**Echelon Institute of Technology**

**(Affiliated to JC Bose University of Science and Technology, YMCA, Faridabad)**

**( Department of Computer Application )**

**UNIT:1**

**Computer Networking**

A computer network is a system that connects numerous independent computers in order to share information (data) and resources. The integration of computers and other different devices allows users to communicate more easily.A computer network is a collection of two or more computer systems that are linked together. A network connection can be established using either cable or wireless media. Hardware and software are used to connect computers and tools in any network.

A computer network consists of various kinds of nodes. Servers, networking hardware, personal computers, and other specialized or general-purpose hosts can all be nodes in a computer network. Host names and network addresses are used to identify them.

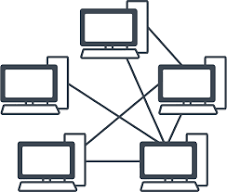
**Diagram of Computer Network**



**How Does a Computer Network Work?**

[Computer Networks](https://www.geeksforgeeks.org/basics-computer-networking/) simply work using nodes and links. Data communication equipment is simply termed as Nodes. For example, Modems, Hubs, [Switches](https://www.geeksforgeeks.org/types-of-switches-in-computer-network/), etc. whereas links in Computer networks can be referred to as a connection between two nodes. We have several types of links like cable wires, [optical fibers](https://www.geeksforgeeks.org/fiber-optics-and-types/), etc.

Whenever a Computer Network is working, nodes have the work of sending and receiving data via the links. Computer Network provides some set of protocols that helps in following the rules and protocols.



## What Do Computer Networks Do?

Computer Networks are one of the important aspects of Computer Science. In the early days, it is used for data transmission on telephone lines and had a very limited use, but nowadays, it is used in a variety of places.

Computer Networks help in providing better connectivity that helps nowadays. Modern computer networks have the following functionality like

1. Computer Networks help in operating virtually.
2. Computer Networks integrate on a large scale.
3. Computer Networks respond very quickly in case of conditions change.
4. Computer Networks help in providing [data security](https://www.geeksforgeeks.org/data-security/).

## ****Criteria of a Good Network****

1. **Performance:**It can be measured in many ways, including transmit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of the network depends on a number of factors, including the number of users, the type of medium & Hardware
2. **Reliability:**In addition to accuracy is measured by frequency of failure, the time it takes a link to recover from failure, and the network’s robustness in catastrophe.
3. **Security:** Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data loss.

## ****Goals of Computer Networking****

* Programs do not have to execute on a single system because of resource and load sharing.
* Reduced costs – Multiple machines can share printers, tape drives, and other peripherals.
* Reliability – If one machine fails, another can take its place.
* Scalability (it’s simple to add more processors or computers)
* Communication and mail (people living apart can work together)
* Information Access (remote information access, access to the internet, e-mail, video conferencing, and online shopping)
* Entertainment that is interactive (online games, videos, etc.)
* Social Networking

## Types of Computer Networks

### ****Division Based on the Communication Medium****

* **Wired Network:**As we all know, “wired” refers to any physical medium made up of cables. Copper wire, twisted pair, or fiber optic cables are all options. A wired network employs wires to link devices to the Internet or another network, such as laptops or desktop PCs.
* **Wireless Network:**“Wireless” means without wire, media that is made up of electromagnetic waves (EM Waves) or infrared waves. Antennas or sensors will be present on all wireless devices. Cellular phones, wireless sensors, TV remotes, satellite dish receivers, and laptops with WLAN cards are all examples of wireless devices. For data or voice communication, a wireless network uses radio frequency waves rather than wires.

### ****Division Based on Area Covered****

* **Local Area Network (LAN):** A [LAN](https://www.geeksforgeeks.org/lan-full-form/) is a network that covers an area of around 10 kilometers. For example, a college network or an office network. Depending upon the needs of the organization, a LAN can be a single office, building, or Campus. We can have two PCs and one printer in-home office or it can extend throughout the company and include audio and video devices. Each host in LAN has an identifier, an address that defines hosts in LAN. A packet sent by the host to another host carries both the source host’s and the destination host’s address.
* **Metropolitan Area Network (MAN):**[MAN](https://www.geeksforgeeks.org/man-full-form-in-computer-networking/) refers to a network that covers an entire city. For example: consider the cable television network.
* **Wide Area Network (WAN):** [WAN](https://www.geeksforgeeks.org/wan-full-form/) refers to a network that connects countries or continents. For example, the Internet allows users to access a distributed system called www from anywhere around the globe.WAN interconnects connecting devices such as switches, routers, or modems. A LAN is normally privately owned by an organization that uses it. We see two distinct examples of WANs today: point-to-point WANs and Switched WANs
  + **Point To Point**: Connects two connecting devices through transmission media.
  + **Switched:** A switched WAN is a network with more than two ends.

### ****Based on Types of Communication****

* **Point To Point networks:** Point-to-Point networking is a type of data networking that establishes a direct link between two networking nodes.  
  A direct link between two devices, such as a computer and a printer, is known as a point-to-point connection.
* **Multipoint**: is the one in which more than two specific devices share links. In the multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection.
* **Broadcast networks:**In broadcast networks, a signal method in which numerous parties can hear a single sender. Radio stations are an excellent illustration of the “Broadcast Network” in everyday life. The radio station is a sender of data/signal in this scenario, and data is only intended to travel in one direction. Away from the radio transmission tower, to be precise.

### ****Based on the Type of Architecture****

* **P2P Networks:**Computers with similar capabilities and configurations are referred to as peers.  
  “Peer to Peer” is the abbreviation for “peer to peer.” The “peers” in a peer-to-peer network are computer systems that are connected to each other over the Internet. Without the use of a central server, files can be shared directly between systems on the network.
* **Client-Server Networks:**Each computer or process on the network is either a client or a server in a client-server architecture (client/server). The client asks for services from the server, which the server provides. Servers are high-performance computers or processes that manage disc drives (file servers), printers (print servers), or network traffic (network servers)
* **Hybrid Networks:**The hybrid model refers to a network that uses a combination of client-server and peer-to-peer architecture. Eg: Torrent.

## Types of Computer Network Architecture

Computer Network Architecture is of two types. These types are mentioned below.

**1. Client-Server Architecture:**[Client-Server Architecture](https://www.geeksforgeeks.org/client-server-model/) is basically the architecture where the clients and the server are connected as two clients can communicate with each other and the devices present work as servers in the network.

**2. Peer-to-Peer Architecture:**[Peer-to-Peer Architecture](https://www.geeksforgeeks.org/what-is-p2ppeer-to-peer-process/), computers are connected to each other and each computer is equally capable of working as there is no central server here. Each device present here can be used as a client or server.

## Types of Enterprise Computer Networks

There are three main types of Enterprise Computer Networks which are mentioned below.

**1. Local Area Network (LAN):**[Local Area Networks](https://www.geeksforgeeks.org/types-of-area-networks-lan-man-and-wan/) are small-scale networks used in small companies or as test networks. It has a limited size.

**2. Wide Area Networks (WAN):**[Wide Area Networks](https://www.geeksforgeeks.org/difference-between-lan-and-wan/) are networks that are used for a larger area than local area networks and are used for long-distance communication.

**3. Service Provider Networks:**Service Provider Networks are the networks that help in wireless communication, high-speed internet access, etc.

## Network Topology

### ****Bus Topology****

Every computer and network device is connected to a single cable in a [bus topology](https://www.geeksforgeeks.org/types-of-network-topology/) network. Linear Bus topology is defined as having exactly two terminals.

**Advantages**

* Installation is simple.
* Compared to mesh, star, and tree topologies, the bus utilizes less cabling.

**Disadvantages**

* Difficulty in reconfiguring and isolating faults.
* A bus cable malfunction or break interrupts all communication.

