
- To communicate over a long distance a network adapter is used.

Types of Network Interface Cards, there are two types NIC they are,

- Ethernet NIC
- Wireless Network NIC



4. Explain RJ45 Connector

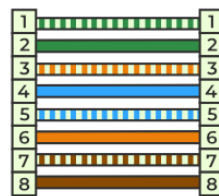
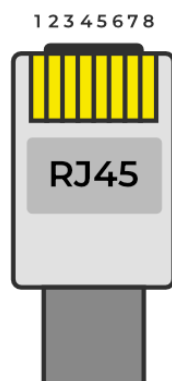
RJ45 stands for Registered Jack 45 and is the most commonly used connector in wired networks. The jacks are mainly used to connect to the Local Area Network (LAN). It was earlier devised for telephones but is now widely used in Ethernet Networking. The 45 in RJ45 basically stands for the listing number. The width of RJ45 is usually greater than that of the telephone cables or other Registered Jacks. Compared to additional jacks the bandwidth provided by these is high and the range is usually 10 Gbps. Because of speed and enhanced security, they are used to connect personal computers to servers, routers etc. These jacks are mostly used in Star Topology.

Structure of RJ45

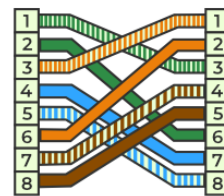
RJ45 has a transparent plastic structure and is an 8-pin connector. It is an 8P8C connector and the number of wires that can be connected is 8. The jacks are mostly used with Shielded Twisted Pair cables or Unshielded Twisted Pair cables. If we take a close look at the end of the Ethernet cable connected to the RJ45 we can see the 8 wires out of which 4 wires are solid coloured and 4 are strip coloured. The classification of RJ45 is done based on the wiring. Some of them include Cat 5e, Cat 6, Cat 7.

Advantages of RJ45

- Initially developed for telephones, RJ45 is now widely used in wired networking. Therefore it has many advantages and some of them are as follows:



Ethernet Patch Cable



Ethernet Crossover Cable

- RJ45 connectors provide much greater speed.
- They are cheaper as compared to other connectors.
- Supports much greater bandwidth (100 Mbps)
- They are very reliable.

Disadvantages of RJ45

- There are many disadvantages of RJ45. Some of them are as follows.
- RJ45 have compatibility issues. They are not compatible with other connectors.
- These connectors are neither weatherproof therefore they do not have much durability.

5. Different Network Devices

Network devices or nodes are computing devices that need to be linked in the network. Some network devices include:



Types of Network Devices

1. Repeater – A repeater operates at the physical layer. Its job is to amplify (i.e., regenerate) the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.

2. Hub – A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

3. Bridge – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2-port device.

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

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

6. Gateway – A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. A gateway is also called a protocol converter.

8. NIC – NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC card is a layer 2 device which means that it works on both the physical and data link layers of the network model.

7. Explain CAT-5 Cable

Alternatively known as an Ethernet cable or LAN cable, a Cat 5 or category 5 is a network cable that consists of four twisted pairs of copper wire terminated by an RJ45 connector. The picture shows an example of a Cat 5 cable.

Cat 5 cable is used in home and business networks, providing data transmission speeds of up to 100 Mbps. The maximum recommended length of a Cat 5 cable is 100 meters. Exceeding this length without the aid of a bridge or other network device could cause network issues, including data packet loss and data transmission speed degradation.

6.1. Wire order in a Cat 5 cable

A Cat 5 cable contains 8 wires and has a specific wire order. If the wires are in a different order, the cable does not work. There are two standards, T568A and T568B, for the order of the wires. Each standard is similar in performance and does not provide an advantage over the other. However, you must use the same wire order on each end of the Cat 5 cable.

The tables and images below display the color and order of the wires in a Cat 5 cable, for each wiring standard.

