**HTML stands for hyper text markup language which is generally used to create web pages. While creating web pages formation of frames is also a vital part to know. Basically, a framed document divides a browser window into multiple panes or smaller window frames. Each frame can contain a different document. The benefit of making frames are that users can view information in one frame while keeping another frame open for reference instead of moving back and forth between pages. The contents of one frame can be manipulated or linked to the contents of other. This enables the web page designer to build sophisticated interfaces.**

**Floating Frame**

**A floating frame is used to embed another document or page within an existing frame.** This frame will be an inline framed region that acts like other embedded objects—meaning that text can flow around it.



**Add the iframe element to the <body> of the HTML document.** The inline frame is defined by the iframe element.

* To create an<iframe> tag the major attributes required is src, height, and width.
* The src is set to the URL of the file to load while the height and width are set either to the pixel or percentage value of the screen that the floating frame region should consume.

the navigation frame appears on the left of the display and contains items that allow you to display a menu or view or to perform an action

The navigation frame appears on the left of the display and contains items that allow you to display a menu or view or to perform an action. The items that are displayed depend on your configuration and authority. For example, if you do not have authority to customize the display, you will not have a link to the View Editor.

The types of links in the navigation frame are:

**Menus and views**

Links that when selected can set the contents of the work frame to another menu or view.

**External links**

Links to external URLs that launch a new Web browser instance.

**Standard links**

These appear automatically and cannot be customized.

**Open links**

**Home**

Opens your home menu using the current context and scope. You may return to the current display using the Go back icon.

**Repeat Last Menu**

Open the last menu that was displayed using the current context and scope. You may return to the current display using the Go back icon.

**Special links**

**Favorites editor link**

Open a new window containing the Web User Interface customization tool, the favorites editor. This is available only to users who have created one or more favorites.

**View editor link**

Open a new window containing the Web User Interface customization tool, the view editor. This is available only to users with the appropriate authority.

**User editor link**

Open a new window containing the Web User Interface customization tool, the user editor. This is available only to users with the appropriate authority.

**New window link**

Open a new Web browser window containing an independent Web User Interface display of the current view or menu using the current selection criteria.

**Close window link**

Close a Web browser window.

**Sign off link**

Sign off your Web User Interface session.

Some items in the navigation frame may be in groups, that can be expanded or collapsed independently of other groups, using the expand and collapse icons

The Internet is theforemost important tool and the prominent resource that is being used by almost every person across the globe. It connects millions of computers, webpages, websites, and servers. Using the internet we can send emails, photos, videos, and messages to our loved ones. Or in other words, the Internet is a widespread interconnected network of computers and electronic devices(that support Internet). It creates a communication medium to share and get information online. If your device is connected to the Internet then only you will be able to access all the applications, websites, social media apps, and many more services. The Internet nowadays is considered the fastest medium for sending and receiving information.

*Internet*

**History of the Internet**

The Internet came in the year 1960 with the creation of the first working model called [ARPANET (Advanced Research Projects Agency)](https://www.geeksforgeeks.org/arpanet-full-form/). It allowed multiple computers to work on a single network which was their biggest achievement at that time. ARPANET uses packet switching to communicate multiple computer systems under a single network. In October 1969, using ARPANET first message was transferred from one computer to another. After that technology continues to grow.

**How is the Internet Set Up?**

The internet is set up with the help of physical optical fiber data transmission cables or copper wires and various other networking mediums like LAN, WAN, MAN, etc. For accessing the Internet even the 2G, 3G, and 4G services and the Wifi require these physical cable setups to access the Internet. There is an authority named **ICANN (Internet Corporation for Assigned Names and Numbers)** located in the USA which manages the Internet and protocols related to it like IP addresses.

**How Does the Internet Work?**

The actual working of the internet takes place with the help of [clients and servers](https://www.geeksforgeeks.org/client-server-model/). Here the client is a laptop that is directly connected to the internet and servers are the computers connected indirectly to the Internet and they are having all the websites stored in those large computers. These servers are connected to the internet with the help of [ISP (Internet Service Providers)](https://www.geeksforgeeks.org/isp-full-form/) and will be identified with the IP address.

Each website has its Domain name as it is difficult for any person to always remember the long numbers or strings. So, whenever you search for any domain name in the search bar of the browser the request will be sent to the server and that server will try to find the IP address from the Domain name because it cannot understand the domain name. After getting the IP address the server will try to search the IP address of the Domain name in a Huge phone directory that in networking is known as a [DNS server (Domain Name Server)](https://www.geeksforgeeks.org/domain-name-system-dns-in-application-layer/). For example, if we have the name of a person and we can easily find the Aadhaar number of him/her from the long directory as simple as that.

So after getting the IP address, the browser will pass on the further request to the respective server and now the server will process the request to display the content of the website which the client wants. If you are using a wireless medium of Internet like 3G and 4G or other mobile data then the data will start flowing from the optical cables and will first reach towers from there the signals will reach your cell phones and PCs through electromagnetic waves and if you are using routers then optical fiber connecting to your router will help in connecting those light-induced signals to electrical signals and with the help of ethernet cables internet reaches your computers and hence the required information

When many computers are connected, connecting means that they can share data such as text, information, photos, audio, videos and many other services together making a "Network". When this network happens worldwide, that becomes the Internet.

Take a real-life simple example, when you are seeing photos on Instagram, tweets on Twitter, or talk through Facebook, that is when you are connected to the internet. Things are happening worldwide.

The [**Internet**](https://www.tutorialspoint.com/internet_technologies/internet_overview.htm) is used on a vast level, and it is impossible to imagine our world without the Internet. Not only for personal use, organizations and government sectors are also connected to the internet and are providing us services.

Application and Features of the Internet

Uses of the Internet on daily basis

Let’s look at some of the uses of the Internet in our daily life −

* Online Food Order
* Grocery Store
* Educational Online Classes
* Online Banking or Net Banking
* Cashless Transactions
* Social Network
* Hospital Registration and Bill Receipts
* Online Train or Flight Bookings

Today, there are countless examples we can see around us. These are some real-life easy examples. Lets now see some of the features of the Internet −

Features of Internet

* Data Transfer is easier while using the internet.
* Accessibility to almost every piece of information.
* Expansion of business in IT technology.
* Faster and Feasible government services.
* Security and Safety of Information virtually.
* Saves lots of time in processing and management.
* The Internet is not centrally dependent upon one center as it is divided into several data centers and extensions to provide scalability.

Ezoic

Advantages and Disadvantages of the Internet

As we know the internet is accessible to every information we want within a fraction of a second. It gives more results and increases productivity. There are many Advantages of the Internet, Lets now see and learn what they are −

Advantages of Internet

* **Connectivity** − As we know we are connected to the internet to stay connected with our family, friends, colleagues, services, etc.
* **Information** − We can search and get many search results for our questions and the information can increase knowledge.
* **Online Payment** − Using payment modes such as Paytm, GPay, and Bhim UPI are many payment methods to pay online.
* **Digital Marketing** − We are making our websites and making business online.
* **Net Banking Services** − Banking services such as payment, debit, credit, changing our details, and scheduling payment are an integral part of secure payment.
* **Productive Collaboration** − As we experienced, after the Covid pandemic, we have worked from home and made things work better than ever before by connecting through video conferencing and saving mobility.

As we know Internet has some of its disadvantages also, let’s now consider them −

Disadvantages Of Internet

* **Wastage of time** − Considering today’s lifestyle, one prominent advantage of the Internet is addiction. People are getting addicted to the internet, watching videos and reels without realizing they are wasting so much of their time.
* **Cybercrime** − It is increasing rapidly as more information is shared and getting leaked.
* **Accessibility of pornographic content** − It is accessible to even children since there is complex information shared every day and it is hard to figure out the source of these images and videos. This is a big concern regarding children and their minds, parental security is necessary on mobile phones being used by children.
* **Identity theft** − It is one major concern on a bigger level such as higher organizations, government, and private sectors.
* **Increase in cyber attacks in the banking sector and corporate sector** − Information is getting leaked, shared, and misused for harm, theft, privacy violation, and harassment.
* **Fake Information or Misleading** − People nowadays can easily manipulate any information and reclaim it to be true this could mislead people and their reliability towards information shared.

|  |  |
| --- | --- |
| **Advantages of Internet** | **Disadvantages of Internet** |
| It provides great Accessibility to information. | Sometimes, the internet gives Complexity and False Information. |
| It inculcates easy and faster communication. | Unavailability in bad weather. |
| People would gain knowledge and obtain loads of information about services. | It leads to the insecurity of information and data loss. |
| It permits online payments and digital marketing. | It has a bigger Workload and Complex Designing. |
| It is efficient for business & organizational growth. | It is very expensive when done at the organizational level. |
| It leads to mass communication among people to spread awareness. | It produces more threats, cyber-attacks, harassment, and violations. |
| It facilitates social networks to increase development and collaboration. | Increase hate and fake information which can lead to mental health issues. |
| It provides more security in the banking sector and feasible solutions to issues. | Reliability and security are there, but as the internet is public and worldwide connected, there are chances that issues(viruses, threats) can occur. |

**Uses of the Internet for Businesses**

The Internet offers a great marketplace where clients may browse the websites of **eCommerce** suppliers, submit their online orders, and pay through a payment gateway. From the **vendor's warehouse**, the ordered items are shipped to the clients in the predetermined number of days. Having even a simple website that provides contact information, a location, products, and services, pricing or rates, etc. is beneficial to many businesses.

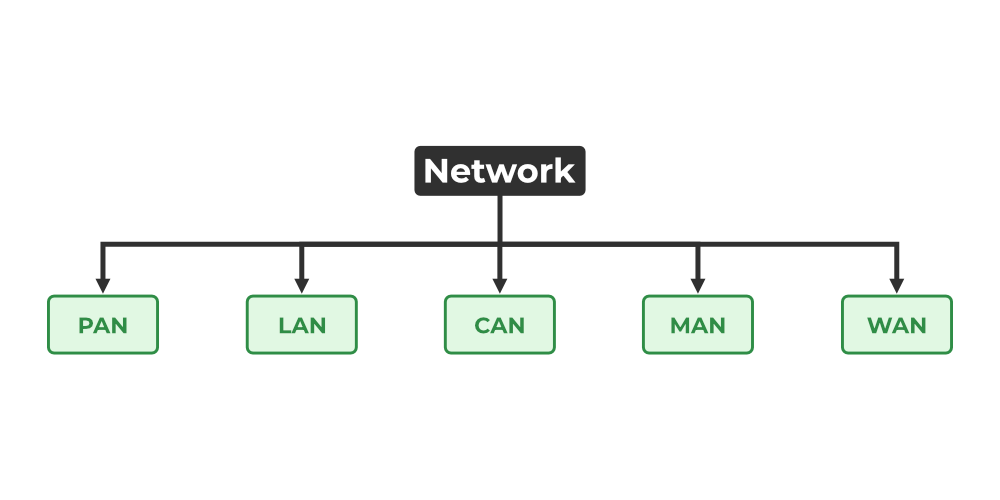
Businesses can effectively communicate with their clients and the general public about the goods and services offered on their websites thanks to the Internet. The company may communicate with all of its clients over the Internet and create solid client relationships.