For more, you can refer to the [Advantages and Disadvantages of Bus Topology.](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-bus-topology/)

Bus Topology

### ****Ring Topology****

The topology is named ring topology because one computer is connected to another, with the final one being connected to the first. Exactly two neighbors for each device. A signal is passed along the ring in one direction. Each ring incorporates a repeater.

**Advantages**

* Data transmission is relatively straightforward because packets only move in one direction.
* There is no requirement for a central controller to manage communication between nodes.
* Easy installation & Reconfiguration
* Simplified Faulty connections

**Disadvantages**

* In a Unidirectional Ring, a data packet must traverse through all nodes.
* All computers must be turned on in order for them to connect with one another.

For more, you can refer to the [Advantages and Disadvantages of Ring Topology.](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-ring-topology/)

Ring Topology

### ****Star Topology****

Each device in a star topology has a dedicated point-to-point link to a central controller, which is commonly referred to as the HUB. There is no direct connection between the devices. Traffic between the devices is not allowed in this topology. As an exchange, the controller is used.

**Advantages**

* When attaching or disconnecting devices, there are no network interruptions.
* It’s simple to set up and configure.
* Identifying and isolating faults is simple.
* Less Expensive than mesh
* Easy to install & configure

**Disadvantages**

* Nodes attached to the hub, switch, or concentrator is failed if they fail.
* Because of the expense of the hubs, it is more expensive than linear bus topologies.
* More cable is required compared to a bus or ring
* Too much dependency on Hub

For more, you can refer to the[Advantages and Disadvantages of Star Topology](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-star-topology/).

**Example:** Used in high-speed LANs

Star Topology

### ****Mesh Topology****

Every device in a mesh topology has dedicated point-to-point connectivity to every other device. The term “dedicated” refers to the fact that the link exclusively transports data between the two devices it links. To connect n devices, a fully connected mesh network contains n \*(n-1)/2 physical channels.

**Advantages**

* Data can be sent from multiple devices at the same time. This topology can handle a lot of traffic.
* Even if one of the connections fails, a backup is always available. As a result, data transit is unaffected.
* Physical boundaries prevent other users from gaining access to messages
* Point to Point links make fault transmission & fault isolation easy

**Disadvantages**

* The amount of cabling and the number of I/O ports that are necessary.
* The sheer bulk of wiring can be greater than the available space can accommodate.
* It is difficult to install and reconfigure.

For more, you can refer to the [Advantages and Disadvantages of Mesh Topology](https://www.geeksforgeeks.org/advantage-and-disadvantage-of-mesh-topology/).

**Example:**  connection of telephone regional office in which each regional office needs to be connected to every other regional office.

Mesh Topology

### ****Tree Topology****

The topology of a tree is similar to that of a star. Nodes in a tree, like those in a star, are connected to a central hub that manages network traffic. It has a root node, which is connected to all other nodes, producing a hierarchy. Hierarchical topology is another name for it. The number of Star networks is connected via Bus in Tree Topology.

**Advantages**

* Network expansion is both possible and simple.
* We partition the entire network into pieces (star networks) that are easier to manage and maintain.
* Other segments are unaffected if one segment is damaged.

**Disadvantages**

* Tree topology relies largely on the main bus cable because of its basic structure, and if it fails, the entire network is handicapped.
* Maintenance becomes more challenging when more nodes and segments are added.

For more, you can refer to the [Advantages and Disadvantages of Tree Topology](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-tree-topology/).

Tree Topology

## Networking Devices

Basic hardware interconnecting network nodes, such as Network Interface Cards (NICs), Bridges, Hubs, Switches, and Routers, are used in all networks. In addition, a mechanism for connecting these building parts is necessary, which is usually galvanic cable and optical cable are less popular (“optical fiber”)The following are the network devices :

* **NIC (Network Interface Card):**A network card, often known as a network adapter or [NIC](https://www.geeksforgeeks.org/nic-full-form/) (network interface card), is computer hardware that enables computers to communicate via a network. It offers physical access to networking media and, in many cases, MAC addresses serve as a low-level addressing scheme. Each network interface card has a distinct identifier. This is stored on a chip that is attached to the card.
* **Repeater:**A repeater is an electrical device that receives a signal, cleans it of unwanted noise, regenerates it, and retransmits it at a higher power level or to the opposite side of an obstruction, allowing the signal to travel greater distances without degradation. In the majority of twisted pair Ethernet networks, Repeaters are necessary for cable lengths longer than 100 meters in some systems. Repeaters are based on physics.
* **Hub:**A [hub](https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/) is a device that joins together many twisted pairs or fiber optic Ethernet devices to give the illusion of a formation of a single network segment. The device can be visualized as a multiport repeater. A network hub is a relatively simple broadcast device. Any packet entering any port is regenerated and broadcast out on all other ports, and hubs do not control any of the traffic that passes through them. Packet collisions occur as a result of every packet being sent out through all other ports, substantially impeding the smooth flow of communication.
* **Bridges:**Bridges broadcast data to all the ports but not to the one that received the transmission. Bridges, on the other hand, learn which MAC addresses are reachable through specific ports rather than copying messages to all ports as hubs do. Once a port and an address are associated, the bridge will only transport traffic from that address to that port.
* **Switches:**A switch differs from a hub in that it only forwards frames to the ports that are participating in the communication, rather than all of the ports that are connected. The collision domain is broken by a switch, yet the switch depicts itself as a broadcast domain. Frame-forwarding decisions are made by switches based on MAC addresses.
* **Routers:**[Routers](https://www.geeksforgeeks.org/introduction-of-a-router/)are networking devices that use headers and forwarding tables to find the optimal way to forward data packets between networks. A router is a computer networking device that links two or more computer networks and selectively exchanges data packets between them. A router can use address information in each data packet to determine if the source and destination are on the same network or if the data packet has to be transported between networks. When numerous routers are deployed in a wide collection of interconnected networks, the routers share target system addresses so that each router can develop a table displaying the preferred pathways between any two systems on the associated networks.
* **Gateways:**To provide system compatibility, a gateway may contain devices such as protocol translators, impedance-matching devices, rate converters, fault isolators, or signal translators. It also necessitates the development of administrative procedures that are acceptable to both networks. By completing the necessary protocol conversions, a protocol translation/mapping gateway joins networks that use distinct network protocol technologies.

## Internet

Computers and their structures are tough to approach, and it is made even extra tough while you want to recognize phrases associated with the difficulty this is already utilized in regular English, Network, and the net will appear to be absolutely wonderful from one some other, however, they may seem like identical.

A **network**is a group of two or more computer systems (Multiple gadgets, additionally called hosts), which are related through a couple of channels for the motive of sending and receiving data (records/media) in a shared environment. The community also can consist of serval gadgets/mediums that resource communique among or extra machines; those gadgets are called Network devices and consist of routers, switches, hubs, and bridges, amongst others.

**Internet** is a group of computer systems connected from all around the world. The Internet protocol suite is a framework defined through the Internet standards. Methods are divided right into a layered set of protocols on this architecture. The Internet gives a huge variety of [statistics](https://www.geeksforgeeks.org/statistics/) and communique offerings, which includes forums, databases, email, and hypertext. It is made of the neighborhood to global personal, public networks connected through plenty of digital, wireless, and networking technologies.

**Working of** **the** **internet:**The internet is a global computer network that connects various devices and sends a lot of information and media. It uses an Internet Protocol (IP) and Transport Control Protocol (TCP)-based packet routing network. TCP and IP work together to ensure that data transmission across the internet is consistent and reliable, regardless of the device or location. Data is delivered across the internet in the form of messages and packets. A message is a piece of data delivered over the internet, but before it is sent, it is broken down into smaller pieces known as packets.

IP is a set of rules that control how data is transmitted from one computer to another via the internet. The IP system receives further instructions on how the data should be transferred using a numerical address (IP Address). The TCP is used with IP to ensure that data is transferred in a secure and reliable manner. This ensures that no packets are lost, that packets are reassembled in the correct order, and that there is no delay that degrades data quality.