T568A	
Wire #	Wire Color
1	Green / White
2	Green
3	Orange / White
4	Blue
5	Blue / White
6	Orange
7	Brown / White
8	Brown

T568B	
Wire #	Wire Color
1	Orange / White
2	Orange
3	Green / White
4	Blue
5	Blue / White
6	Green
7	Brown / White
8	Brown



7. Crimping

7.1. What is crimping an ethernet cable?

Crimping an ethernet cable is the process of attaching connectors onto the ends of ethernet cables. This process is also called 'RJ45 crimping' because RJ45 is the name of the connectors that are used for ethernet cables, and they are what is being crimped.

7.2. Why?

Setting up networks involves setting up long ethernet cable connections between different devices. Instead of buying premade ethernet cables of varying lengths (e.g. 5ft, 10ft, 50ft, etc.), it's more practical to just have a big spool of cabling that we can roll out and cut to the exact length we need.

Therefore, we need to be able to attach RJ45 connectors to the ends of these cut cables so that we can actually plug them in

8. Crimping Kit

Here are some tools you should have in your crimping kit!

8.1. RJ45 Crimping Tool

An RJ45 crimping tool is the most essential tool. Although it's technically possible to crimp ethernet cables without this specialized tool, it's not very practical for crimping lots of cables. Its primary utility is to do the actual 'crimping' part of compressing/crimping the tiny gold pins in the RJ45 connector onto the ethernet cables. It also has blades that can be used to cut or strip wires.



8.2. Cable Stripper

Cable strippers are used to take off the protecting shielding around cables and expose the inner wires. You can also do the same thing with a simple blade or pair of scissors. The trickiest part about stripping cables is trying to avoid cutting the inner wires!



8.3. RJ45 Connectors

RJ45 connectors are required for crimping because they feature the 8 golden pins that get crimped onto the 8 wires of the ethernet cable. They are what get plugged into ethernet ports! They also feature a latch/clip that locks the ethernet cable into the port once it is plugged in.



8.4. RJ45 Boots

RJ45 boots can be optionally used to protect the RJ45 connector. It provides insulation and prevents the cable from being breaking easily. They have to be slipped onto the cable before you put on the RJ45 connectors though!



8.5. RJ45 Cable Tester

RJ45 cable testers allow you to guarantee that you did the job correctly! They have two pieces that separate from each other, and you plug each end of your crimped ethernet cable into the port on each piece. Then you turn it on and the cable tester will test the connection for all 8 pins. If there are any missing lights on any of the pins, it means that you messed up somewhere and have to restart!



9. What is Network Topology?

Network topology refers to the arrangement of different elements like nodes, links, and devices in a computer network. It defines how these components are connected and interact with each other. Understanding various types of network topologies helps in designing efficient and robust networks.

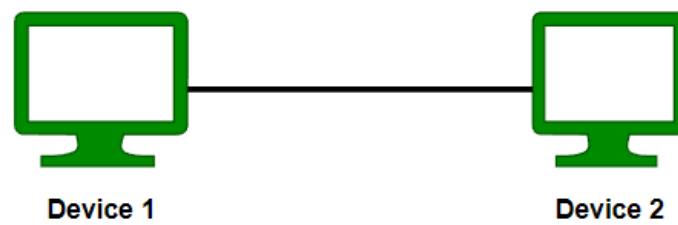
10. Different Types of Network Topology

The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as Network Topology. The various network topologies are:

10.1. Point to Point Topology

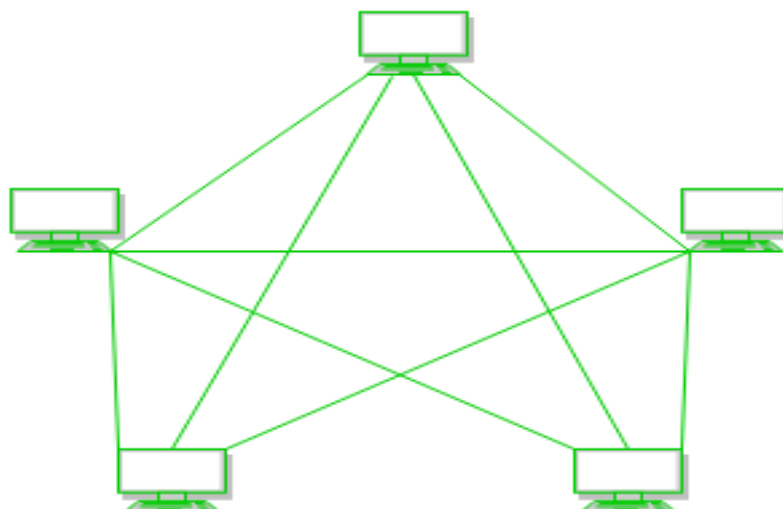
Point-to-point topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.

