Computer Networking

**1. Basic of Computer Networking**

-------------------------------------------------------------------------------------------------------

Computer Networking is the practice of connecting computers together to enable communication and data exchange between them.

In general, Computer Network is a collection of two or more computers. It helps users to communicate more easily.

**How Does a Computer Network Work?**

Basics building blocks of a Computer network are Nodes and Links. A Network Node can be illustrated as Equipment for Data Communication like a Modem, Router, etc., or Equipment of a Data Terminal like connecting two computers or more. Link in Computer Networks can be defined as wires or cables or free space of wireless networks.

The working of Computer Networks can be simply defined as rules or protocols which help in sending and receiving data via the links which allow Computer networks to communicate. Each device has an **IP Address**, that helps in identifying a device.

## Basic Terminologies of Computer Networks

* **Network:**A network is a collection of computers and devices that are connected together to enable communication and data exchange.
* **Nodes:**Nodes are devices that are connected to a network. These can include computers, Servers, Printers, [Routers,](https://www.geeksforgeeks.org/introduction-of-a-router/) [Switches](https://www.geeksforgeeks.org/types-of-switches-in-computer-network/), and other devices.
* **Protocol:**A protocol is a set of rules and standards that govern how data is transmitted over a network. Examples of protocols include [TCP/IP](https://www.geeksforgeeks.org/tcp-ip-model/), [HTTP](https://www.geeksforgeeks.org/http-full-form/), and [FTP](https://www.geeksforgeeks.org/file-transfer-protocol-ftp-in-application-layer/).
* **Topology:** Network topology refers to the physical and logical arrangement of nodes on a network. The common network topologies include **bus, star, ring, mesh, and tree**.
* **Service Provider Networks:**These types of Networks give permission to take Network Capacity and Functionality on lease from the Provider. Service Provider Networks include Wireless Communications, Data Carriers, etc.
* **IP Address**: An IP address is a unique numerical identifier that is assigned to every device on a network. IP addresses are used to identify devices and enable communication between them.
* **DNS:**The [Domain Name System (DNS)](https://www.geeksforgeeks.org/domain-name-system-dns-in-application-layer/) is a protocol that is used to translate human-readable domain names (such as www.google.com) into IP addresses that computers can understand.
* **Firewall:**A [firewall](https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/) is a security device that is used to monitor and control incoming and outgoing network traffic. Firewalls are used to protect networks from unauthorized access and other security threats.

## Types of Enterprise Computer Networks

* **LAN:**A [Local Area Network (LAN)](https://www.geeksforgeeks.org/types-of-area-networks-lan-man-and-wan/)is a network that covers a small area, such as an office or a home. LANs are typically used to connect computers and other devices within a building or a campus.
* **WAN:**A [Wide Area Network (WAN)](https://www.geeksforgeeks.org/wan-full-form/) is a network that covers a large geographic area, such as a city, country, or even the entire world. WANs are used to connect LANs together and are typically used for long-distance communication.
* **Cloud Networks:**[Cloud Networks](https://www.geeksforgeeks.org/cloud-networking/) can be visualized with a Wide Area Network (WAN) as they can be hosted on public or private cloud service providers and cloud networks are available if there is a demand. Cloud Networks consist of Virtual Routers, Firewalls, etc.
* **Open system:** A system that is connected to the network and is ready for communication.
* **Closed system:** A system that is not connected to the network and can’t be communicated with.

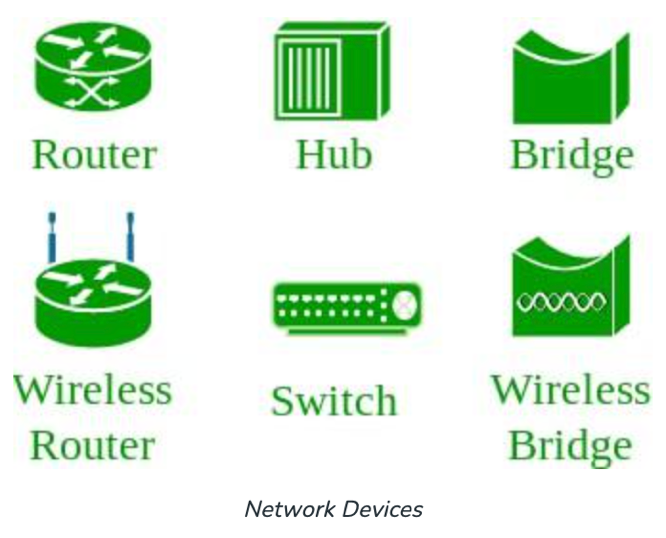
## Types of Computer Network Architecture