Through the internet, employees are linked to their workplace, allowing them to work remotely and forego the difficulties of commuting. **Online training** is also provided to workers through the internet.

**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/)

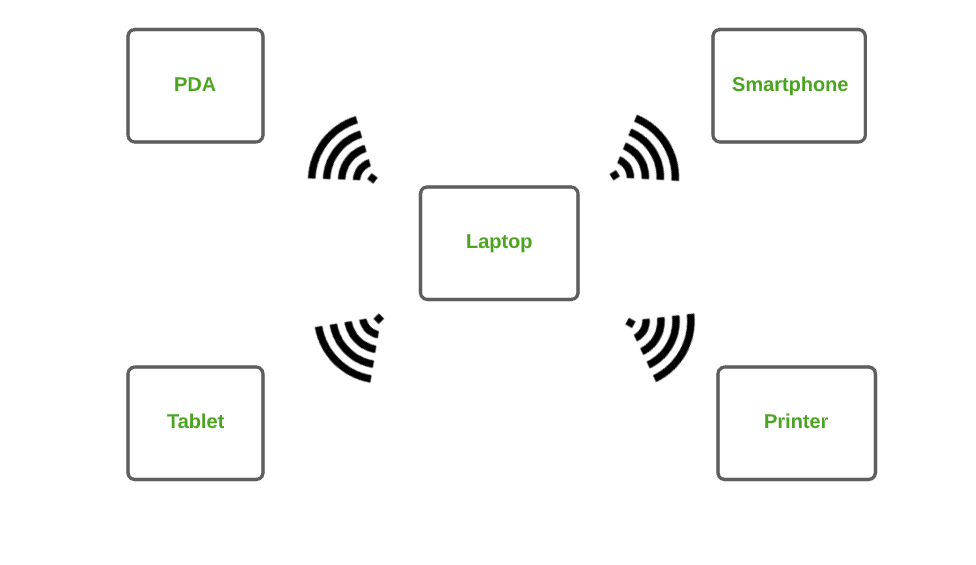


*Types of Computer Networks*

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

[PAN](https://www.geeksforgeeks.org/overview-of-personal-area-network-pan/) is the most basic type of computer network. It is a type of network designed to connect devices within a short range, typically around one person. It allows your personal devices, like smartphones, tablets, laptops, and wearables, to communicate and share data with each other. PAN offers a network range of 1 to 100 meters from person to device providing communication. Its transmission speed is very high with very easy maintenance and very low cost. This uses[Bluetooth](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.





*Personal Area Network (PAN)*

**Types of PAN**

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

**Advantages of PAN**

* PAN is relatively flexible and provides high efficiency for short network ranges.



* It needs easy setup and relatively low cost.



* It does not require frequent installations and maintenance
* It is easy and portable.



* Needs fewer technical skills to use.



**Disadvantages of PAN**

* Low network coverage area/range.



* Limited to relatively low data rates.
* Devices are not compatible with each other.
* Inbuilt WPAN devices are a little bit costly.

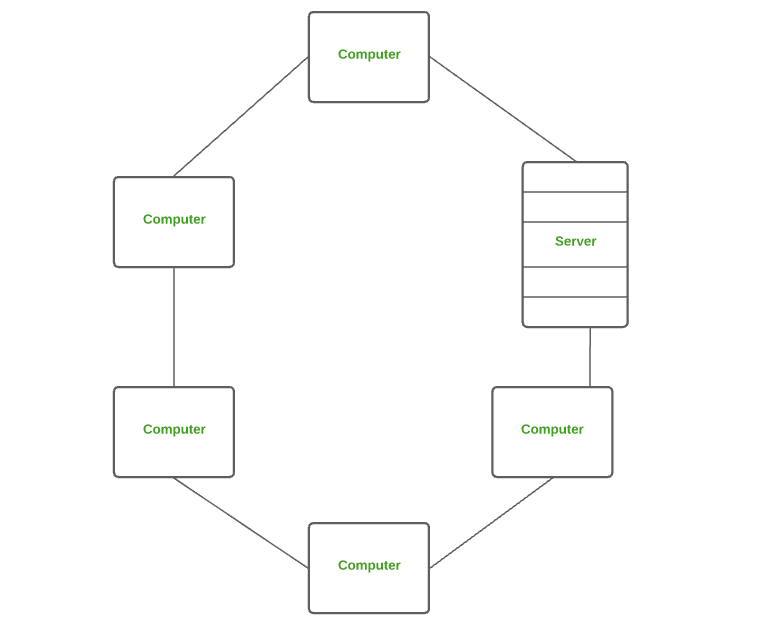
**Applications of PAN**

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

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

LAN is the most frequently used network. A [LAN](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.





*Local Area Network (LAN)*

**Advantages of a LAN**

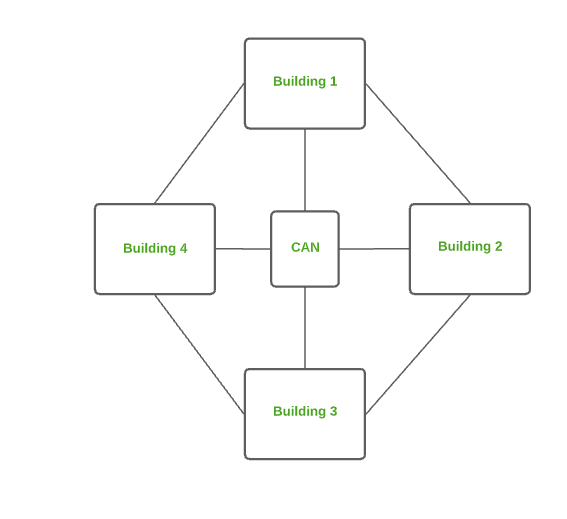
* **Privacy:** LAN is a private network, thus no outside regulatory body controls it, giving it a privacy.
* **High Speed:** LAN offers a much higher speed(around 100 mbps) and data transfer rate comparatively to WAN.
* **Supports different transmission mediums:** LAN support a variety of communications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

**Disadvantages of LAN**

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

**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.



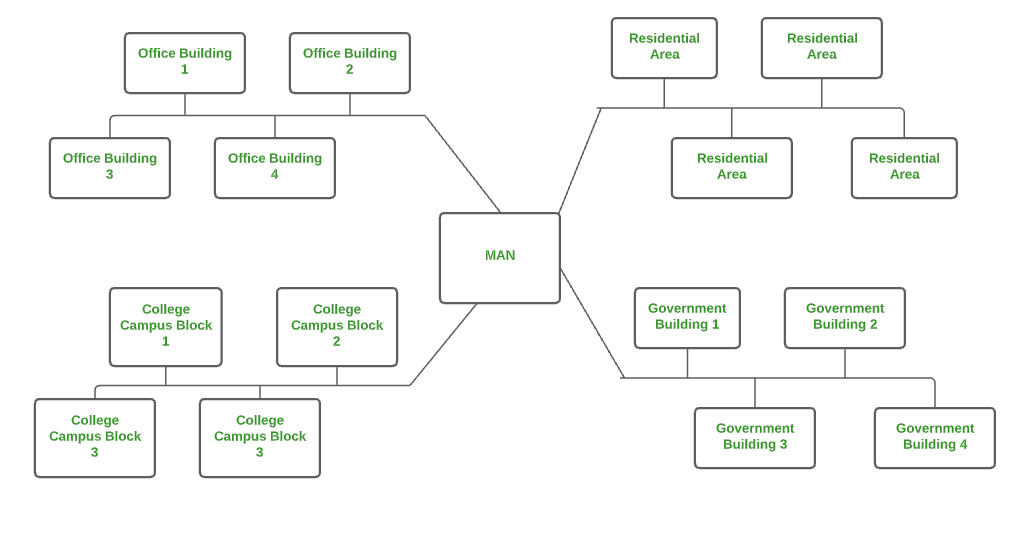
*Campus Area Network (CAN)*

**Advantages of CAN**

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

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

A [MAN](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)*

**Advantages of MAN**

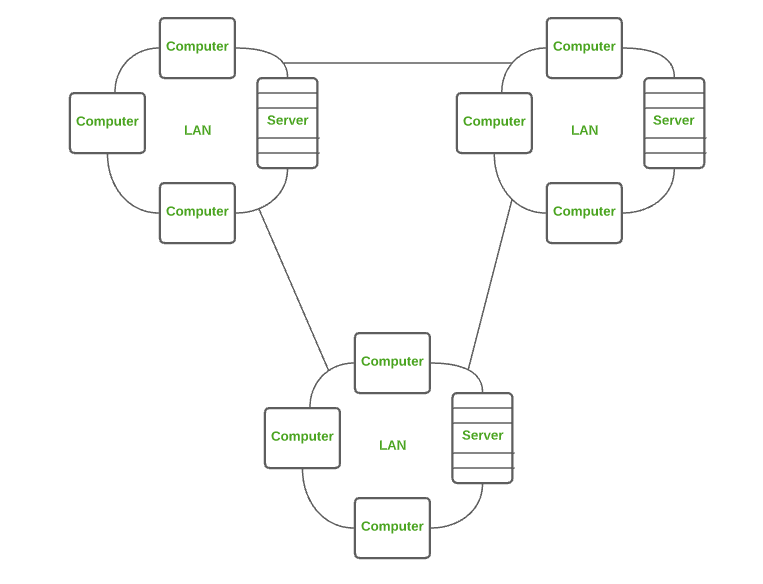
* MAN offers high-speed connectivity in which the speed ranges from 10-100 Mbps.
* The security level in MAN is high and strict as compared to WAN.
* It support to transmit data in both directions concurrently because of dual bus architecture.
* MAN can serve multiple users at a time with the same high-speed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

**Disadvantages of MAN**

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

**5. Wide Area Network (WAN)**

WAN is a type of computer network that connects computers over a large geographical distance through a shared communication path. It is not restrained to a single location but extends over many locations. [WAN](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)*

**Advantages of WAN**

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

**Disadvantages of WAN**

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

**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 |

**Network Topology**

Network topology refers to the arrangement of different elements like nodes, links, or devices in a computer network. It defines how these components are connected and interact with each other. Understanding various types of network topologies helps in designing efficient and robust networks. Common types include bus, star, ring, mesh, and tree topologies, each with its own advantages and disadvantages. In this article, we are going to discuss different types of network topology their advantages and disadvantages in detail.