Point to Point Topology



10.2. Mesh Topology

In a mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.



- Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is $\frac{N(N-1)}{2}$ i.e. $\frac{N(N-1)}{2}$. In Figure 1, there are 5 devices connected to each other, hence the total number of links required is $\frac{5*4}{2} = 10$.

Advantages of Mesh Topology

- Communication is very fast between the nodes.
- Mesh Topology is robust.
- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

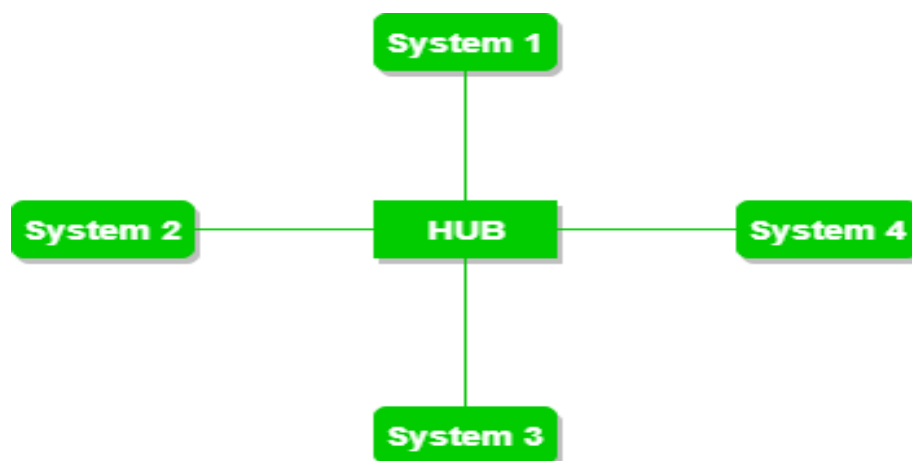
Disadvantages of Mesh Topology

- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

A common example of mesh topology is the internet backbone, where various internet service providers are connected to each other via dedicated channels. This topology is also used in military communication systems and aircraft navigation systems.

10.3. Star Topology

In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. Coaxial cables or RJ-45 cables are used to connect the computers. In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.



Advantages of Star Topology

- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.
- It is Robust. If one link fails only that link will affect and not other than that.
- Easy to fault identification and fault isolation.
- Star topology is cost-effective as it uses inexpensive coaxial cable.

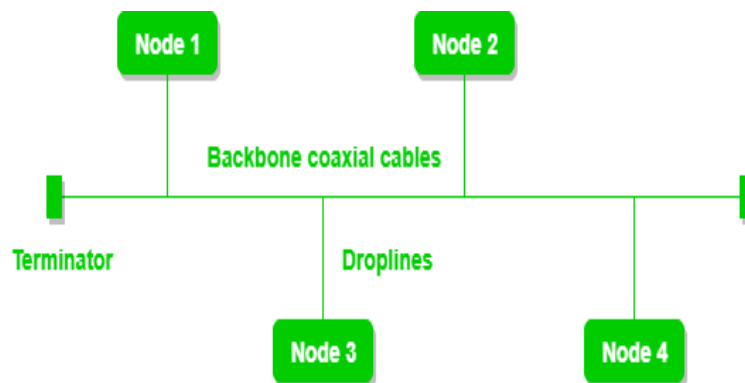
Disadvantages of Star Topology

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- The cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

A common example of star topology is a local area network (LAN) in an office where all computers are connected to a central hub. This topology is also used in wireless networks where all devices are connected to a wireless access point.