Computer Network falls under these broad Categories:

* **Client-Server Architecture:** [Client-Server Architecture](https://www.geeksforgeeks.org/client-server-model/) is a type of Computer Network Architecture in which Nodes can be Servers or Clients. Here, the server node can manage the Client Node Behaviour.
* **Peer-to-Peer Architecture:**In [P2P (Peer-to-Peer) Architecture](https://www.geeksforgeeks.org/what-is-p2ppeer-to-peer-process/), there is not any concept of a Central Server. Each device is free for working as either client or server.

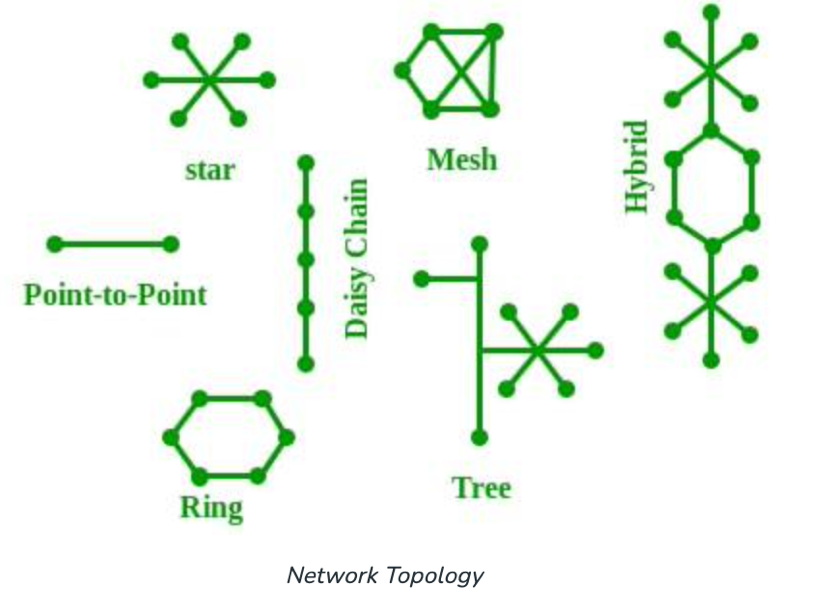
## Network Devices

An interconnection of multiple devices, also known as **hosts**, that are connected using multiple paths for the purpose of sending/receiving data or media. Computer networks can also include multiple devices/mediums which help in the communication between two different devices; these are known as [Network devices](https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/) and include things such as routers, switches, hubs, and bridges.



## Network Topology

The [Network Topology](https://www.geeksforgeeks.org/types-of-network-topology/) is the layout arrangement of the different devices in a network. Common examples include Bus, Star, Mesh, Ring, and Daisy chain.



**OSI Model**

OSI stands for [Open Systems Interconnection](https://www.geeksforgeeks.org/layers-of-osi-model/). It is a reference model that specifies standards for communications protocols and also the functionalities of each layer. The OSI has been developed by the International Organization For Standardization and it is 7 layer architecture. Each layer of OSI has different functions and each layer has to follow different protocols. The 7 layers are as follows:

* [Physical Layer](https://www.geeksforgeeks.org/physical-layer-in-osi-model/)
* [Data link Layer](https://www.geeksforgeeks.org/data-link-layer/)
* [Network Layer](https://www.geeksforgeeks.org/network-layer-services-packetizing-routing-and-forwarding/)
* [Transport Layer](https://www.geeksforgeeks.org/transport-layer-responsibilities/)
* [Session Layer](https://www.geeksforgeeks.org/session-layer-in-osi-model/)
* [Presentation Layer](https://www.geeksforgeeks.org/presentation-layer-in-osi-model/)
* [Application Layer](https://www.geeksforgeeks.org/application-layer-in-osi-model/)

**Protocol**

A protocol is a set of rules or algorithms which define the way how two entities can communicate across the network and there exists a different protocol defined at each layer of the OSI model. A few such protocols are TCP, IP, UDP, ARP, DHCP, FTP, and so on.