**Types of Network Topology**

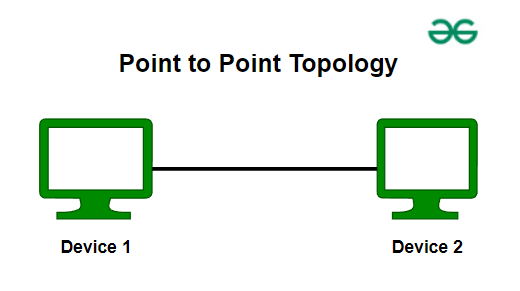
The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as **Network Topology**. The various network topologies are:

* [Point to Point Topology](https://www.geeksforgeeks.org/differences-between-point-to-point-and-multi-point-communication/)
* [Mesh Topology](https://www.geeksforgeeks.org/advantage-and-disadvantage-of-mesh-topology/)
* [Star Topology](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-star-topology/)
* [Bus Topology](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-bus-topology/)
* [Ring Topology](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-ring-topology/)
* [Tree Topology](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-tree-topology/)
* [Hybrid Topology](https://www.geeksforgeeks.org/what-is-hybrid-topology/)

A strong understanding of network topologies is essential for competitive exams like GATE, where computer networks are a significant subject. To deepen your knowledge and enhance your exam preparation, consider enrolling in the [GATE CS Self-Paced Course](https://gfgcdn.com/tu/R8G/). This course covers all critical networking concepts, including detailed explanations of various network topologies, equipping you with the expertise needed to excel in your exams.

**Point to Point Topology**

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



*Point to Point Topology*

**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](https://www.geeksforgeeks.org/dynamic-host-configuration-protocol-dhcp/)(Dynamic Host Configuration Protocol), etc.



*Mesh Topology*

**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 N C 2 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 Mesh Topology**

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

**Disadvantages of Mesh Topology**

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

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

**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](https://www.geeksforgeeks.org/what-is-ethernet/)LAN protocols are used as CD(Collision Detection), [CSMA](https://www.geeksforgeeks.org/carrier-sense-multiple-access-csma/)(Carrier Sense Multiple Access), etc.



*Star Topology*

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

**Advantages of Star Topology**

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

**Disadvantages of Star Topology**

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

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

**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](https://www.geeksforgeeks.org/mac-address-in-computer-network/)(Media Access Control) protocols are followed by LAN ethernet connections like [TDMA](https://www.geeksforgeeks.org/difference-between-fdma-tdma-and-cdma/), [Pure Aloha](https://www.geeksforgeeks.org/what-is-pure-aloha/), CDMA, [Slotted Aloha](https://www.geeksforgeeks.org/what-is-slotted-aloha/), etc.



*Bus Topology*

**Figure 3**: A bus topology with shared backbone cable. The nodes are connected to the channel via drop lines.

**Advantages of Bus Topology**

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

**Disadvantages of  Bus Topology**

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

A common example of bus topology is the Ethernet LAN, where all devices are connected to a single coaxial cable or twisted pair cable. This topology is also used in cable television networks..

**Ring Topology**

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

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



*Ring Topology*

**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.

**Operations of Ring Topology**

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

**Advantages of Ring Topology**

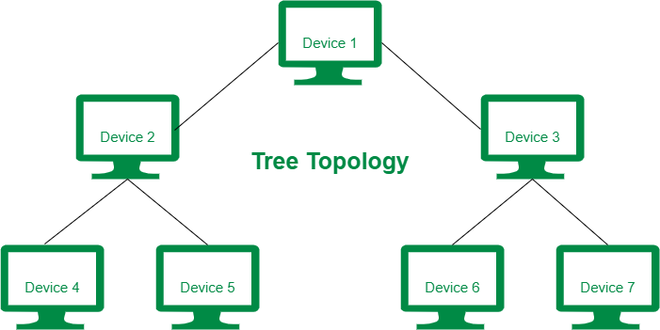
* The data transmission is high-speed.
* The possibility of collision is minimum in this type of topology.
* Cheap to install and expand.
* It is less costly than a star topology.

**Disadvantages of Ring Topology**

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

**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](https://www.geeksforgeeks.org/student-activity-council-sac-interview-experience/)(Standard Automatic Configuration ) are used.



*Tree Topology*

**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 Tree Topology**

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

**Disadvantages of Tree Topology**

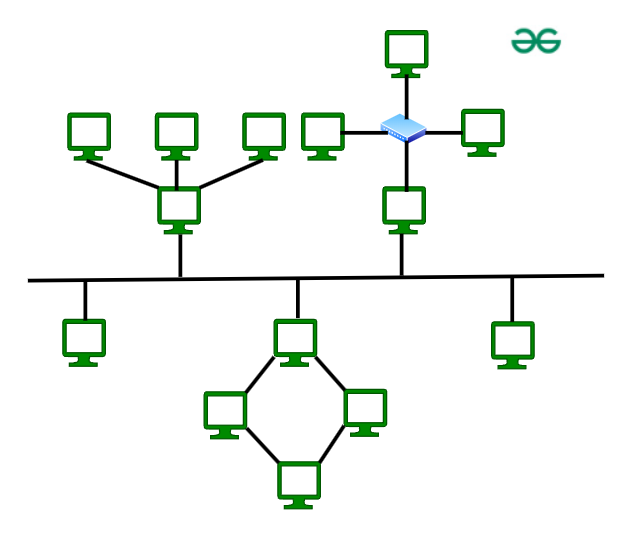
* If the central hub gets fails the entire system fails.
* The cost is high because of the cabling.
* If new devices are added, it becomes difficult to reconfigure.

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

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

**Hybrid Topology**

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



*Hybrid Topology*

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

**Advantages of Hybrid Topology**

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

**Disadvantages of Hybrid Topology**

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

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

A modem and router are two of the most frequent components in a home network configuration. A router establishes a local area network (LAN), whereas a modem connects to an internet service provider (ISP). For a home network to work, both devices are necessary.

**What is a Modem?**

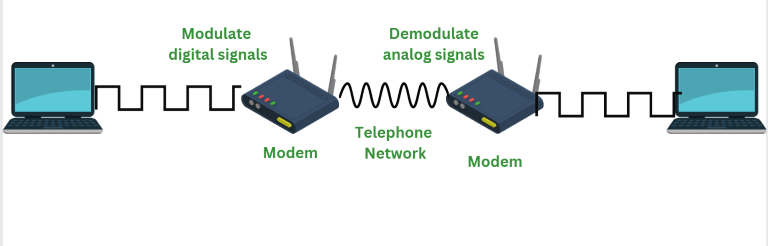
[Modem](https://www.geeksforgeeks.org/how-to-install-a-modem/) stands for Modulator/Demodulator. The modem is defined as a [networking device](https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/) that is used to connect devices connected in the network to the[internet](https://www.geeksforgeeks.org/internet-and-its-services/). The main function of a modem is to convert the [analog signals](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-analog-signals/) that come from telephone wire into a digital form. In digital form, these converted signals are stored in the form of 0s and 1s. The modem can perform both the task of [modulation](https://www.geeksforgeeks.org/what-is-modulation/) and demodulation simultaneously. Modems are majorly used to transfer digital data in personal systems. The modem is also known as a signal translator as it translates one signal into another signal by modulating the [digital signal](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-digital-signals/)into an analog signal for transmission and then demodulates receiving analog signals into digital signals.

**Features of Modem**

* Modems can modulate as well as demodulate the signals simultaneously.
* Modem allows to connect only a specific number of devices to the internet.
* According to the features of modem, it’s price ranges.
* Modems can be upgraded with the help of a specific[software](https://www.geeksforgeeks.org/software-and-its-types/)patch.
* To use the devices over the internet with a modem devices need to be configured with an [Internet Service Provider(ISP)](https://www.geeksforgeeks.org/internet-service-provider-isp-hierarchy/).
* When the modem is connected to [Hub](https://www.geeksforgeeks.org/difference-between-hub-and-bridge/) it slows down its process.

**Working of Modem**

The two main components of a modem are modulation and demodulation. Where the modem can perform both tasks simultaneously. The step-by-step working of the modem is given below:



**Step 1: Data Generation:** When data needs to be transmitted it is first generated. Therefore computer system generated the data which is in digital form of 0s and 1s.

**Step 2: Modulation:**Modulation is defined as a process of converting digital data signals of the computer into analog data signals so that these signals can travel on the internet. The digital data is encoded onto a carrier wave.

**Step 3: Transmission:** The resultant of modulation that is modulated data is transmitted over the communication line to the modem that is receiving it.

**Step 4: Demodulation:**Demodulation is defined as a process in which analog data signals from the internet are converted into digital data signals so they can be understood by computer systems. In the process of demodulation the digital data from the carrier wave is decoded.

**Step 5: Decoding:** The resultant of demodulation that is demodulated data is being sent to the computer systems for their further use.

**Types of Modem**

There are different types of modems available. Each modem has different features and provides with different benefits. Below are the different types of modems:

**1. Optical Modem**

In modem, different type of media is used to transfer the signals. Optical Modem is the type of modem that makes use of optical cables instead of using another metallic type of media. The digital data is converted into the pulse of light that is transmitted on the [optical fiber](https://www.geeksforgeeks.org/types-of-joints-in-optical-fiber/)used in the optical Modem.

**2. Digital Modem**

Digital Modem is defined as a type of modem that is used to convert digital data into digital signals. Digital data is in form of 0s and 1s. For this, it performs the process of modulation. Digital Modem modulates the digital data on digital carrier signals for transmission.

**3. Cable Modem**

Cable modems are defined as a type of modem used to establish a communication between computer systems and the Internet Service Providers. A cable modem helps to access high-speed data through cable TV networks. Such modems are usually connected to desktops or systems and work like external devices.

**4. Satellite Modem**

Satellite Modems are defined as a type of modem that provides with the internet connection through satellite dishes. This type of modem works by sending the input bits into output radio signals and vice versa. The internet network that is provided by such types of modems is more reliable and efficient as compared to other types of modems.

 gateway is a network node or device that connects two networks that use different transmission protocols. Gateways play an important role in connecting two networks. It works as the entry-exit point for a network because all traffic that passes across the networks must pass through the gateway. In this article, we are going to discuss all important points related to Gateways.

**What are Gateways?**

A network gateway is a device that connects different networks by translating messages from one protocol into another protocol. The gateway monitors and controls all the incoming and outgoing [network traffic](https://www.geeksforgeeks.org/scraping-data-in-network-traffic-using-python/). Gateways are also known as protocol converters because they play an important role in converting protocols supported by traffic on different networks. As a result, it allows smooth communication between two networks.