**History of Internet**

Talking about the [**history of internet**](https://news.geeksforgeeks.org/knowledge/history-of-internet), the ARPANET (Advanced Research Projects Agency Network, later renamed the internet) established a successful link between the University of California Los Angeles and the Stanford Research Institute on October 29, 1969. Libraries automate and network catalogs outside of ARPANET in the late 1960s.

TCP/IP (Transmission Control Protocol and Internet Protocol) is established in the 1970s, allowing internet technology to mature. The development of these protocols aided in the standardization of how data was sent and received via the internet. NSFNET (National Science Foundation Network), the 56 Kbps backbone of the internet, was financed by the National Science Foundation in 1986. Because government monies were being used to administer and maintain it, there were commercial restrictions in place at the time.

In the year 1991, a user-friendly internet interface was developed. Delphi was the first national commercial online service to offer internet connectivity in July 1992. Later in May 1995, All restrictions on commercial usage of the internet are lifted. As a result, the internet has been able to diversify and grow swiftly. Wi-Fi was first introduced in 1997. The year is 1998, and Windows 98 is released. Smartphone use is widespread in 2007. The 4G network is launched in 2009. The internet is used by 3 billion people nowadays. By 2030, there are expected to be 7.5 billion internet users and 500 billion devices linked to the internet.

**Uses of the Internet:**

* **E-mail:**E-mail is an electronic message sent across a network from one computer user to one or more recipients. It refers to the internet services in which messages are sent from and received by servers.
* **Web Chat:**Web chat is an application that allows you to send and receive messages in real-time with others. By using Internet chat software, the user can log on to specific websites and talk with a variety of other users online. Chat software is interactive software that allows users to enter comments in one window and receive responses from others who are using the same software in another window.
* **World Wide Web:**The World Wide Web is the Internet’s most popular information exchange service. It provides users with access to a large number of documents that are linked together using hypertext or hyperlinks.
* **E-commerce:**E-commerce refers to electronic business transactions made over the Internet. It encompasses a wide range of product and service-related online business activities.
* **Internet telephony:**The technique that converts analog speech impulses into digital signals and routes them through packet-switched networks of the internet is known as internet telephony.
* **Video conferencing:**The term “video conferencing” refers to the use of voice and images to communicate amongst users.

**Web Client**

The client (or user) side of the Internet. The Web browser on the user’s computer or mobile device is referred to as a Web client. It could also apply to browser extensions and helper software that improve the browser’s ability to support specific site services.

**Web browser**

A web browser is a software program software that searches for, retrieves, and presentations material which includes Web pages, photos, videos, and different files. The browser sends a request to the Webserver, which then transmits the [statistics](https://www.geeksforgeeks.org/statistics/) returned to the browser, which presentations the findings at the laptop. Example – Mozilla Firefox, Microsoft Edge, Google Chrome, Safari etc.

**Webpage**

An internet web page (additionally called a web page) is a report that may be regarded in an internet browser at the World Wide Web. HTML (HyperText Markup Language) and CSS (Cascading Style Sheet) are used to generate the primary shape of an internet web page. An internet web page is generally a segment of an internet site that carries statistics in plenty of formats, which includes textual content inside the shape of paragraphs, lists, tables, and so on.

The home web page is the beginning or first web page of an internet site. It gives trendy [statistics](https://www.geeksforgeeks.org/statistics/) and connections to all the internet pages which are associated. Every internet web page has its personal deal with. This may be visible withinside the deal with the bar. As a result, if we need to get admission to a selected internet web page, the deal needs to be placed inside the browser’s deal with bar.

**Website**

An internet site, in trendy, is a group of [statistics](https://www.geeksforgeeks.org/statistics/) approximately statistics prepared into many internet pages. An internet site is probably made for a sure motive, subject matter, or to provide a service. An internet site (abbreviated as “website” or “site”) is a group of online pages connected collectively through links and saved on an internet server. By clicking on links, a tourist can pass from one web page to the next. An internet site’s pages also are connected below one area call and proportion a not unusual place subject matter and template.

**Search Engine**

Search engines are websites that search on the internet on behalf of users and show a listing of results. More than actually written may be discovered on seek engines. You can be capable of looking for different online content material which includes photographs, video content material, books, and news, in addition to gadgets and offerings, relying on the seek engine you are the use of.

To make use of the Internet, you do not always want to recognize the deal with an internet site. It is crucial to recognize the way to do a look for [statistics](https://www.geeksforgeeks.org/statistics/). Using a seek engine is one of the only methods to seek. A seek engine can help you in finding what you are looking for. You also can appearance up net maps and instructions to help you to plot your adventure from one factor to some other. Example: Google, Bing, DuckDuckGo, yahoo, etc.

**Web 1.0: The Beginning of the Internet**

Web 1.0, which emerged with the invention of the Internet, featured static web pages that could only be viewed. These early websites were essentially digital brochures, with limited interactivity and no ability for users to contribute content. This era saw the rise of early browsers such as Mosaic and Netscape Navigator, which made it easier for users to access the Web.

**Web 2.0: The Era of Social Media and User-Generated Content**

Web 2.0, which emerged during the “Internet Boom” era of the late 1990s and early 2000s, introduced more dynamic web pages and websites, and allowed for user-generated content. This era saw the rise of social media platforms such as Facebook, Twitter, and YouTube, as well as the introduction of blogs, wikis, and other forms of user-generated content.

**Web 3.0: The Future of the Internet**

Web 3.0, which is still in development, promises to bring a more personalized and intuitive experience for users. It is expected to be more intelligent and able to understand the context and intent of the user’s actions. This will be achieved through the integration of Artificial Intelligence (AI) and Machine Learning (ML) technologies.

Many experts in the tech industry claimed that Web 3.0 is the next evolution of the internet that is focused on decentralization, intelligence, and security. It aims to create a more personalized, intuitive, and inclusive experience for users by leveraging new technologies such as blockchain and artificial intelligence. The goal of Web 3.0 is to make the internet more democratic, open-source, and secure.

**Differentiation between Network and Internet**

The number one distinction between a network and the internet is that a network is made of computer systems that are bodily related and may be used as a personal laptop at the same time as additionally sharing records. The Internet, on the alternative hand, might be an era that connects those small and massive networks and creates a brand new in-intensity community.

**Advantages of the Internet:**

* It is the best source of a wide range of information. There is no better place to conduct research than the internet.
* Online gaming, talking, browsing, music, movies, dramas, and TV series are quickly becoming the most popular ways to pass the time.
* Because there are hundreds of thousands of newsgroups and services that keep you updated with every tick of the clock, the Internet is a source of the most recent news.
* Because of virtual shops where you may buy anything you want and need without leaving your house, internet shopping is becoming increasingly popular. Recently, virtual shops have been making a lot of money.
* With the emergence of online businesses, virtual stores, and credit card usage, purchasing goods without going to the store has never been easier.

**Disadvantages of the Internet:**

* Spending too much time on the internet is hazardous for the young generation’s physical and mental health.
* Children who use the internet develop an addiction, which is quite dangerous.
* It is now quite easy to decipher someone’s chat or email messages thanks to the hacking community.
* With the emergence of online stores, people prefer to order online rather than going to local stores which results in less social interactions among people.

# What is VPN & How It Works?

VPN stands for the **Virtual Private Network**. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the Internet. A Virtual Private Network is a way to extend a private network using a public network such as the Internet. The name only suggests that it is a “Virtual Private Network”, i.e. user can be part of a local network sitting at a remote location. It makes use of tunnelling protocols to establish a secure connection.

## How does a VPN work?

**Let us understand VPN with an example:** Think of a situation where the corporate office of a bank is situated in Washington, USA. This office has a local network consisting of say 100 computers. Suppose other branches of the bank are in Mumbai, India, and Tokyo, Japan. The traditional method of establishing a secure connection between the head office and the branch was to have a leased line between the branches and head office which was a very costly as well as troublesome job. VPN lets us effectively overcome this issue.