## Unique Identifiers of Network

**Hostname:**Each device in the network is associated with a unique device name known as Hostname. (Type “hostname” in terminal for displaying the hostname of your machine).

**IP Address (Internet Protocol address):**  Also known as the Logical Address, the IP Address is the network address of the system across the network. To identify each device in the world-wide-web, the Internet Assigned Numbers Authority (IANA) assigns an IPV4 (Version 4) address as a unique identifier to each device on the Internet. The length of an IPv4 address is 32 bits, hence, we have 232 IP addresses available. The length of an IPv6 address is 128 bits. Type “ipconfig” in the command prompt and press ‘Enter’, this gives us the IP address of the device.

**MAC Address (Media Access Control address):**Also known as physical address, the[MAC Address](https://www.geeksforgeeks.org/introduction-of-mac-address-in-computer-network/) is the unique identifier of each host and is associated with its [NIC (Network Interface Card)](https://www.geeksforgeeks.org/nic-full-form/). A MAC address is assigned to the NIC at the time of manufacturing. The length of the MAC address is: 12-nibble/ 6 bytes/ 48 bits Type “ipconfig/all” in the command prompt and press ‘Enter’, this gives us the MAC address.

**Port:**A port can be referred to as a logical channel through which data can be sent/received to an application. Any host may have multiple applications running, and each of these applications is identified using the port number on which they are running.

**Socket:** The unique combination of IP address and Port number together is termed a Socket.

**Other Related Concepts**

**DNS Server:** [DNS](https://www.geeksforgeeks.org/domain-name-system-dns-in-application-layer/) stands for **Domain Name System**. DNS is basically a server that translates web addresses or URLs (ex: www.google.com) into their corresponding IP addresses. We don’t have to remember all the IP addresses of each and every website. The command ‘**nslookup**’ gives you the IP address of the domain you are looking for. This also provides information on our DNS Server.

**ARP:** [ARP](https://www.geeksforgeeks.org/how-address-resolution-protocol-arp-works/) stands for **Address Resolution Protocol**. It is used to convert an IP address to its corresponding physical address(i.e., MAC Address). ARP is used by the Data Link Layer to identify the MAC address of the Receiver’s machine.

**RARP:** [RARP](https://www.geeksforgeeks.org/what-is-rarp/) stands for **Reverse Address Resolution Protocol**. As the name suggests, it provides the IP address of the device given a physical address as input. But RARP has become obsolete since the time DHCP has come into the picture.

**2. Goals of Networks**

-------------------------------------------------------------------------------------------------------

Computer Network means an interconnection of autonomous (standalone) computers for information exchange. The connecting media could be a copper wire, optical fiber, microwave, or satellite.

**Networking Elements –** The computer network includes the following networking elements:

1. At least two computers
2. Transmission medium either wired or wireless
3. Protocols or rules that govern the communication
4. Network software such as Network Operating System

**Network Criteria:**

The criteria that have to be met by a computer network are:

**1. Performance –** It is measured in terms of transit time and response time

* Transit time is the time for a message to travel from one device to another
* Response time is the elapsed time between an inquiry and a response.

Performance is dependent on the following factors:

* The number of users
* Type of transmission medium
* Capability of connected network
* Efficiency of software
* Bandwidth
* Network topology
* Network protocols
* Distance
* Network congestion
* Network hardware

**2. Reliability –** It is measured in terms of

* Frequency of failure
* Recovery from failures
* Robustness during catastrophe
* Quality of service (QoS)
* Reducing single points of failure
* Capacity planning
* Network architecture

**3. Security –** It means protecting data from unauthorized access.

**4. Network topology -**it is another crucial factor to consider when designing a computer network. It refers to the way in which computers, devices, and links are arranged in a network. Common topologies include **bus, star, ring, mesh, and hybrid**, each with its own advantages and disadvantages in terms of cost, scalability, reliability, and performance. The choice of topology depends on the specific needs and constraints of the network. Other important criteria that must be met by a computer network include performance, reliability, and security.