**Features of Gateways**

Gateways provide a wide variety of features. Some of these are:

* A gateway is situated at a network’s edge and manages all data that enters or exits the network.
* A gateway is distinct from other network devices in that it can operate at any layer of the [OSI model](https://www.geeksforgeeks.org/open-systems-interconnection-model-osi/).
* Gateways made the transmission more feasible as it queued up all the data and divided it into small packets of data rather than sending it bulk.
* Gateways provide security within the network.

**Types of Gateways**

These below are the types of Gateway on the basis of **direction of flow of data**:

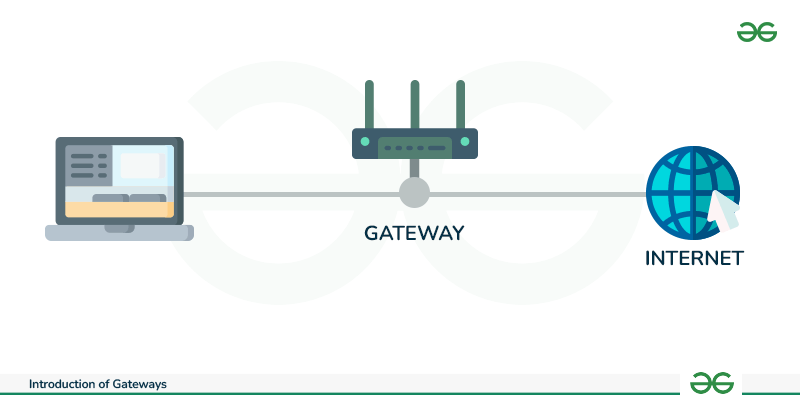
* **Unidirectional Gateways:**Data can only pass through unidirectional gateways in one direction. The destination node replicates changes made in the source node but not the other way around. They are tools for archiving the packets.
* **Bidirectional Gateway:**Data can pass through bidirectional gateways in both directions. They are tools for synchronisation.

These below are the types of Gateway on the basis of **functionality** of Gateway:

* **Network Gateway:** The most popular kind of gateway, known as a network gateway acts as an interface between two disparate networks using distinct protocols. Anytime the word gateway is used without a type designation, it refers to a network gateway.
* **Cloud Storage Gateway**: A network node or server known as a cloud storage gateway translates storage requests made using various cloud storage service API calls, such as [SOAP (Simple Object Access Protocol)](https://www.geeksforgeeks.org/basics-of-soap-simple-object-access-protocol/) or [REST (Representational State Transfer)](https://www.geeksforgeeks.org/rest-api-introduction/). Data communication is made simpler since it makes it easier to integrate private cloud storage into applications without first moving those programmes to a public cloud.
* **Internet-To-Orbit Gateway (I2O):** Project HERMES and Global Educational Network for Satellite Operations (GENSO) are two well-known I2O gateways that connect devices on the Internet to satellites and spacecraft orbiting the earth.
* **IoT Gateway:**Before delivering sensor data to the cloud network, [IoT gateways](https://www.geeksforgeeks.org/internet-of-things-iot-gateways/) assimilate it from [Internet of Things (IoT)](https://www.geeksforgeeks.org/introduction-to-internet-of-things-iot-set-1/) devices in the field and translate between sensor protocols. They link user applications, cloud networks, and IoT devices.
* **VoIP Trunk Gateway:** By using a [VoIP (voice over Internet Protocol)](https://www.geeksforgeeks.org/voice-over-internet-protocol-voip/) network, it makes data transmission between POTS (plain old telephone service) devices like landlines and fax machines easier.

**How Gateways Work?**

* The gateway receives data from devices within the network.
* After receiving data the gateway intercept and analyze data packets, which include analyzing packet header, payload etc.
* Based on the analysis of the data packets, the gateway calculate an appropriate destination address of [data packet](https://www.geeksforgeeks.org/what-is-packet-sniffing/). It then routes the data packets to their destination address.
* In some cases, the gateway might also want to transform the format of the obtained data to ensure compatibility at the receiver.
* Once the data packets have been analyzed, routed, and converted, then the gateway sends the last packets to their respective destinations address inside the network.



*Gateways*

**Advantages of Gateways**

* Gateway helps in connecting two different network.
* Gateway is used to filters and does not allow anything that can harm to the network.
* Gateway is worked as the protocol converter.
* Gateway is the highly secure device that provides security from external attacks.

**Limitations of Gateways**

There are few limitations of gateways as well. Here are some of them:

* Gateway causes time delay since the conversion of data according to the network requires time.
* Failure of the gateway might lead to the failure of connection with other networks.
* The implementation of Gateway is very complex and it is not cost efficient.
* Gateway is hard to manage

**Network Devices:**Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example Repeater, Hub, Bridge, Switch, Routers, Gateway, Brouter, and NIC, etc.

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

Understanding network devices is key to mastering networking concepts, which are heavily tested in exams like GATE. To ensure you’re fully prepared, consider the [GATE CS Self-Paced Course](https://gfgcdn.com/tu/R8J/). This course offers in-depth coverage of networking topics, including detailed tutorials on the various network devices, helping you build the expertise needed to excel in your exams.

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

**Types of Hub**

* **Active Hub:-**These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
* **Passive Hub:-**These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can’t be used to extend the distance between nodes.
* **Intelligent Hub:-**It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

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

**Types of Bridges**

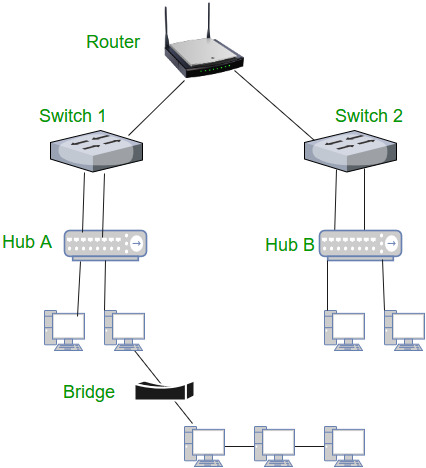
* **Transparent Bridges:-**These are the bridge in which the stations are completely unaware of the bridge’s existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
* **Source Routing Bridges:-**In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

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

**Types of  Switch**

1. Unmanaged switches: These switches have a simple plug-and-play design and do not offer advanced configuration options. They are suitable for small networks or for use as an expansion to a larger network.
2. Managed switches: These switches offer advanced configuration options such as VLANs, QoS, and link aggregation. They are suitable for larger, more complex networks and allow for centralized management.
3. Smart switches: These switches have features similar to managed switches but are typically easier to set up and manage. They are suitable for small- to medium-sized networks.
4. Layer 2 switches: These switches operate at the Data Link layer of the OSI model and are responsible for forwarding data between devices on the same network segment.
5. Layer 3 switches: These switches operate at the Network layer of the OSI model and can route data between different network segments. They are more advanced than Layer 2 switches and are often used in larger, more complex networks.
6. PoE switches: These switches have Power over Ethernet capabilities, which allows them to supply power to network devices over the same cable that carries data.
7. Gigabit switches: These switches support Gigabit Ethernet speeds, which are faster than traditional Ethernet speeds.
8. Rack-mounted switches: These switches are designed to be mounted in a server rack and are suitable for use in data centers or other large networks.
9. Desktop switches: These switches are designed for use on a desktop or in a small office environment and are typically smaller in size than rack-mounted switches.
10. Modular switches: These switches have modular design, which allows for easy expansion or customization. They are suitable for large networks and data centers.

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



What is Internet Connection?

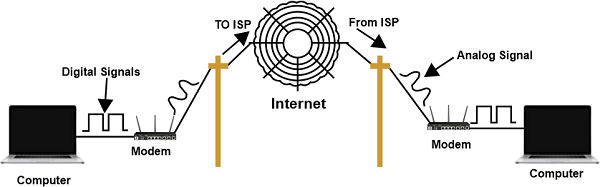
A user can connect to the Internet either by dialing into an ISP's computer or by directly connecting to the ISP. A dial-up connection is the one you initiate by dialing into a modem over a telephone link whereas a direct connection is a continuous connection to an ISP through a dedicated phone line.

**The various types of Internet connections are:**

* Dial-up connection
* Broad band connection

Cable TV Internet connections

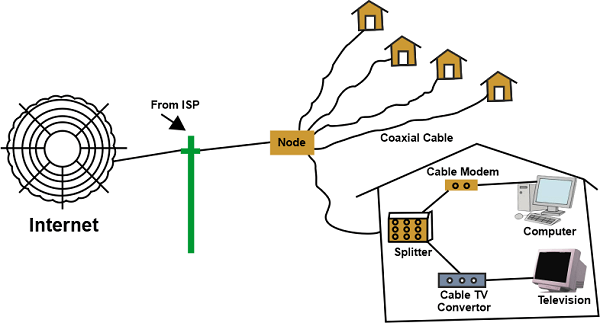
Satellite Internet Connections

* Wireless Internet Connections
* DIAL-UP CONNECTION
* A dial-up connection is one of the most common types of Internet connection offered by ISPS. This connection uses a telephone line to connect your computer to the Internet. In order to access using such a connection, a hardware device known as a modem is needed. A modem acts as an interface between your computer and a telephone line A communication program (such as Dial Up Networking) instructs the modem to place a telephone call to a specific phone number provided by an ISP, establish a connection and then connect your computer to the Internet.
* In dial-up connection, a connection is not always on. You connect only when you want to access the services provided by the Internet and when you are finished using it just disconnect.
* 
* The dial-up connection uses either the SLIP (Serial Line Internet Protocol) or PPP (Point to Point Protocol) protocols. However, most of the dial up connections are PPP protocol.
* Most ISPs support modems at a speed upto 56 kbps, so these basically used to read Emails and for Internet browsing. However, this type of connection has problems with video connections, high speed gaming and multimedia intensive websites. While using a dial up connection to access the Internet, you cannot talk on the phone. Thus a dial-up connection does not allow simultaneous talking and Internet access.
* **Advantages of Dial-up Connection:**
* It is fast enough to read information and download small files.
* It is easy to set up and most widely available Many ISPs provide this type of service.
* It is the cheapest form of Internet access in a limited way.
* Hardware cost in establishing such a connection is minimum.
* **Disadvantages of Dial-up connection:**
* Very slow connection You must wait several minutes for reading e-mails with large file attachments, viewing videos on the net, listening to music and appearance of web pages containing a lot of pictures, animations etc.
* Connection is not always You need to dial up every time you want to use Internet services.
* Using this connection, you cannot use the Internet and receive phone calls simultaneously. A busy signal will be received by the person who calls you.
* It is the slowest connection available, especially when multiple users on the network need to access the Internet.