* All 100 hundred computers of the corporate office in Washington are connected to the VPN server(which is a well-configured server containing a public [IP address](https://www.geeksforgeeks.org/what-is-an-ip-address/)and a switch to connect all computers present in the local network i.e. in the US head office).
* The person sitting in the Mumbai office connects to The VPN server using a dial-up window and the VPN server returns an IP address that belongs to the series of IP addresses belonging to a local network of the corporate office.
* Thus person from the Mumbai branch becomes local to the head office and information can be shared securely over the public internet.
* So this is the intuitive way of extending the local network even across the geographical borders of the country.

**VPN is well exploited all across the globe**

We will explain to you with an example. Suppose we are using smartphones regularly. Spotify-a Swedish music app that is not active in India But we are making full use of it sitting in India. So how ?? VPN can be used to camouflage our geolocation.

* Suppose the IP address is 101.22.23.3 which belongs to India. That’s why our device is not able to access the Spotify music app.
* But the magic began when we used the Psiphon app which is an Android app used to change the device IP address to the IP address of the location we want(say US where Spotify works seamlessly).
* The IP address is changed using VPN technology. Basically what happens is that your device will connect to a VPN server of the respective country that you have entered in your location textbox of the Psiphon app and now you will inherit a new IP from this server.

**What is VPN used for?**

Do you need help determining when you should use a VPN? Let us shed some light on the subject and show you how the best VPNs can revolutionize your online activities.

* **For Unlimited Streaming:**Love streaming your favourite shows and sports games? A VPN is your ultimate companion for unlocking streaming services like Netflix or Hulu. Access all the content you desire and never miss a moment of your beloved NFL games.
* **For elevating your Gaming Experience:** Unleash your gaming potential with the added layer of security and convenience provided by a VPN. Defend yourself against vengeful competitors aiming to disrupt your gameplay while improving your ping for smoother, lag-free sessions. Additionally, gain access to exclusive games that may be restricted in your region, opening up a world of endless gaming possibilities.
* **For Anonymous Torrenting**: When it comes to downloading copyrighted content through torrenting, it’s essential to keep your IP address hidden. A VPN can mask your identity and avoid potential exposure, ensuring a safe and private torrenting experience.
* **For supercharging your Internet Speed:**Are you tired of your Internet speed slowing down when downloading large files? Your Internet Service Provider (ISP) might be intentionally throttling your bandwidth. Thankfully, a VPN can rescue you by keeping your online activities anonymous, effectively preventing ISP throttling. Say goodbye to sluggish connections and embrace blazing-fast speeds.
* **Securing Public Wi-Fi:**VPNs are essential for maintaining security when using public Wi-Fi networks, such as those in coffee shops, airports, or hotels. These networks are often vulnerable to cyberattacks, and using a VPN encrypts your internet connection, protecting your data from potential hackers and eavesdroppers when you connect to untrusted Wi-Fi hotspots.

**Are VPNs legal or illegal?**

Using a VPN  is legal in most countries, The legality of using a VPN service depends on the country and its geopolitical relations with another country as well. A reliable and secure VPN is always legal if you do not intend to use it for any illegal activities like committing fraud online, cyber theft, or in some countries downloading copyrighted content.

China has decided to block all VPNs (Virtual private network) by next year, as per the report of Bloomberg. Many Chinese Internet users use VPNs to privately access websites that are blocked under China’s so-called “great firewall”. This is done to avoid any information leakage to rival countries and to tighten the information security.

# Types of Computer Networks

A computer network is a cluster of computers over a shared communication path that works to share resources from one computer to another, provided by or located on the network nodes.

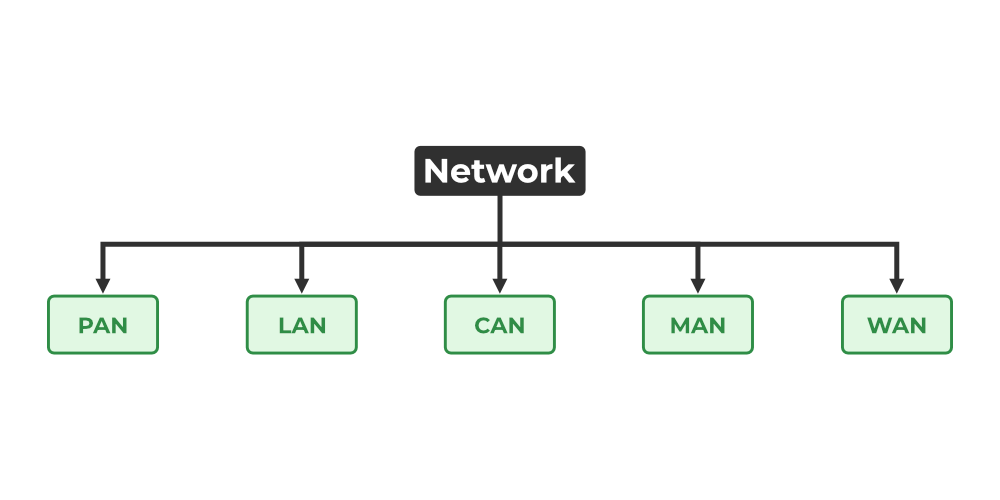
## Uses of Computer Networks

* Communicating using email, video, instant messaging, etc.
* Sharing devices such as printers, scanners, etc.
* Sharing files.
* Sharing software and operating programs on remote systems.
* Allowing network users to easily access and maintain information.

## Types of Computer Networks

There are mainly five types of Computer Networks

1. [Personal Area Network (PAN)](https://www.geeksforgeeks.org/overview-of-personal-area-network-pan/)
2. [Local Area Network (LAN)](https://www.geeksforgeeks.org/lan-full-form/)
3. [Campus Area Network (CAN)](https://www.geeksforgeeks.org/overview-of-campus-area-network-can/)
4. [Metropolitan Area Network (MAN)](https://www.geeksforgeeks.org/man-full-form-in-computer-networking/)
5. [Wide Area Network (WAN)](https://www.geeksforgeeks.org/wan-full-form/)



### ****1. Personal Area Network (PAN)****

[PAN](https://www.geeksforgeeks.org/overview-of-personal-area-network-pan/) is the most basic type of computer network. This network is restrained to a single person, that is, communication between the computer devices is centered only on an individual’s workspace. 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](https://www.geeksforgeeks.org/bluetooth/)**,**[IrDA](https://www.geeksforgeeks.org/irda-infrared-data-association/)**,**and [Zigbee](https://www.geeksforgeeks.org/introduction-of-zigbee/) as technology.

Examples of PAN are USB, computer, phone, tablet, printer, PDA, etc.

### Lightbox****2. Local Area Network (LAN)****

LAN is the most frequently used network. A [LAN](https://www.geeksforgeeks.org/lan-full-form/)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](https://www.geeksforgeeks.org/local-area-network-lan-technologies/)and [Wi-fi](https://www.geeksforgeeks.org/what-is-wi-fiwireless-fidelity/).  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.

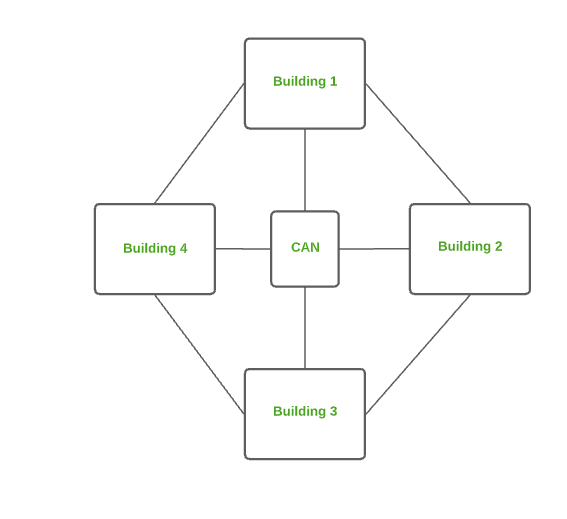
### Lightbox

### ****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](https://www.geeksforgeeks.org/overview-of-campus-area-network-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.