**Goals of Computer Networks:** The following are some important goals of computer networks:

1. **Resource Sharing –** Many organization has a substantial number of computers in operations, which are located apart. Ex. A group of office workers can share a common printer, fax, modem, scanner, etc.
2. **High Reliability –** If there are alternate sources of supply, all files could be replicated on two or more machines. If one of them is not available, due to hardware failure, the other copies could be used.
3. **Inter-process Communication –** Network users, located geographically apart, may converse in an interactive session through the network. In order to permit this, the network must provide almost error-free communications.
4. **Flexible access –** Files can be accessed from any computer in the network. The project can be begun on one computer and finished on another.
5. **Security** – Computer networks must be secure to protect against unauthorized access, data breaches, and other security threats. This includes implementing measures such as firewalls, antivirus software, and encryption to ensure the confidentiality, integrity, and availability of data.
6. **Performance**– Computer networks must provide high performance and low latency to ensure that applications and services are responsive and available when needed. This requires optimizing network infrastructure, bandwidth utilization, and traffic management.
7. **Scalability-** Computer networks must be designed to scale up or down as needed to accommodate changes in the number of users, devices, and data traffic. This requires careful planning and management to ensure the network can meet current and future needs.

Other goals include Distribution of processing functions, Centralized management, and allocation of network resources, Compatibility of dissimilar equipment and software, Good network performance, Scalability, Saving money, Access to remote information, Person to person communication, etc.

# **3. 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:

## 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.



**Figure 1**: Every device is connected to another via dedicated channels.

These channels are known as links. 

* Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. The total number of ports required=N\*(N-1).
* 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 NC2 i.e. N(N-1)/2. In Figure 1, there are 5 devices connected to each other, hence the total number of links required is 5\*4/2 = 10.

**Advantages of this topology:**

* Communication is very fast between the nodes.
* It 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.

**Problems with this 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.

**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.



**Figure 2**: A star topology having four systems connected to a single point of connection

**Advantages of this 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.

**Problems with this 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.

**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.



**Figure 3**: A bus topology with shared backbone cable.

The nodes are connected to the channel via drop lines.

**Advantages of this 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.

**Problems with this 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.

## Ring Topology:

In this 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.



**Figure 4**: A ring topology comprises 4 stations connected with each forming a ring.

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.

The following operations take place in ring topology are :

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 this topology:**

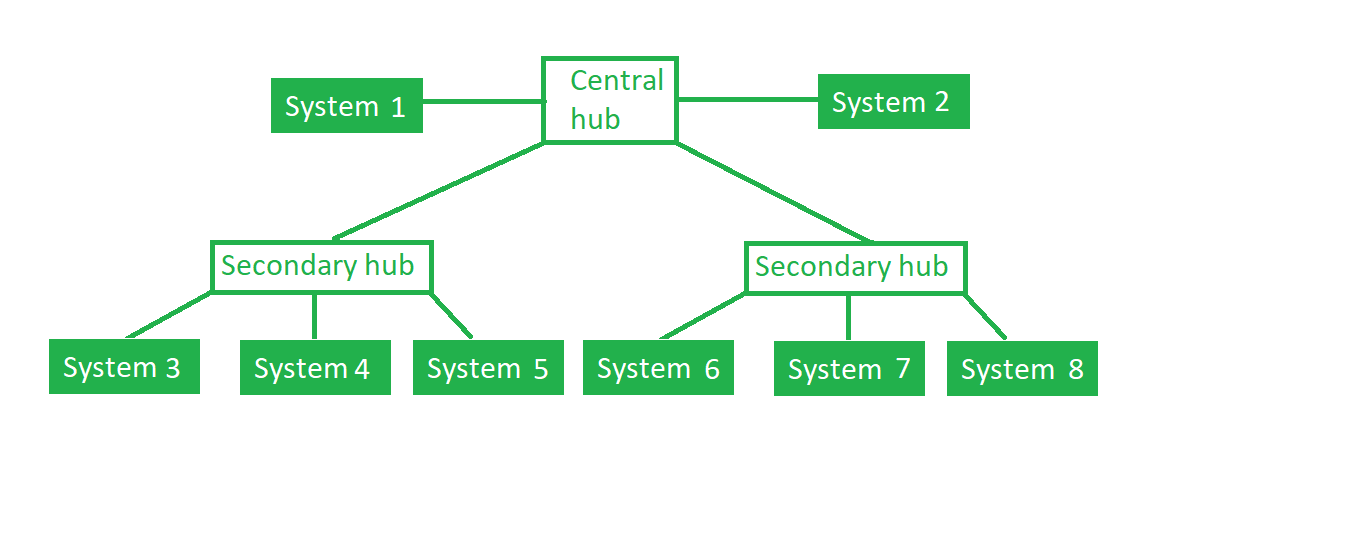
* The data transmission is high-speed.
* The possibility of collision is minimum in this type of topology.
* Cheap to install and expand.
* It is less costly than a star topology.