CABLE TV INTERNET CONNECTION

Cable TV Internet Connection is a high speed Internet connection service provided through existing Cable TV lines. You can watch TV in a normal manner and at the same time access the Internet. It is one of the most widely growing services in homes because of its affordability and ease of use. The cable TV lines use the coaxial cable which transfers data at much higher speed than common telephone lines. Its speed usually ranges from 256 Kbps to 1 Mbps

In order to access this service, a cable modem is used which is provided by a Cable TV operator. A cable modem typically has two connections, one for the Internet service and other for the Cable TV signals. These modems are specially designed so that data transmission doesn't interfere with TV signals, making it possible to use both the services simultaneously.



Cable TV Internet connections share a set amount of bandwidth with a group of customers. So the data transfer speed available to a user depends upon how many customers are using the Internet at the same time. Data transfer speeds can be extremely fast when only a few customers are online but it reduces drastically as the number of customers online increases.

Cable TV Internet Services are far more available in residential communities than in business organizations.

**Advantages of Cable TV Internet Connection:**

1. Data transfer speed is very fast.
2. It provides continuous and instantaneous connectivity i.e. connection is always ON.
3. There is no internet login required and the user never gets busy signals as in case of dialup connection.

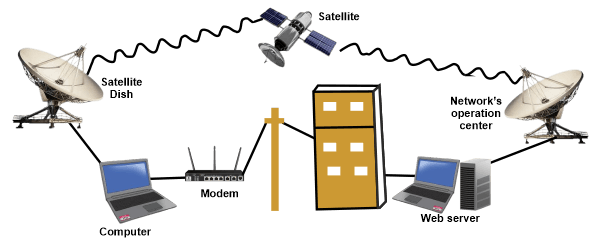
**Disadvantages of Cable TV Internet Connection:**

1. As the connection may be shared by multiple customers this may slow down the connection to the Internet during peak time.)
2. Only available in areas with Cable TV connections
3. Customers are not able to telecommunicate host websites, use video teleconferencing and many other bandwidth eating applications.
4. It is inexpensive as compared to other types of connections though.
5. Its initial cost may be high
6. Customers sharing the same cable network with other customers poses certain security risks such as unauthorized monitoring and hacking, denial of service etc.

SATELLITE INTERNET CONNECTION

Satellite Internet Connection offers yet another option for accessing the Internet. It is the most expensive alternative for getting a high speed connection to the Internet. These connections are aimed for those remote areas where other Internet connections such as dial-up. ISDN, DSL cannot be used.

Satellite Internet connection can either be a one way connection or a two way connection. In one way connection, you can only download data but in order to upload the data you need a dialup access through an ISP over telephone line. However, in a two way connection, downloads and uploads are done by the satellite without a need of dialup connection.



In order to use this connection, you need a satellite dish, a coaxial cable and communication software. In addition, we may also need a phone line and a dial-up Internet connection if the user has to upload also

**WIRELESS INTERNET CONNECTION or Direct connection**

With the recent advancement in wireless technology, the high speed Internet access is not limited to the desktop but it is now accessible on laptops, PDA's, mobiles also, Wireless Internet is the broadband Internet connection that use the radio frequency bands to connect to the Internet instead of using a telephone line or a cable network. This type of connection provides a very high speed, usually more than 10 Mbps and costs considerably less than the equivalent other wired versions. Its speeds range from 256 Kbps to 10 Mbps. It is possible to use this type of connection to transmit data over long distances. This type of connection is used by business travelers and persons who are away from home as long as they are within the network's coverage area.

**(wi-fi):** A number of ISP's have placed 802.11b (wi-fi) network standards in public places such as hostels, coffee shops, airports, convention centers. These networks provide easy access to the Internet for anyone with a compatible device (e.g. Laptop or PDA).

**Bluetooth:** It is also used for Internet access although it doesn't have the potential of wi-fi due to its limited distance. It was primarily promoted as it eliminated the need for cables between devices such as keyboard, computers, cellular phones, PDA's etc. The current standard allows upto 8 devices to be connected to it.

**IP addresses**

the computers of the world on the Internet network communicate with each other with underground or underwater cables or wirelessly. If I want to download a file from the internet or load a web page or literally do anything related to the internet, my computer must have an address so that other computers can find and locate mine in order to deliver that particular file or webpage that I am requesting. In technical terms, that address is called **IP Address or Internet Protocol Address**.

Let us understand it with another example, like if someone wants to send you a mail then he/she must have your home address. Similarly, your computer too needs an address so that other computers on the internet can communicate with each other without the confusion of delivering information to someone else’s computer. And that is why each computer in this world has a unique IP Address. Or in other words, an IP address is a unique address that is used to identify computers or nodes on the internet. This address is just a string of numbers written in a certain format. It is generally expressed in a set of numbers for example 192.155.12.1. Here each number in the set is from 0 to 255 range. Or we can say that a full IP address ranges from 0.0.0.0 to 255.255.255.255. And these IP addresses are assigned by IANA(known as Internet Corporation For Internet Assigned Numbers Authority).

But what is Internet protocol? This is just a set of rules that makes the internet work. You are able to read this article because your computer or phone has a unique address where the page that you requested (to read this article from GeeksforGeeks) has been delivered successfully.

**Working of IP addresses**

The working of IP addresses is similar to other languages. It can also use some set of rules to send information. Using these protocols we can easily send, and receive data or files to the connected devices. There are several steps behind the scenes. Let us look at them

* Your device directly requests your Internet Service Provider which then grants your device access to the web.
* And an IP Address is assigned to your device from the given range available.
* Your internet activity goes through your service provider, and they route it back to you, using your IP address.
* Your IP address can change. For example, turning your router on or off can change your IP Address.
* When you are out from your home location your home IP address doesn’t accompany you. It changes as you change the network of your device.

**Types of IP Address**

IP Address is of two types:

**1. IPv4:**Internet Protocol version 4. It consists of 4 numbers separated by the dots. Each number can be from 0-255 in decimal numbers. But computers do not understand decimal numbers, they instead change them to binary numbers which are only 0 and 1. Therefore, in binary, this (0-255) range can be written as (00000000 – 11111111). Since each number N can be represented by a group of 8-digit binary digits. So, a whole IPv4 binary address can be represented by 32-bits of binary digits. In IPv4, a unique sequence of bits is assigned to a computer, so a total of (2^32) devices approximately = 4,294,967,296 can be assigned with IPv4.

IPv4 can be written as:

*189.123.123.90*

**Classes of IPv4 Address:** There are around 4.3 billion IPv4 addresses and managing all those addresses without any scheme is next to impossible. Let’s understand it with a simple example. If you have to find a word from a language dictionary, how long will it take? Usually, you will take less than 5 minutes to find that word. You are able to do this because words in the dictionary are organized in alphabetical order. If you have to find out the same word from a dictionary that doesn’t use any sequence or order to organize the words, it will take an eternity to find the word. If a dictionary with one billion words without order can be so disastrous, then you can imagine the pain behind finding an address from 4.3 billion addresses. For easier management and assignment IP addresses are organized in numeric order and divided into the following 5 classes :

| **IP Class** | **Address Range** | **Maximum number of networks** |
| --- | --- | --- |
| Class A | 1-126 | 126 (27-2) |
| Class B | 128-191 | 16384 |
| Class C | 192-223 | 2097152 |
| Class D | 224-239 | Reserve for multitasking |
| Class E | 240-254 | Reserved for Research and development |

The 0.0.0.0 is a[Non-routable address](https://www.geeksforgeeks.org/difference-between-127-0-0-1-and-0-0-0-0/) is  that indicates an invalid, or inapplicable end-user address.

A [loopback address](https://www.geeksforgeeks.org/what-is-a-loopback-address/) is a distinct reserved IP address range that starts from 127.0.0.0 ends at 127.255.255.255 though 127.255.255.255 is the broadcast address for 127.0.0.0/8. The loopback addresses are built into the IP domain system, enabling devices to transmit and receive the data packets. The loopback address 127.0.0.1 is generally known as localhost.

**2. IPv6:**But, there is a problem with the IPv4 address. With IPv4, we can connect only the above number of 4 billion devices uniquely, and apparently, there are much more devices in the world to be connected to the internet. So, gradually we are making our way to **IPv6 Address**which is a 128-bit IP address. In human-friendly form, IPv6 is written as a group of 8 hexadecimal numbers separated with colons(:). But in the computer-friendly form, it can be written as 128 bits of 0s and 1s. Since, a unique sequence of binary digits is given to computers, smartphones, and other devices to be connected to the internet. So, via IPv6 a total of (2^128) devices can be assigned with unique addresses which are actually more than enough for upcoming future generations.

IPv6 can be written as:

*2011:0bd9:75c5:0000:0000:6b3e:0170:8394*

**Classification of IP Address**

An IP address is classified into the following types:

**1. Public IP Address:** This address is available publicly and it is assigned by your network provider to your router, which further divides it to your devices. Public IP Addresses are of two types,

* **Dynamic IP Address:**When you connect a smartphone or computer to the internet, your Internet Service Provider provides you an IP Address from the range of available IP Addresses. Now, your device has an IP Address and you can simply connect your device to the Internet and send and receive data to and from your device. The very next time when you try to connect to the internet with the same device, your provider provides you with different IP Addresses to the same device and also from the same available range. Since IP Address keeps on changing every time when you connect to the internet, it is called a Dynamic IP Address.
* **Static IP Address:**Static address never changes. They serve as a permanent internet address. These are used by DNS servers. What are DNS servers? Actually, these are computers that help you to open a website on your computer. Static IP Address provides information such as device is located on which continent, which country, which city, and which Internet Service Provider provides internet connection to that particular device. Once, we know who is the ISP, we can trace the location of the device connected to the internet. Static IP Addresses provide less security than Dynamic IP Addresses because they are easier to track.

**2. Private IP Address:** This is an internal address of your device which are not routed to the internet and no exchange of data can take place between a private address and the internet.

**3. Shared IP addresses:**Many websites use shared IP addresses where the traffic is not huge and very much controllable, they decide to rent it to other similar websites so to make it cost-friendly. Several companies and email sending servers use the same IP address (within a single mail server) to cut down the cost so that they could save for the time the server is idle.

**4. Dedicated IP addresses:**A dedicated IP Address is an address used by a single company or an individual which gives them certain benefits using a private Secure Sockets Layer (SSL) certificate which is not in the case of a shared IP address. It allows to access the website or log in via File Transfer Protocol (FTP) by IP address instead of its domain name. It increases the performance of the website when the traffic is high. It also protects from a shared IP address that is black-listed due to spam

**URL**

A URL (Uniform Resource Locator, also called a *web address*) is a unique identifier used to locate a resource on the internet. URLs consist of multiple parts -- including a protocol and domain name -- that tell web browsers how and where to retrieve a resource.