10.4. Bus Topology

Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.



Advantages of Bus Topology

- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, known as backbone cable, and N drop lines are required.
- Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.
- The cost of the cable is less compared to other topologies, but it is used to build small networks.
- Bus topology is familiar technology as installation and troubleshooting techniques are well known.
- CSMA is the most common method for this type of topology.

Disadvantages of Bus Topology

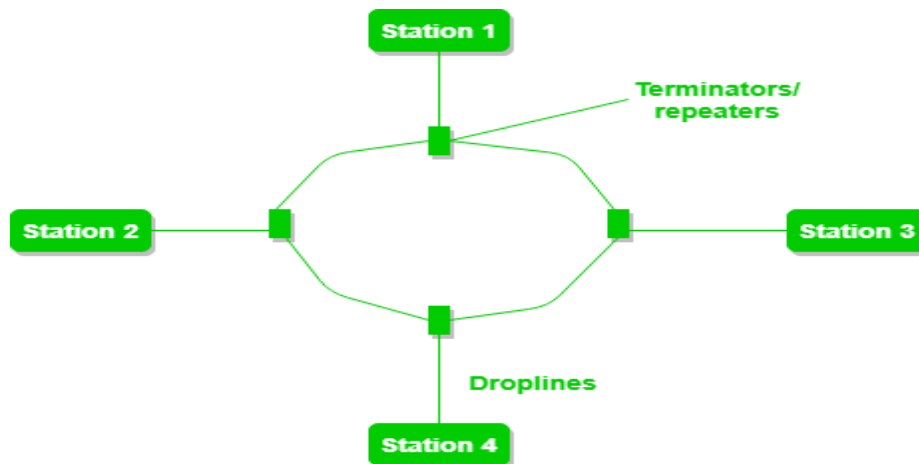
- A bus topology is quite simpler, but still, it requires a lot of cabling.
- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.
- Adding new devices to the network would slow down networks.
- Security is very low.

A common example of bus topology is the Ethernet LAN, where all devices are connected to a single coaxial cable or twisted pair cable. This topology is also used in cable television networks. For more, refer to the Advantages and Disadvantages of Bus Topology.

10.5. Ring Topology

In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The data flows in one direction, i.e. it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.



The most common access method of ring topology is token passing.

- Token passing: It is a network access method in which a token is passed from one node to another node.
- Token: It is a frame that circulates around the network.

Operations of Ring Topology

1. One station is known as a monitor station which takes all the responsibility for performing the operations.
2. To transmit the data, the station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
3. When no station is transmitting the data, then the token will circulate in the ring.
4. There are two types of token release techniques: Early token release releases the token just after transmitting the data and Delayed token release releases the token after the acknowledgment is received from the receiver.

Advantages of Ring Topology

- The data transmission is high-speed.
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.
- It is less costly than a star topology.

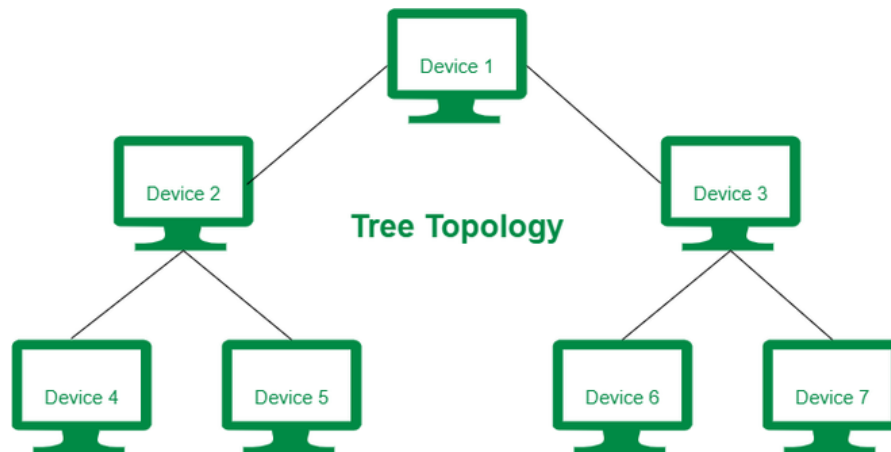
Disadvantages of Ring Topology

- The failure of a single node in the network can cause the entire network to fail.
- Troubleshooting is difficult in this topology.
- The addition of stations in between or the removal of stations can disturb the whole topology.