**Problems with this 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.

**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.



**Figure 5**: In this, the various secondary hubs are connected to the central hub which contains the repeater. This data flow from top to bottom i.e. from the central hub to the secondary and then to the devices or from bottom to top i.e. devices to the secondary hub and then to the central hub. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

**Advantages of this 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.

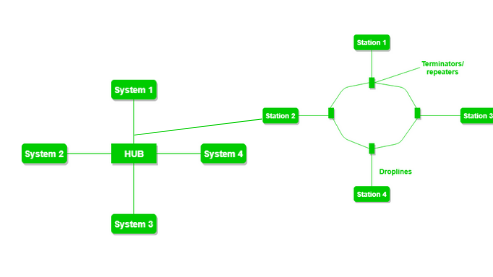
**Problems with this topology :**

* 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.

**Hybrid Topology:**

This topological technology is the combination of all the various types of topologies we have studied above. It 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.



**Figure 6**: The above figure shows the structure of the Hybrid topology. As seen it contains a combination of all different types of networks.

**Advantages of this topology :**

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

**Problems with this 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.

# **3. Types of Area Network – LAN, MAN and WAN**

-------------------------------------------------------------------------------------------------------

The **Network** allows computers to **connect and communicate** with different computers via any medium. LAN, MAN, and WAN are the three major types of networks designed to operate over the area they cover. There are some similarities and dissimilarities between them. One of the major differences is the geographical area they cover, i.e. **LAN** covers the smallest area, **MAN** covers an area larger than LAN and **WAN** comprises the largest of all.   
There are other types of Computer Networks also, like : 

* PAN (Personal Area Network)
* SAN (Storage Area Network)
* EPN (Enterprise Private Network)
* VPN (Virtual Private Network)

**Personal Area Network (PAN)**

PAN is a personal area network having an interconnection of personal technology devices to communicate over a short distance. It covers only less than 10 meters or 33 feet of area. PAN has fewer users as compared to other networks such as LAN, WAN, etc. PAN typically uses some form of wireless technology. PAN involves the transmission of data between information devices such as smartphones, personal computers, tablet computers, etc.

**Advantages:**

* Allows for easy communication between personal devices in close proximity.
* Can be set up easily and quickly.
* Uses wireless technology, which eliminates the need for wires and cables.
* PANs are designed to be energy efficient, which means that devices can communicate with each other without draining their batteries quickly.
* PANs are typically secured using encryption and authentication protocols, which helps to prevent unauthorized access to data and resources.

**Disadvantages:**

* Limited coverage area.
* May not be suitable for large-scale data transfer or communication.PANs typically have limited bandwidth, which means that they may not be able to handle large amounts of data or high-speed communication.
* May experience interference from other wireless devices.

**Local Area Network (LAN)**

LAN or Local Area Network connects network devices in such a way that personal computers and workstations can share data, tools, and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol. Private addresses are unique in relation to other computers on the local network. Routers are found at the boundary of a LAN, connecting them to the larger WAN.