End users use URLs by typing them directly into a browser address bar or by clicking a hyperlink found on a webpage, bookmark list, email or another application.

**How is a URL structured?**

The URL contains the name of the [protocol](https://www.techtarget.com/searchnetworking/definition/protocol) needed to access a resource, as well as a resource name. The first part of a URL identifies what protocol to use as the primary access medium. The second part identifies the [IP address](https://www.techtarget.com/whatis/definition/IP-address) or domain name -- and possibly subdomain -- where the resource is located.

URL protocols include [HTTP](https://www.techtarget.com/whatis/definition/HTTP-Hypertext-Transfer-Protocol) (Hypertext Transfer Protocol) and [HTTPS](https://www.techtarget.com/searchsoftwarequality/definition/HTTPS) (HTTP Secure) for web resources, mailto for email addresses, FTP for files on a File Transfer Protocol server and telnet for a session to access remote computers. A colon and two forward slashes follow most URL protocols, but only a colon follows the mailto protocol.

URLs can also specify the following optional information after the domain:

* A path to a specific page or file within a domain.
* A network [port](https://www.techtarget.com/searchnetworking/definition/port) to use to make the connection.
* A specific reference point within a file, such as a named anchor in an HTML file.
* A query or search parameters used -- commonly found in URLs for search results.

**Importance of URL design**

URLs can only be sent over the internet using the [ASCII](https://www.techtarget.com/whatis/definition/ASCII-American-Standard-Code-for-Information-Interchange) character set. Because URLs often contain non-ASCII characters, the URL must convert into a valid ASCII format. URL encoding replaces unsafe ASCII characters with a percent sign (%) followed by two hexadecimal digits. URLs cannot contain spaces.

**URL examples**

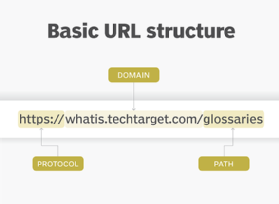
When designing URLs, there are different theories about how to make the syntax most usable for readers and archivists. For example, the URL's path can include dates, authors and topics in a section referred to as the *slug*. Consider the URL for this definition:

**https://www.techtarget.com/searchnetworking/definition/URL**

Look past the HTTPS protocol and the permalink (www.techtarget.com). The file includes two paths (*searchnetworking* and *definition*) and the definition title (*URL*). Though not present in this example, some URL designers choose to add the date of the post, usually as YYYY/MM/DD.

**Parts of a URL**

Using the URL **https://www.techtarget.com/whatis/search/query?q=URL** as an example, components of a URL can include the following:



* **The protocol or scheme.** This is used to access a resource on the internet. Protocols include http, https, ftps, mailto and file. The [domain name system](https://www.techtarget.com/searchnetworking/definition/domain-name-system) name reaches the resource. In this example, the protocol is https.
* **Host name or domain name.** This is the unique reference that represents a webpage. For this example, it is techtarget.com.
* **Subdomain.**This precedes the main domain name. In this case, "www" denotes the Word Wide Web. Other subdomain options include "blog," "mail" and "support."
* **Port name.** These usually aren't visible in URLs, but they're necessary. Ports 80 and 443 are the default ports for web servers, but there are other options. In a URL, ports always follow a colon. For this example, https://www.techtarget.com:443.
* **Path.** A path refers to a file or location on the web server. For this example, the path is whatis/search/query.
* **Query.** Found in the URL of dynamic pages, the query consists of a question mark, followed by parameters or the query string. In this example, "?" marks the beginning of the query.
* **Parameters.** These are pieces of information in a query string of a URL. Multiple parameters can be separated by ampersands (&). In this example, the parameter is "q=URL."
* **Fragment.** This is an internal page reference, which refers to a section within the webpage. It appears at the end of a URL and begins with a pound sign (#). Although not in the example above, an example could be #history in the URL https://en.wikipedia.org/wiki/Internet#History.

Other examples of parts of a URL can include the following:

* The URL **mailto:president@whitehouse.gov** initiates a new email addressed to the mailbox "president" in the whitehouse.gov domain.
* The URL **ftp://www.companyname.com/whitepapers/widgets.ps** specifies FTP use to download a file.

**HTTP vs. HTTPS**

Computers use both HTTP and HTTPS to retrieve data from web servers to view content in a browser. One difference between them is that HTTPS uses a [Secure Sockets Layer](https://www.techtarget.com/searchsecurity/definition/Secure-Sockets-Layer-SSL) certificate to encrypt the end-user and server connection. Another difference is that HTTPS uses [TCP/IP](https://www.techtarget.com/searchnetworking/definition/TCP-IP) port number 443 by default, whereas HTTP uses port 80.

**ISP**

**ISP** stands for **Internet Service Provider** which is a term used to refer to a company that provides internet access to people who pay the company or subscribe to the company for the same. For their services, the customers have to pay the internet service provider a nominal fee which varies according to the amount of data they actually use or the data plan which they purchase. An Internet Service Provider is also known as an Internet Access Provider or an online service provider. An Internet Service Provider is a must if one wants to connect to the Internet.

**History**

The first Internet Service Provider was [Telenet](https://www.geeksforgeeks.org/introduction-to-telnet/" \t "_blank). Telenet was the commercialized version of the [ARPANET](https://www.geeksforgeeks.org/arpanet-full-form/) – a precursor to the internet, of sorts. Telenet was introduced in 1974. Since then, many Internet Service Providers have entered the scene and this was partly because of the proliferation of the internet as a commodity that fuelled the consumerist attitude of the people. Pretty soon, an Internet Service Provider called “The World” came to be in vogue and ever since it started serving its customers today in 1989 has cemented itself as the first archetypal Internet Service Provider. Examples of major Internet Service Providers include Google Fiber, Verizon, Jio, AT&T etc.

**Characteristics**

* **E-mail Account:** Many Internet Service Providers offer an e-mail address to their consumers.
* **User Support:** Professionals and an increasing number of lay users prefer an ISP that can provide them with customer support so that they have someone they can refer to if things go awry.
* **Access to High-Speed Internet:** Probably the most obvious item on this list as this feature of an Internet Service Provider lies literally in its name. Furthermore, the higher the speed an Internet Service Provider can offer one, the better it’s standing in the market and the more customers it can attract.
* **Spam Blocker:** An Internet Service Provider that hinders its customers’ productivity by way of not blocking [spam](https://www.geeksforgeeks.org/protection-against-spam/) and displaying frequent ads is not something that is generally favoured in the market today. Therefore, many of the Internet Service Providers offer spam blocking features to their customers.
* **Web Hosting:** Some of the ISPs offer web hosting services to their clientele as well.

**Different Types of ISP Connections**

* DSL
* Wi-Fi broadband
* mobile broadband
* fibre optic broadband
* cable broadband

Networks are crucial in today’s globalized world because they allow the acquisition, exchange, and organization of knowledge. Of all the first order networks the Internet, Intranet, and Extranet are commonly utilized for various applications. Every network type meets specific roles that are required in connecting the global population, and internal organization, and secure communication with external subjects. About these networks, this article will aim at identifying their fundamental and specific applications.

**What is the Internet?**

The Internet is a huge network of millions of computers and related devices from all corners of the globe through which users are able to communicate, exchange information, and partake in general resources. Its mechanism is more decentralized and does not have a specific owner; it works only as a common idea shared by various institutions, governments, and users. The Internet is the tool that links people, companies, and organizations, offering various opportunities for cooperation and development, as well as offering various possibilities to find the necessary information, using Internet resources, such as websites and services, research data, and social networks.

**What is an Intranet?**

An Intranet is a local area network that has been designed for use within an organization by its employees to share information as well as work together. An Intranet is also constructed from the technologies of the Internet from [TCP/IP](https://www.geeksforgeeks.org/tcp-ip-model/), [HTTP](https://www.geeksforgeeks.org/http-full-form/), and web browsers but exist behind a security firewall and has only a limited number of authorized users. Its use is to enhance the cooperation internally, control the distribution of facilities and to work more effectively. These include company news that include the latest updates posted internally to and including personnel directories, project management applications and access to databases all of which assist the organization in enhancing its efficiency.

**What is Extranet ?**

An Extranet is an extended form of an Intranet that enables secure communication and collaboration between an organization and external entities, such as suppliers, partners, or clients. While it uses Internet protocols to facilitate connectivity, an Extranet is controlled and accessible only to authorized users with login credentials. The primary purpose of an Extranet is to extend the reach of internal resources to trusted external users while maintaining security through firewalls, [encryption](https://www.geeksforgeeks.org/what-is-data-encryption/), and access control measures.

**Difference between Internet, Intranet and Extranet**

| **Point of difference** | **Internet** | **Intranet** | **Extranet** |
| --- | --- | --- | --- |
| **Accessibility of network** | Public | Private | Private |
| **Availability** | Global system. | Specific to an organization. | To share information with suppliers and vendors it makes the use of public network. |
| **Coverage** | All over the world. | Restricted area upto an organization. | Restricted area upto an organization and some of its stakeholders or so. |
| **Accessibility of content** | It is accessible to everyone connected. | It is accessible only to the members of organization. | Accessible only to the members of organization and external members with logins. |
| **No. of computers connected** | It is largest in number of connected devices. | The minimal number of devices are connected. | The connected devices are more comparable with Intranet. |
| **Owner** | No one. | Single organization. | Single/ Multiple organization. |
| **Purpose of the network** | It’s purpose is to share information throughout the world. | It’s purpose is to share information throughout the organization. | It’s purpose is to share information between members and external, members. |
| **Security** | It is dependent on the user of the device connected to network. | It is enforced via firewall. | It is enforced via firewall that separates internet and extranet. |
| **Users** | General public. | Employees of the organization. | Employees of the organization which are connected. |
| **Policies behind setup** | There is no hard and fast rule for policies. | Policies of the organization are imposed. | Policies of the organization are imposed. |
| **Maintenance** | It is maintained by ISP. | It is maintained by CIO. HR or communication department of an organization. | It is maintained by CIO. HR or communication department of an organization. |
| **Economical** | It is more economical to use. | It is less economical. | It is also less economical. |
| **Relation** | It is the network of networks. | It is derived from Internet. | It is derived from Intranet. |
| **Example** | What we are normally using is internet. | WIPRO using internal network for its business operations. | DELL and Intel using network for its business operations. |

**VPN**

VPN stands for **"Virtual Private Network"** and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in **real time**.

**How does a VPN work?**

A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host. This means that if you surf online with a VPN, the VPN server becomes the source of your data. This means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online. A VPN works like a filter that turns all your data into "gibberish". Even if someone were to get their hands on your data, it would be useless.