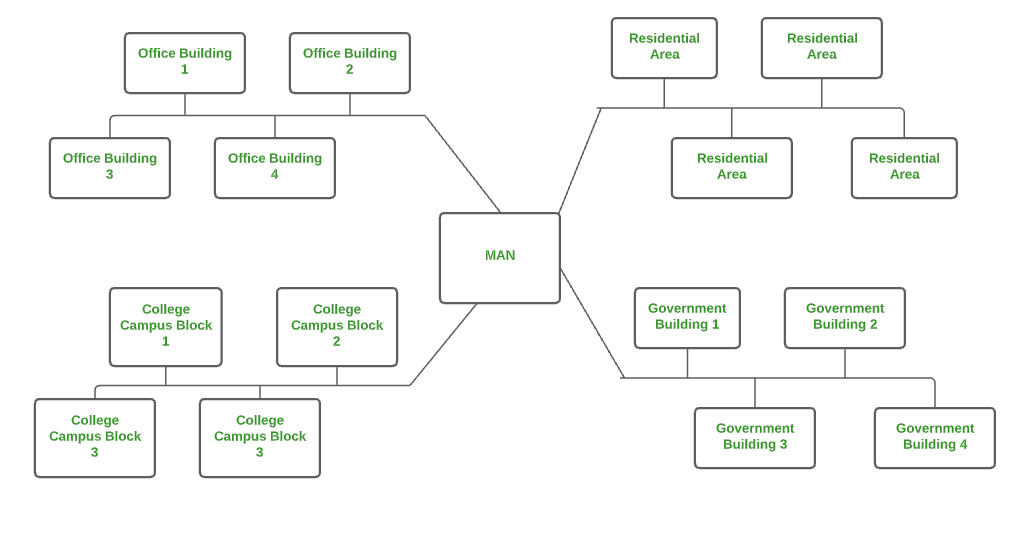


Campus Area Network (CAN)

### ****4. Metropolitan Area Network (MAN)****

A [MAN](https://www.geeksforgeeks.org/man-full-form-in-computer-networking/) 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.



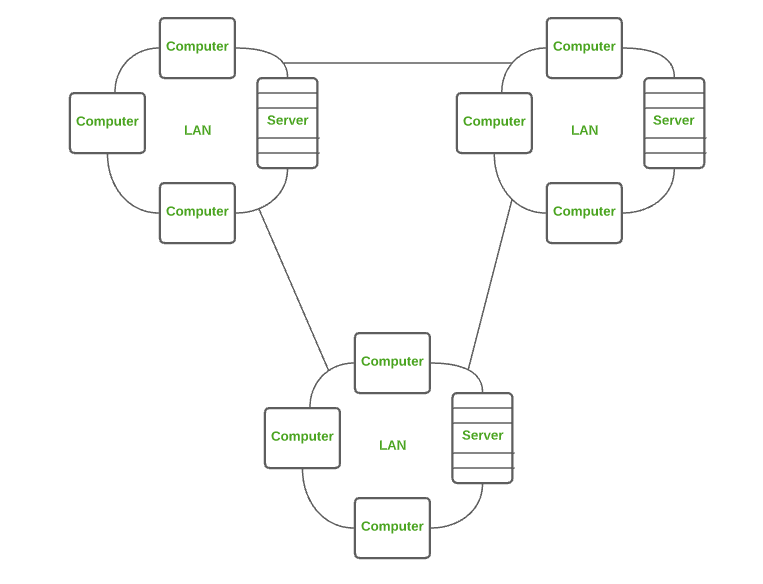
Metropolitan Area Network (MAN)

### ****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](https://www.geeksforgeeks.org/wan-full-form/) 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.



Wide Area Network (WAN)

## Comparison between Different Computer Networks

| **Parameters** | **PAN** | **LAN** | **CAN** | **MAN** | **WAN** |
| --- | --- | --- | --- | --- | --- |
| Full Name | Personal Area Network | Local Area Network | Campus Area Network | Metropolitan Area Network | Wide Area Network |
| Technology | Bluetooth, IrDA,Zigbee | Ethernet & Wifi | Ethernet | FDDI, CDDi. ATM | Leased Line, Dial-Up |
| Range | 1-100 m | Upto 2km | 1 – 5 km | 5-50 km | Above 50 km |
| Transmission Speed | Very High | Very High | High | Average | Low |
| Ownership | Private | Private | Private | Private or Public | Private or Public |
| Maintenance | Very Easy | Easy | Moderate | Difficult | Very Difficult |
| Cost | Very Low | Low | Moderate | High | Very High |

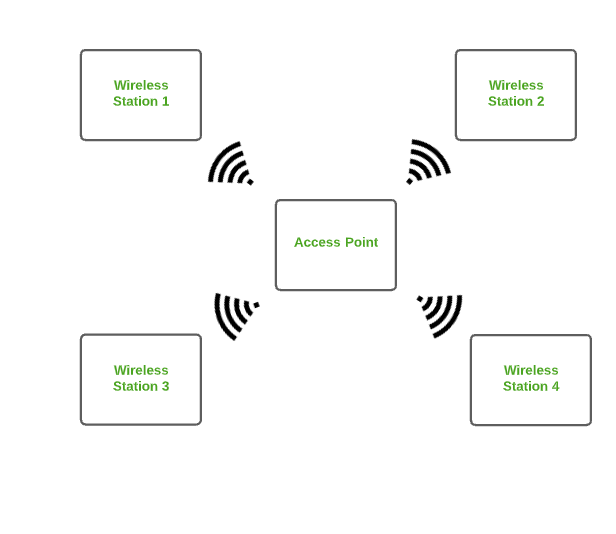
## Other Types of Computer Networks

1. Wireless Local Area Network (WLAN)
2. Storage Area Network (SAN)
3. System-Area Network (SAN)
4. Passive Optical Local Area Network (POLAN)
5. Enterprise Private Network (EPN)
6. Virtual Private Network (VPN)
7. Home Area Network (HAN)

### ****1. Wireless Local Area Network (WLAN)****

[WLAN](https://www.geeksforgeeks.org/wlan-full-form/) 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.



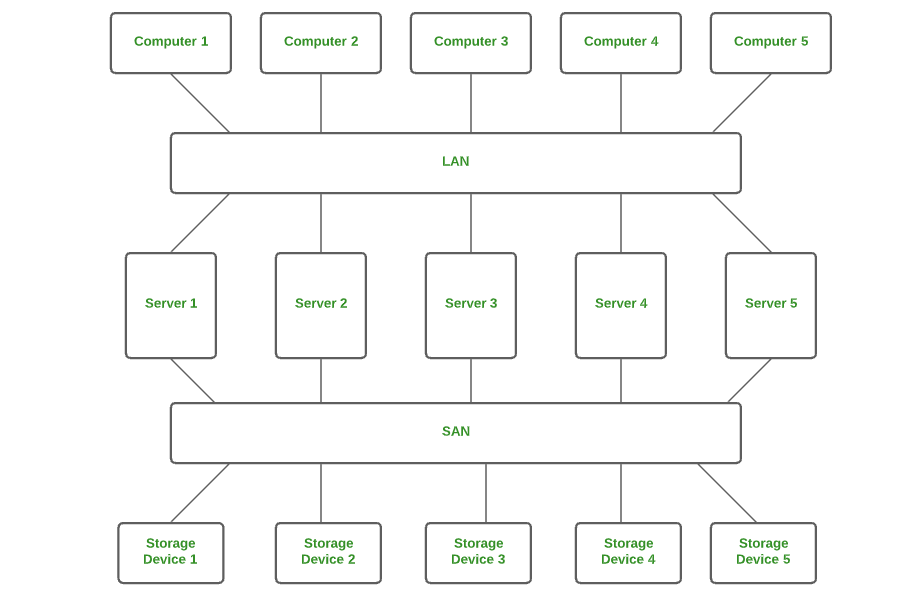
Wireless Local Area Network (WLAN)

There are several computer networks available; more information is provided below.