Data transmits at a very fast rate as the number of computers linked is limited. By definition, the connections must be high-speed and relatively inexpensive hardware (Such as hubs, network adapters, and Ethernet cables). LANs cover a smaller geographical area (Size is limited to a few kilometres) and are privately owned. One can use it for an office building, home, hospital, school, etc. LAN is easy to design and maintain. A Communication medium used for LAN has twisted-pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized.

Early LANs had data rates in the 4 to 16 Mbps range. Today, speeds are normally 100 or 1000 Mbps. Propagation delay is very short in a LAN. The smallest LAN may only use two computers, while larger LANs can accommodate thousands of computers. LAN has a range up to 2km. A LAN typically relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN. The fault tolerance of a LAN is more and there is less congestion in this network. For example A bunch of students playing Counter-Strike in the same room (without internet).

**Advantages:**

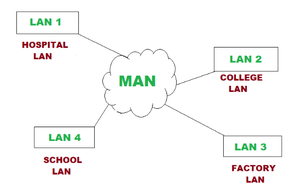
* Provides fast data transfer rates and high-speed communication.
* Easy to set up and manage.
* Can be used to share peripheral devices such as printers and scanners.
* Provides increased security and fault tolerance compared to WANs.

**Disadvantages:**

* Limited geographical coverage.
* Limited scalability and may require significant infrastructure upgrades to accommodate growth.
* May experience congestion and network performance issues with increased usage.

**Metropolitan Area Network (MAN)**

MAN or Metropolitan area Network covers a larger area than that covered by a LAN and a smaller area as compared to WAN. MAN has a range of 5-50km. It connects two or more computers that are apart but reside in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need high-speed connectivity. Speeds of MAN range in terms of Mbps. It’s hard to design and maintain a Metropolitan Area Network.



The fault tolerance of a MAN is less and also there is more congestion in the network. It is costly and may or may not be owned by a single organization. The data transfer rate and the propagation delay of MAN are moderate. Devices used for transmission of data through MAN are Modem and Wire/Cable. Examples of a MAN are part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network in a city.

**Advantages:**

* Provides high-speed connectivity over a larger geographical area than LAN.
* Can be used as an ISP for multiple customers.
* Offers higher data transfer rates than WAN in some cases.

**Disadvantages:**

* Can be expensive to set up and maintain.
* May experience congestion and network performance issues with increased usage.
* May have limited fault tolerance and security compared to LANs

**Wide Area Network (WAN) –**

WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. WAN has a range of above 50 km. A WAN could be a connection of LAN connecting to other LANs via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high-speed and relatively expensive.

There are two types of WAN: Switched WAN and Point-to-Point WAN. WAN is difficult to design and maintain. Similar to a MAN, the fault tolerance of a WAN is less and there is more congestion in the network. A Communication medium used for WAN is PSTN or Satellite Link. Due to long-distance transmission, the noise and error tend to be more in WAN.

WAN’s data rate is slow about a 10th LAN’s speed since it involves increased distance and increased number of servers and terminals etc. The speed of WAN ranges from a few kilobits per second (Kbps) to megabits per second (Mbps). Propagation delay is one of the biggest problems faced here. Devices used for the transmission of data through WAN are Optic wires, Microwaves, and Satellites. An example of a Switched WAN is the asynchronous transfer mode (ATM) network and Point-to-Point WAN is a dial-up line that connects a home computer to the Internet.

**Advantages:**

* Covers large geographical areas and can connect remote locations.
* Provides connectivity to the internet.
* Offers remote access to resources and applications.
* Can be used to support multiple users and applications simultaneously.

**Disadvantages:**

* Can be expensive to set up and maintain.
* Offers slower data transfer rates than LAN or MAN.
* May experience higher latency and longer propagation delays due to longer distances and multiple network hops.
* May have lower fault tolerance and security compared to LANs.

***Conclusion –***

*There are many advantages of LAN over MAN and WAN, such as LAN provide excellent reliability, a high data transmission rate, and can easily be managed and shares peripheral devices too. Local Area Network cannot cover cities or towns and for that Metropolitan Area Network is needed, which can connect a city or a group of cities together. Further, for connecting a Country or a group of Countries one requires a Wide Area Network.*