**What are the benefits of a VPN connection?**

A VPN connection disguises your data traffic online and protects it from external access. Unencrypted data can be viewed by anyone who has network access and wants to see it. With a VPN, hackers and cyber criminals can’t decipher this data.

**Secure encryption:** To read the data, you need an *encryption key* . Without one, it would take millions of years for a computer to decipher the code in the event of a [brute force attack](https://www.kaspersky.com/resource-center/definitions/brute-force-attack) . With the help of a VPN, your online activities are hidden even on public networks.

**Disguising your whereabouts** : VPN servers essentially act as your proxies on the internet. Because the demographic location data comes from a server in another country, your actual location cannot be determined. In addition, most VPN services do not store logs of your activities. Some providers, on the other hand, record your behavior, but do not pass this information on to third parties. This means that any potential record of your user behavior remains permanently hidden.

**Access to regional content:** Regional web content is not always accessible from everywhere. Services and websites often contain content that can only be accessed from certain parts of the world. Standard connections use local servers in the country to determine your location. This means that you cannot access content at home while traveling, and you cannot access international content from home. With **VPN location spoofing** , you can switch to a server to another country and effectively “change” your location.

**Secure data transfer:** If you work remotely, you may need to access important files on your company’s network. For security reasons, this kind of information requires a secure connection. To gain access to the network, a VPN connection is often required. VPN services connect to private servers and use encryption methods to reduce the risk of data leakage.

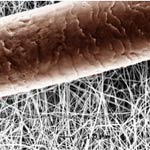
**Why should you use a VPN connection?**

Your ISP usually sets up your connection when you connect to the internet. It tracks you via an IP address. Your network traffic is routed through your ISP's servers, which can log and display everything you do online.

Your ISP may seem trustworthy, but it may share your browsing history with advertisers, the police or government, and/or other third parties. ISPs can also fall victim to attacks by cyber criminals: If they are hacked, your personal and private data can be compromised.

This is especially important if you regularly connect to public Wi-Fi networks. You never know who might be monitoring your internet traffic and what they might steal from you, including passwords, personal data, payment information, or even your entire identity.

**What is nanotechnology?**

*  
A human hair is approximately 80 000 nm wide*

[Nanotechnology](https://ec.europa.eu/health/scientific_committees/opinions_layman/glossary/mno/nanotechnology.htm) refers to the branch of science and engineering devoted to designing, producing, and using structures, devices, and systems by manipulating [atoms](https://ec.europa.eu/health/scientific_committees/opinions_layman/glossary/abc/atom.htm) and [molecules](https://ec.europa.eu/health/scientific_committees/opinions_layman/glossary/mno/molecule.htm) at [nanoscale](https://ec.europa.eu/health/scientific_committees/opinions_layman/glossary/mno/nanoscale.htm), i.e. having one or more dimensions of the order of 100 [nanometres](https://ec.europa.eu/health/scientific_committees/opinions_layman/glossary/mno/nanometre.htm) (100 millionth of a millimetre) or less.

In the natural world, there are many examples of structures with one or more [nanometre](https://ec.europa.eu/health/scientific_committees/opinions_layman/glossary/mno/nanometre.htm) dimensions, and many technologies have incidentally involved such [nanostructures](https://ec.europa.eu/health/scientific_committees/opinions_layman/glossary/mno/nanostructure.htm) for many years, but only recently has it been possible to do it intentionally.

Many of the applications of [nanotechnology](https://ec.europa.eu/health/scientific_committees/opinions_layman/glossary/mno/nanotechnology.htm) involve new materials that have very different properties and new effects compared to the same materials made at larger sizes. This is due to the very high surface to volume ratio of [nanoparticles](https://ec.europa.eu/health/scientific_committees/opinions_layman/glossary/mno/nanoparticle.htm) compared to larger particles, and to effects that appear at that small scale but are not observed at larger scales.

The applications of [nanotechnology](https://ec.europa.eu/health/scientific_committees/opinions_layman/glossary/mno/nanotechnology.htm) can be very beneficial and have the potential to make a significant impact on society. Nanotechnology has already been embraced by industrial sectors, such as the information and communications sectors, but is also used in food technology, energy technology, as well as in some medical products and medicines. [Nanomaterials](https://ec.europa.eu/health/scientific_committees/opinions_layman/glossary/mno/nanomaterial.htm) may also offer new opportunities for the reduction of environmental pollution.

But these new materials may also present new health risks. Humans have developed mechanisms of protection against various environmental agents of different sizes. However, until recently, they had never been [exposed](https://ec.europa.eu/health/scientific_committees/opinions_layman/glossary/def/exposure-exposed-expose.htm) to synthetic [nanoparticles](https://ec.europa.eu/health/scientific_committees/opinions_layman/glossary/mno/nanoparticle.htm) and their specific characteristics. Therefore the normal human defence mechanisms associated with, for example, [immune](https://ec.europa.eu/health/scientific_committees/opinions_layman/glossary/ghi/immune-system.htm) and [inflammatory](https://ec.europa.eu/health/scientific_committees/opinions_layman/glossary/ghi/inflammation.htm) systems may well not be able to respond adequately to these nanoparticles. In addition, nanoparticles may also disperse and persist in the environment, and therefore have an impact on the environment.

As far as health risks are concerned, there are two types of [nanostructure](https://ec.europa.eu/health/scientific_committees/opinions_layman/glossary/mno/nanostructure.htm) to consider:

* those where the structure itself is a free particle, called free [nanoparticles](https://ec.europa.eu/health/scientific_committees/opinions_layman/glossary/mno/nanoparticle.htm), which is the group of greater concern; and
* those where the [nanostructure](https://ec.europa.eu/health/scientific_committees/opinions_layman/glossary/mno/nanostructure.htm) is an integral part of a larger object, for instance, materials with coatings composed of [nanomaterials](https://ec.europa.eu/health/scientific_committees/opinions_layman/glossary/mno/nanomaterial.htm). However, as long as the nanoparticles are fixed to the carrier, there is no reason to suppose that they pose a greater risk for health or the environment than the larger scale materials.

**internet security**

**What are the most common internet security threats?**

To ensure privacy and security on the internet, it’s important to be aware of different types of internet attacks. Common internet security threats include:

**Phishing**

[Phishing](https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips) is a cyber-attack involving disguised emails. Hackers try to trick email recipients into believing that a message is genuine and relevant – a request from their bank or a note from a co-worker, for example – so that they click on a link or open an attachment. The goal is to deceive people into handing over their personal information or downloading malware.

Phishing is one of the oldest internet security threats, dating back to the 1990s. It has remained popular to this day since it is one of the cheapest and easiest ways for criminals to steal information. In recent years, phishing techniques and messages have become increasingly sophisticated.

**Hacking and remote access**

Hackers are always looking to exploit a private network or system's vulnerabilities so they can steal confidential information and data. Remote access technology gives them another target to exploit. Remote access software allows users to access and control a computer remotely – and since the pandemic, with more people working remotely, its usage has increased.

The protocol which allows users to control a computer connected to the internet remotely is called Remote Desktop Protocol, or RDP. Because businesses of all sizes so widely use RDP, the chances of an improperly secured network are relatively high. Hackers use different techniques to exploit RDP vulnerabilities until they have full access to a network and its devices. They may carry out data theft themselves or else sell the credentials on the dark web.

**Malware and malvertising**

[Malware](https://www.kaspersky.com/resource-center/threats/malware-protection) is a portmanteau of "malicious" and "software". It's a broad term related to viruses, worms, trojans, and other harmful programs that hackers use to cause havoc and steal sensitive information. Any software intended to damage a computer, server, or network can be described as malware.

Malvertising is a portmanteau of “malicious” and “advertising”. The term refers to online advertising, which distributes malware. Online advertising is a complex ecosystem involving publisher websites, ad exchanges, ad servers, retargeting networks, and content delivery networks. Malvertisers exploit this complexity to place malicious code in places that publishers and ad networks don’t always detect. Internet users who interact with a malicious ad could download malware onto their device or be redirected to malicious websites.

**Ransomware**

[Ransomware](https://www.kaspersky.com/resource-center/threats/ransomware-examples) is a type of malware that prevents you from using your computer or accessing specific files on your computer unless a ransom is paid. It is often distributed as a trojan – that is, malware disguised as legitimate software. Once installed, it locks your system’s screen or certain files until you pay.

Because of their perceived anonymity, ransomware operators typically specify payment in cryptocurrencies such as [Bitcoin](https://www.kaspersky.com/resource-center/definitions/what-is-bitcoin). Ransom prices vary depending on the ransomware variant and the price or exchange rate of digital currencies. It isn’t always the case that if you pay, the criminals will release the encrypted files.

Ransomware attacks are on the rise, and new ransomware variants continue to emerge. Some of the most talked-about ransomware variants include [Maze](https://www.kaspersky.com/resource-center/definitions/what-is-maze-ransomware), Conti, GoldenEye, Bad Rabbit, Jigsaw, Locky, and [WannaCry](https://www.kaspersky.com/resource-center/threats/ransomware-wannacry).

**Botnets**

The term [botnet](https://www.kaspersky.com/resource-center/threats/botnet-attacks) is a contraction of “robot network”. A botnet is a network of computers that have been intentionally infected by malware so they can carry out automated tasks on the internet without the permission or knowledge of the computers’ owners.

Once a botnet’s owner controls your computer, they can use it to carry out malicious activities. These include:

* Generating fake internet traffic on third party websites for financial gain.
* Using your machine’s power to assist in Distributed Denial of Service (DDoS) attacks to shut down websites.
* Emailing spam to millions of internet users.
* Committing fraud and identity theft.
* Attacking computers and servers.

Computers become part of a botnet in the same ways that they are infected by any other type of malware – for example, opening email attachments that download malware or visiting websites infected with malware. They can also spread from one computer to another via a network. The number of bots in a botnet varies and depends on the ability of the botnet owner to infect unprotected devices.

**Wi-Fi threats, in public and at home**

[Public Wi-Fi carries risks](https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks) because the security on these networks – in coffee shops, shopping malls, airports, hotels, restaurants, and so on – is often lax or non-existent. The lack of security means that cybercriminals and identity thieves can monitor what you are doing online and steal your passwords and personal information. Other public Wi-Fi dangers include:

* **Packet sniffing** – attackers monitor and intercept unencrypted data as it travels across an unprotected network.
* **Man-in-the-middle-attacks** – attackers compromise a Wi-Fi hotspot to insert themselves into communications between the victim and the hotspot to intercept and modify data in transit.
* **Rogue Wi-Fi networks** – attackers set up a [honeypot](https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot) in the form of free Wi-Fi to harvest valuable data. The attacker’s hotspot becomes the conduit for all data exchanged over the network.