### ****2. Storage Area Network (SAN)****

[SAN](https://www.geeksforgeeks.org/storage-area-networks/) is a type of computer network that is high-speed and connects groups of storage devices to several servers. This network does not depend on LAN or WAN. Instead, a SAN moves the storage resources from the network to its high-powered network. A SAN provides access to block-level data storage.

Examples of SAN are a network of disks accessed by a network of servers.

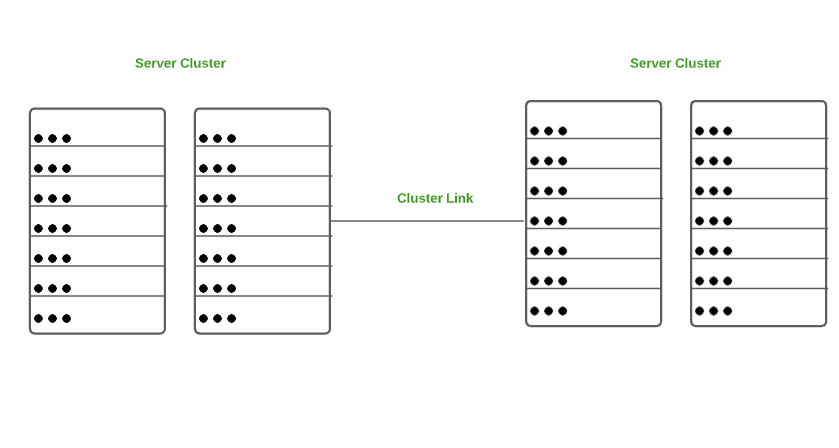


Storage Area Network (SAN)

### ****3. System Area Network (SAN)****

A SAN is a type of computer network that connects a cluster of high-performance computers. It is a connection-oriented and high-bandwidth network. A SAN is a type of LAN that handles high amounts of information in large requests. This network is useful for processing applications that require high network performance.

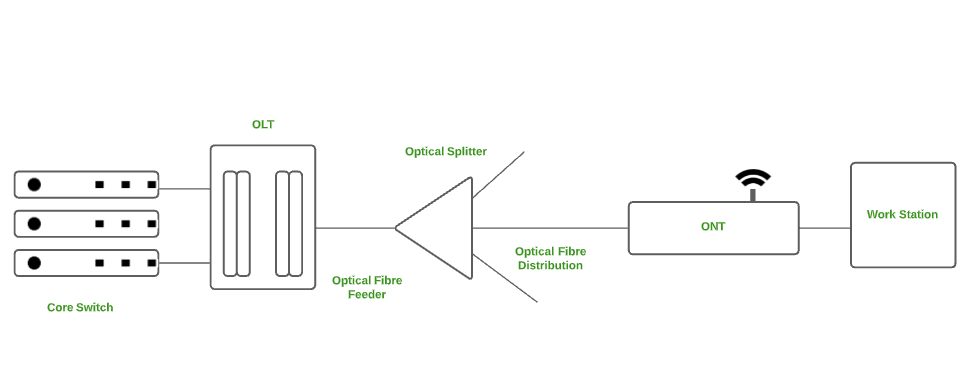
Microsoft SQL Server 2005 uses SAN through a virtual interface adapter.



System Area Network (SAN)

### ****4. Passive Optical Local Area Network (POLAN)****

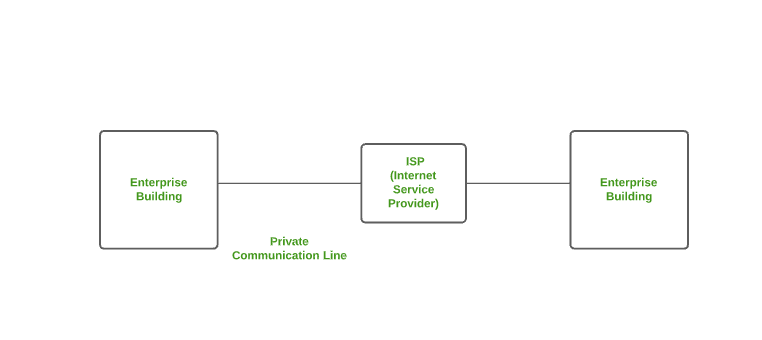
A POLAN is a type of computer network that is an alternative to a LAN. POLAN uses optical splitters to split an optical signal from a single strand of single-mode optical fiber to multiple signals to distribute users and devices. In short, POLAN is a point to multipoint LAN architecture.



Passive Optical Local Area Network (POLAN)

### ****5. Enterprise Private Network (EPN)****

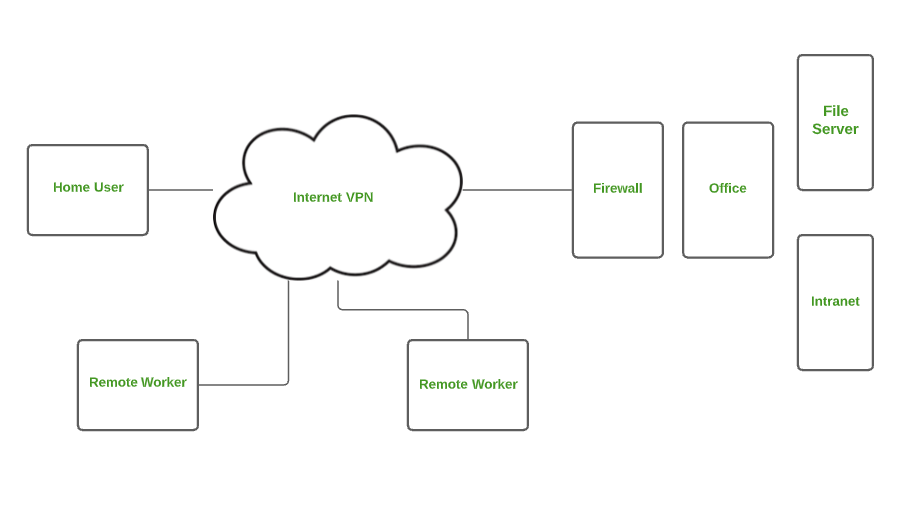
EPN is a type of computer network mostly used by businesses that want a secure connection over various locations to share computer resources.



Enterprise Private Network (EPN)

### ****6. Virtual Private Network (VPN)****

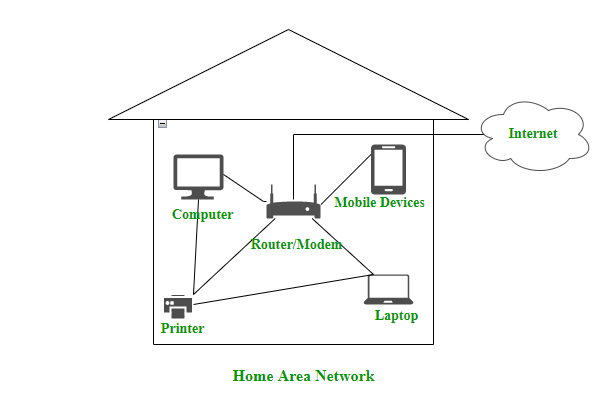
A [VPN](https://www.geeksforgeeks.org/virtual-private-network-vpn-introduction/) is a type of computer network that extends a private network across the internet and lets the user send and receive data as if they were connected to a private network even though they are not. Through a virtual point-to-point connection users can access a private network remotely. VPN protects you from malicious sources by operating as a medium that gives you a protected network connection.