- Less secure.

10.6. Tree Topology

This topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, protocols like DHCP and SAC (Standard Automatic Configuration) are used.



Advantages of Tree Topology

- It allows more devices to be attached to a single central hub thus it decreases the distance that is traveled by the signal to come to the devices.
- It allows the network to get isolated and also prioritize from different computers.
- We can add new devices to the existing network.
- Error detection and error correction are very easy in a tree topology.

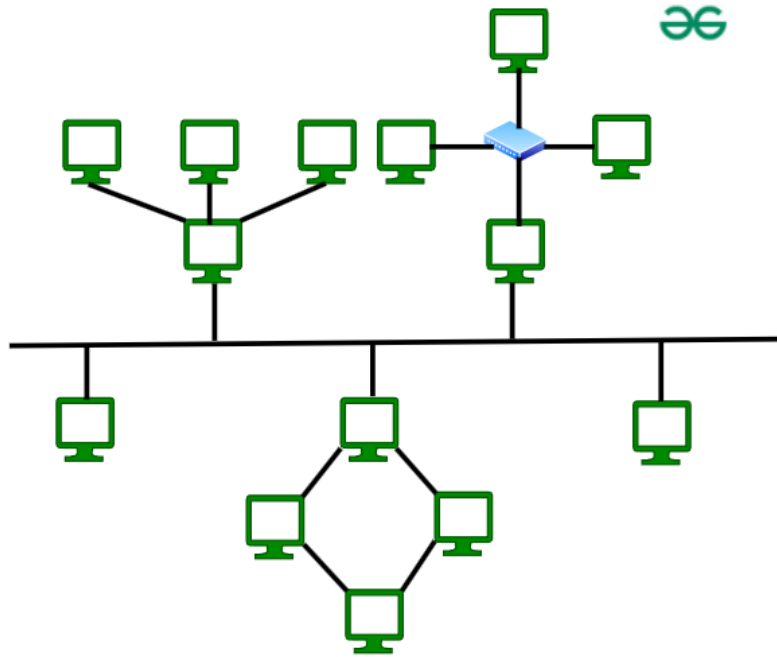
Disadvantages of Tree Topology

- If the central hub gets fails the entire system fails.
- The cost is high because of the cabling.
- If new devices are added, it becomes difficult to reconfigure.

A common example of a tree topology is the hierarchy in a large organization. At the top of the tree is the CEO, who is connected to the different departments or divisions (child nodes) of the company. Each department has its own hierarchy, with managers overseeing different teams (grandchild nodes). The team members (leaf nodes) are at the bottom of the hierarchy, connected to their respective managers and departments.

10.7. Hybrid Topology

This topological technology is the combination of all the various types of topologies we have studied above. Hybrid Topology is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above. Each individual topology uses the protocol that has been discussed earlier.



Advantages of Hybrid Topology

- This topology is very flexible.
- The size of the network can be easily expanded by adding new devices.

Disadvantages of Hybrid Topology

- It is challenging to design the architecture of the Hybrid Network.
- Hubs used in this topology are very expensive.
- The infrastructure cost is very high as a hybrid network requires a lot of cabling and network devices.

A common example of a hybrid topology is a university campus network. The network may have a backbone of a star topology, with each building connected to the backbone through a switch or router. Within each building, there may be a bus or ring topology connecting the different rooms and offices. The wireless access points also create a mesh topology for wireless devices. This hybrid topology allows for efficient communication between different buildings while providing flexibility and redundancy within each building.