Virtual Private Network (VPN)

### ****7. Home Area Network (HAN)****

Many of the houses might have more than a computer. To interconnect those computers and with other peripheral devices, a network should be established similar to the local area network (LAN) within that home. Such a type of network that allows a user to interconnect multiple computers and other digital devices within the home is referred to as Home Area Network (HAN). [HAN](https://www.geeksforgeeks.org/introduction-of-home-area-network-han/) encourages sharing of resources, files, and programs within the network. It supports both wired and wireless communication.



Home Area Network (HAN)

## Advantages of Computer Network

Some of the main advantages of Computer Networks are:

* **Central Storage of Data:** Files are stored on a central storage database which helps to easily access and available to everyone.
* **Connectivity:**A single connection can be routed to connect multiple computing devices.
* **Sharing of Files:**Files and data can be easily shared among multiple devices which helps in easily communicating among the organization.
* **Security through Authorization:** Computer Networking provides additional security and protection of information in the system.

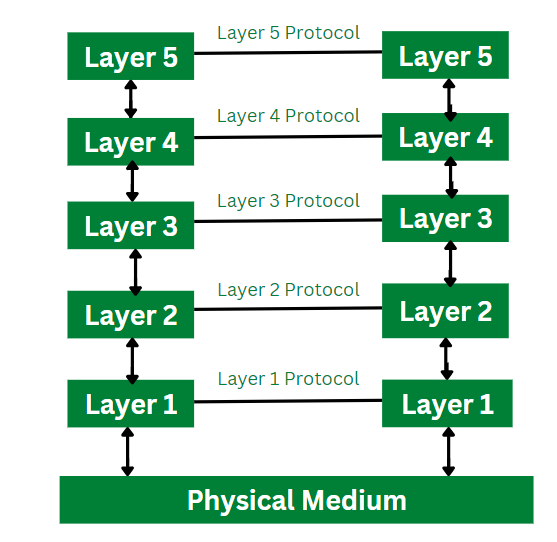
## Disadvantages of Computer Network

Some of the main disadvantages of Computer Networks are:

* **Virus and Malware:**A [virus](https://www.geeksforgeeks.org/what-is-computer-virus/)is a program that can infect other programs by modifying them. Viruses and Malware can corrupt the whole network.
* **High Cost of Setup:** The initial setup of Computer Networking is expensive because it consists of a lot of wires and cables along with the device.
* **loss of Information:**In case of a System Failure, might lead to some loss of data.
* **Management of Network:**Management of a Network is somehow complex for a person, it requires training for its proper use.

# Layered Architecture in Computer Networks

Every network consists of a specific number of functions, layers, and tasks to perform. Layered Architecture in a computer network is defined as a model where a whole network process is divided into various smaller sub-tasks. These divided sub-tasks are then assigned to a specific layer to perform only the dedicated tasks. A single layer performs only s specific type of task. To run the application and provide all types of services to clients a lower layer adds its services to the higher layer present above it. Therefore layered architecture provides interactions between the sub-systems. If any type of modification is done in one layer it does not affect the next layer.



Layered Architecture

As shown in the above diagram, there are five different layers. Therefore it is a five-layered architecture. Each layer performs a dedicated task. The lower level data for example from layer 1 data is transferred to layer 2. Below all the layers Physical Medium is present. The physical medium is responsible for the actual communication to take place. For the transfer of data and communication layered architecture provides with a clean cut interface.

## Features of Layered Architecture

* Use of Layered architecture in computer network provides with the feature of modularity and distinct interfaces.
* Layered architecture ensures independence between layers, by offering services to higher layers from the lower layers and without specifying how this services are implemented.
* Layered architecture segments as larger and unmanageable design into small sub tasks.
* In layer architecture every network has different number of functions, layers and content.
* In layered architecture, the physical route provides with communication which is available under the layer 1.
* In layered architecture, the implementation done by one layer can be modified by the another layer.

## Elements of Layered Architecture

There are three different types of elements of a layered architecture. They are described below:

* **Service:** Service is defined as a set of functions and tasks being provided by a lower layer to a higher layer. Each layer performs a different type of task. Therefore, actions provided by each layer are different.
* **Protocol:**Protocol is defined as a set rules used by the layer for exchanging and transmission of data with its peer entities. This rules can consists details regarding a type of content and their order passed from one layer to another.
* **Interface:**Interface is defined as a channel that allows to transmit the messages from one layer to the another.

## Need of Layered Architecture

* **Divide and Conquer Approach:**Layered architecture supports divide and conquer approach. The unmanageable and complex task is further divided into smaller sub tasks. Each sub task is then carried out by the different layer. Therefore using this approach reduces the complexity of the problem or design process.
* **Easy to Modify:**The layers are independent of each other in layered architecture. If any sudden change occurs in the implementation of one layer, it can be changed. This change does not affect the working of other layers involved in the task. Therefore layered architectures are required to perform any sudden update or change.
* **Modularity:**Layered architecture is more modular as compared to other architecture models in [computer network](https://www.geeksforgeeks.org/basics-computer-networking/). Modularity provides with more independence between the layers and are more easier to understand.
* **Easy to Test:**Each layer in layered architecture performs a different and dedicated task. Therefore each layer can be analyzed and tested individually. It helps to analyze the problem and solve them more efficiently as compared to solving all the problems at a time.

## Application of Layered Architecture in computer Networks

In computer networks, layered architecture is majorly used for communication. The two network models that makes use of layered architecture are:

* OSI Model
* TCP/IP Model

## OSI Model

OSI stands for Open Systems Interconnection. [OSI](https://www.geeksforgeeks.org/layers-of-osi-model/) is a seven layered architecture. All these seven layers work collaboratively to transmit data from one layer to another. Below are the layers of OSI Model.

**1. Physical Layer:**Physical layer is the lowest layer of OSI model and is responsible for the physical connection between all the required devices. The information present in [physical layer](https://www.geeksforgeeks.org/physical-layer-in-osi-model/) is in the form of bits. Physical layer performs various functions such as bit rate control, bit synchronization, transmission mode etc.

**2. Data Link Layer:** Data Link layer provides with successful delivery of message from one node to the another. It checks whether this delivery of message is error free. Other functions performed by data link layer are error control, framing, flow control etc.

**3. Network Layer:**Network Layer is responsible for the transmission of data from one host to the another host that is connected in different network. It performs other tasks such routing and logical addressing.

**4. Transport Layer:** Transport Layer is defined as a layer that takes services from network layer and provides services to application layer. Other tasks performed by [transport layer](https://www.geeksforgeeks.org/transport-layer-responsibilities/) are service point addressing, segmentation and reassembling.

**5. Session Layer:**Session layer is defined as a layer that is responsible for establishing a connection, maintenance of session and to provide with security. Other functions of session Layer are to establish session, termination and [synchronisation](https://www.geeksforgeeks.org/classical-problems-of-synchronization-with-semaphore-solution/).

**6. Presentation Layer:** The data from application layer is extracted at the presentation layer. This layer is also known as translation layer. The functions of presentation layer are encryption, decryption, compression and translation.

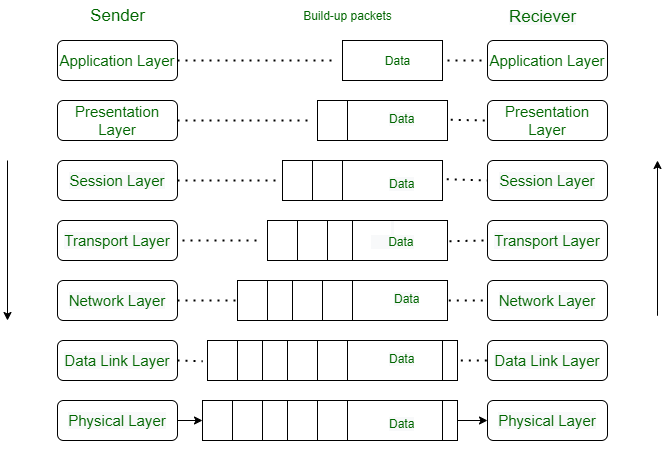
**7. Application Layer:**Application layer is the topmost layer of [OSI](https://www.geeksforgeeks.org/layers-of-osi-model/) Model. Application layer is also known as desktop layer. It provides with other functions such as directory services, mail services, network virtual terminal etc.

# What is OSI Model? – Layers of OSI Model

**OSI stands for Open Systems Interconnection**. It was developed by ISO – ‘International Organization for Standardization’, in the year 1984. It is a 7-layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

## What is OSI Model?

The OSI model, created in 1984 by ISO, is a reference framework that explains the process of transmitting data between computers. It is divided into seven layers that work together to carry out specialised network functions, allowing for a more systematic approach to networking.



## What are the 7 layers of the OSI Model?

The OSI model consists of seven abstraction layers arranged in a top-down order:

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

## ****Physical Layer – Layer 1****

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of**bits.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

### Functions of the Physical Layer

* **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level.
* **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
* **Physical topologies:** Physical layer specifies how the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.
* **Transmission mode:** Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.

**Note:**

1. Hub, Repeater, Modem, and Cables are Physical Layer devices.
2. Network Layer, Data Link Layer, and Physical Layer are also known as **Lower Layers** or **Hardware Layers**.

## ****Data Link Layer (DLL) – Layer 2****

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address.   
The Data Link Layer is divided into two sublayers:

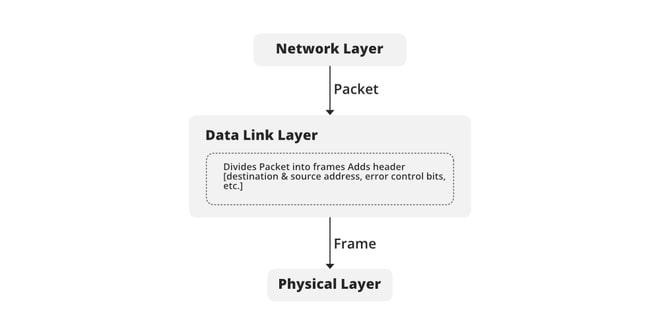
1. [Logical Link Control (LLC)](https://www.geeksforgeeks.org/logical-link-control-llc-protocol-data-unit/)
2. [Media Access Control (MAC)](https://www.geeksforgeeks.org/introduction-of-mac-address-in-computer-network/)

The packet received from the Network layer is further divided into frames depending on the frame size of the NIC(Network Interface Card). DLL also encapsulates Sender and Receiver’s MAC address in the header.

The Receiver’s MAC address is obtained by placing an [ARP(Address Resolution Protocol)](https://www.geeksforgeeks.org/how-address-resolution-protocol-arp-works/)request onto the wire asking “Who has that IP address?” and the destination host will reply with its MAC address.

### Functions of the Data Link Layer

* **Framing:**Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
* **Physical addressing:** After creating frames, the Data link layer adds physical addresses (MAC addresses) of the sender and/or receiver in the header of each frame.
* **Error control:** The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
* **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment.
* **Access control:**When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.



**Note:**

1. Packet in the Data Link layer is referred to as **Frame.**
2. Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.
3. Switch & Bridge are Data Link Layer devices.

## ****Network Layer – Layer 3****

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver’s IP addresses are placed in the header by the network layer.

### Functions of the Network Layer

* **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
* **Logical Addressing:**To identify each device on Internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver’s IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

**Note:**

1. Segment in the Network layer is referred to as **Packet**.
2. Network layer is implemented by networking devices such as routers and switches.

## ****Transport Layer – Layer 4****

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as Segments. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

**At the sender’s side:**The transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.

**Note:** The sender needs to know the port number associated with the receiver’s application.

Generally, this destination port number is configured, either by default or manually. For example, when a web application requests a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned.

**At the receiver’s side:** Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

### Functions of the Transport Layer

* **Segmentation and Reassembly:** This layer accepts the message from the (session) layer, and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
* **Service Point Addressing:** To deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

#### Services Provided by Transport Layer

1. [Connection-Oriented Service](https://www.geeksforgeeks.org/connection-oriented-service/)
2. [Connectionless Service](https://www.geeksforgeeks.org/connection-less-service/)

**1. Connection-Oriented Service:** It is a three-phase process that includes

* Connection Establishment
* Data Transfer
* Termination/disconnection

In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.

**2. Connectionless service:** It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

**Note:**

1. Data in the Transport Layer is called **Segments**.
2. Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.
3. The transport layer is called as **Heart of the OSI** model.
4. **Device or Protocol Use :** TCP, UDP  NetBIOS, PPTP

## ****Session Layer – Layer 5****

This layer is responsible for the establishment of connection, maintenance of sessions, and authentication, and also ensures security.

### Functions of the Session Layer

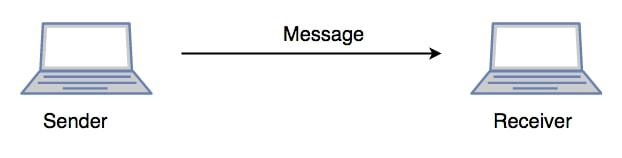
* **Session establishment, maintenance, and termination:** The layer allows the two processes to establish, use and terminate a connection.
* **Synchronization:** This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
* **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

**Note:**

1. All the below 3 layers(including Session Layer) are integrated as a single layer in the TCP/IP model as the ????pplication Layer”.
2. Implementation of these 3 layers is done by the network application itself. These are also known as **Upper Layers or** **Software Layers.**
3. **Device or Protocol Use :**  NetBIOS, PPTP.

**for Example:-**

Let us consider a scenario where a user wants to send a message through some Messenger application running in his browser. The “Messenger” here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data), and converted into bits (0’s and 1’s) so that it can be transmitted.



Communication in Session Layer

## ****Presentation Layer – Layer 6****

The presentation layer is also called the **Translation layer**. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

### Functions of the Presentation Layer

* **Translation:** For example, ASCII to EBCDIC.
* **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
* **Compression:** Reduces the number of bits that need to be transmitted on the network.

Note: **Device or Protocol Use :**  JPEG, MPEG, GIF

## ****Application Layer – Layer 7****

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

**Example**: Application – Browsers, Skype Messenger, etc.

**Note:** 1. The application Layer is also called Desktop Layer.

2.**Device or Protocol Use :**  SMTP

### Functions of the Application Layer

The main functions of application layer are given below.

* Network Virtual Terminal: It allows a user to log on to a remote host.
* FTAM- File transfer access and management : This application allows a user to  
  access file in a remote host, retrieve files in remote host and manage or  
  control files from a remote computer.
* Mail Services : Provide email service.
* Directory Services : This application provides distributed database sources  
  and access for global information about various objects and services.

**Note:**OSI model acts as a reference model and is not implemented on the Internet because of its late invention. The current model being used is the TCP/IP model.

## ****OSI Model in a Nutshell****

| **Layer No** | **Layer Name** | **Responsibility** | **Information Form(Data Unit)** | **Device or Protocol** |
| --- | --- | --- | --- | --- |
| **7** | Application Layer | Helps in identifying the client and synchronizing communication. | Message | SMTP |
| **6** | Presentation Layer | Data from the application layer is extracted and manipulated in the required format for transmission. | Message | JPEG, MPEG, GIF |
| **5** | Session Layer | Establishes Connection, Maintenance, Ensures Authentication, and Ensures security. | Message | Gateway |
| **4** | Transport Layer | Take Service from Network Layer and provide it to the Application Layer. | Segment | Firewall |
| **3** | Network Layer | Transmission of data from one host to another, located in different networks. | Packet | Router |
| **2** | Data Link Layer | Node to Node Delivery of Message. | Frame | Switch, Bridge |
| **1** | Physical Layer | Establishing Physical Connections between Devices. | Bits | Hub, Repeater, Modem, Cables |