You don't have to worry so much about someone spying on the Wi-Fi network at home because you own the network hardware. But there are still threats – in the US, [internet service providers (ISPs) are allowed to sell data about their users](https://uk.pcmag.com/fastest-isps/88516/trump-officially-hands-control-of-your-data-to-isps). While the data is anonymized, it can still be an unsettling thought for those who value privacy and security on the internet. A VPN at home makes it much harder for outsiders to correlate your online activity to you.

**How to protect your data online**

If you are wondering how to ensure internet protection and how to protect your data online, sensible internet security tips you can follow include:

**Enable multifactor authentication wherever you can**

Multifactor authentication (MFA) is an authentication method that asks users to provide two or more verification methods to access an online account. For example, instead of simply asking for a username or password, multifactor authentication goes further by requesting additional information, such as:

* An extra one-time password that the website's authentication servers send to the user's phone or email address.
* Answers to personal security questions.
* A fingerprint or other biometric information, such as voice or [face recognition](https://www.kaspersky.com/resource-center/definitions/what-is-facial-recognition).

Multifactor authentication decreases the likelihood of a successful cyber-attack. To make your online accounts more secure, it is a good idea to implement multifactor authentication where possible. You can also consider using a third-party authenticator app, such as Google Authenticator and Authy, to help with internet security.

**Use a firewall**

A [firewall](https://www.kaspersky.com/resource-center/definitions/firewall) acts as a barrier between your computer and another network, such as the internet. Firewalls block unwanted traffic and can also help to block malicious software from infecting your computer. Often, your operating system and security system come with a pre-installed firewall. It is a good idea to make sure those features are turned on, with your settings configured to run updates automatically, to maximize internet security.

**Choose your browser carefully**

Our browsers are our primary gateway to the web and therefore play a key role in internet security. A good web browser should be secure and help to protect you from data breaches. The Freedom of the Press Foundation has compiled [a detailed guide here, explaining the security pros and cons of the leading web browsers on the market](https://freedom.press/training/-depth-guide-choosing-web-browser/).

**Create strong passwords, and use a secure password manager**

[A strong password](https://www.kaspersky.com/resource-center/threats/how-to-create-a-strong-password) will help you maintain internet security. A strong password is:

* Long – made up of at least 12 characters and ideally more.
* A mix of characters – that is, upper- and lower-case letters plus symbols and numbers.
* Avoids the obvious – such as using sequential numbers (“1234”) or personal information that someone who knows you might guess, such as your date of birth or a pet’s name.
* Avoids memorable keyboard paths.

These days, it’s no longer enough to substitute lookalike characters for letters or numbers – for example, “P@ssw0rd” for “password” – since hackers are wise to it. The more complex and involved your password, the harder it is to crack. Using a [password manager](https://www.kaspersky.com/password-manager) will help – by generating, storing, and managing all your passwords in one secure online account.

Keep your passwords private – avoid sharing them with others or writing them down. Try to avoid using the same password for all your accounts and remember to change them regularly.

**Keep an up-to-date security program installed on your devices**

Internet security antivirus is critical for ensuring privacy and security online. The best internet security software protects you from different types of internet attacks and protects your data online. It’s important to keep antivirus software up to date – most modern programs update themselves automatically to stay on top of the latest internet security threats.

**How to keep your family safe online**

Internet security for kids is critical – protecting children from harmful or inappropriate content and contacts, as well as malicious software or attacks. [Teaching your children online safety tips](https://www.kaspersky.com/resource-center/preemptive-safety/kids-online-safety) can help to keep them safe.

**Internet safety tips for children**

Children are spending more and more time online, and it’s important to talk to them about how to stay safe on the internet. Making sure that kids know what information to keep private online is essential, for example explaining why they need to keep their passwords private, and not give out personal information. Keeping the computer in a common area, where you can watch and monitor its use, can also be a useful way of ensuring children use the internet safely.

Many kids enjoy watching YouTube videos. So, to make this a safer experience, you can use YouTube parental controls. You may also want to use YouTube’s dedicated app for children, YouTube Kids. This provides a more child-friendly interface, and videos on the app are reviewed by a combination of human moderators and automated filters to help ensure videos are appropriate for younger children.

**What is a Website?**

When we google ‘website’, the very first definition we get from a reliable source such as Wikipedia is, ‘a website is a collection of related web pages, including multimedia content, typically identified with a common domain name, and published on at least one web server.’ To explain it further it is an interlinked collection of web pages grouped in various ways and together called a website or simply a site.

However still there is a lot of confusion, isn’t it? You might now ask what is a webpage? What is a web server? What is a domain name? etc. To drown out your confusion, a webpage is a document(page) or a hypertexted document connected to the World Wide Web and can be displayed on a web browser like Chrome, Firefox, Internet Explorer, Edge, Safari, Opera, Bing, and others. A web server is a computer that hosts the collection of web pages interlinked together or in one term we can say the website on the internet, on an identification string named as a domain name.

Moving on further, for once since you have got a little idea of what is website lets start by finding why a website is made and why it is so essential part of a business journey, in short here are some of the functions of a website that will help you understand its participation in an online business.

**Functions of Websites:**

* **Tell Your Story:** A website gives you the power to tell your clients about your services and products and help you engage them in long interactions to convince them to choose your company.
* **Answer FAQs:** Websites help you resolve confusion or questions asked by new clients that further can also become your most potent client base. Thus, including these questions on your website help you attract a better client force while reducing your and your client’s time.
* **Provide Clear Contact Details:** The contact us page on your website is a gateway to better client force, it allows your clients to investigate details about various ways to contact you like your email address, your office address, phone number, etc. Quit traditional ways now to help your business reach out to your clients on a platform that is highly trusted by everyone.
* **Build Credibility** Build your website with a lot of professional edges, choose themes, and functions, and allow your websites to say it all about your products, services, your policies, and your partnership and membership. You can also include a portfolio on your website that makes your clients rely more on you.
* **Expand Your Client Base:**With website and SEO activities you can increase your business visibility and create a good deal of client awareness around the globe.
* **Process of Website Development**The right way of building a website or the web development company approach gives a lot of definition to your development. The right way to build a good website includes the following steps: 1. Information gathering 2. Planning 3. Brainstorming 4. Content Writing 5. Coding 6. Testing, Review, and Launch.
* **Languages and Frameworks prominently used in developing websites:**Our technology and web development world from the very beginning has seen the emergence and downfall of many web development languages and frameworks, of which some still prevail and rule while some have become history. Some of the most prominently used old, new, and contemporary languages and frameworks are 1. Java 2. Ruby 3. Python 4. PHP 5. CSS etc.

These are some of the most widely used languages, but that’s not all they have different frameworks which make the development of different types of websites easy. Some of them are 1. Django 2. Ruby on Rails 3. Symfony 4. Laravel 5. Bootstrap 6. CakePHP 7. Zend 8. CodeIgniter etc. You see the most widely used and trusted language is PHP which is recommended by many development companies and developers.

**What is Web Portal?**

This might come as confusion, but Web Portal is a specially designed website that provides information catered from various sources such as emails, online forums, and search engines on one platform, uniformly. It is a personalized and customized library that helps in the navigation and personalization of notifications that provide well-integrated information from diverse sources with advanced features such as task management, collaboration, business intelligence, etc.

**Functions of Web Portal**

* **Upgrading your website** Web Portal development helps you in improving the capability of the web pages that help you deliver quality information, thus a web portal is the new world toolset that makes the implementation of information better and behaves as a different communication approach.
* **Improves Relations immensely** It helps in enhanced customer-company relations as it helps in improving their customer relations by providing high-end and filtered information on a user-friendly and comprehensive platform.
* Domain-Specific Domain-Specific development of web portals helps you attract the users that seek information and services on that domain. Thus, helping you attract a particular area of domain.
* **Interaction**When done efficiently web portal design services help you a lot in interacting better with your customers and clients. They help you make your web pages very interactive and target better to your audience.
* **Process of web portal designing services** Web portal development and designing is a complex art as its functionality is highly difficult to render. The complex process of web portal development includes similar steps to website development. However, the difference is in its features, functionality, coding, testing, and integration. Since we have covered the features and functionality let’s start with the languages and frameworks that are used dominantly in web portal development services by eminent web portal development companies and web portal developers.
* **Languages and Frameworks prominently used in developing web portals** Since web portals are differently designed websites, the languages are similar that those used in building and web designing services in website development. Thus, the top 10 frameworks that we use in building web portals are 1. AngularJS 2. Laravel 3. React.JS 4. NodeJS 5. Ruby on Rails 6. Symfony 7. Asp.Net 8. Yii 9. Metor.JS and 10. CakePHP.

**Now The difference between a Website and a Web portal**

Websites and web portals thus can be differentiated in different aspects, firstly websites are majorly focused on driving traffic while web portals are for limiting the traffic. Whereas the web portals require users to log in while websites are open to being visited by any individual.

Thus, on differentiating it based on its uses, a web portal is creating and attracting a specific audience experience, controlling users’ functionality on your page, multiple source integrations to provide uniform information, and other user management and permitting features.

| **S. No.** | **Website** | **Web portal** |
| --- | --- | --- |
| 1. | Location on the internet, publicly accessible with a unique URL(Web Address) | A private location on the internet it can be accessible with a unique URL and unique username and password |
| 2. | No requirement for any login | Login required |
| 3. | Anyone can visit and can see the content of the website. | The only members of the web portal having access can see the content of the web portal. |
| 4. | The content type is the same for all users. | The content type is adjusted according to different user groups. |
| 5. | A single admin team manages the website. | Multiple admin teams are required for managing different levels of access. |
| 6. | Content does not change by different individuals. | Dynamic content changes more frequently than on typical websites. |
| 7. | When to use it?   * To be used while developing a public website with the goal of delivering and maintaining content. * If you need a site that’s independent of your internal systems. * If you need to attract visitors from a large number of anonymous people. | When to use it?   * For providing personalized content to the intended audience * Advanced user management and permission functions are required. * Need control over what users view. * For Improving customer/client relationship * Focused on automation of the business process * You have a number of systems that need to be brought together into a single visual design. |
| 8. | Pros-   * Simple content management * It is a solution when you require that your system works separately from the internal system * Attracting the audience from a broader perspective | Pros-   * Target specific audience for providing a personalized experience * Provides advanced content management * Integration of multiple systems into one for having a single visual design. |

**Types:**

|  |  |
| --- | --- |
| Personal Websites | Personal |
| Photo Sharing Websites | Government |
| Writers / Authors Websites | Cultural |
| Community Building Websites | Corporate |
| Mobile Device Websites | Stock |
| Blogging Websites | Tender |
| Social Websites | Hosted, Domain-specific |

**WiMax**

WiMax (Worldwide Interoperability for Microwave Access) is a wireless communication standard designed to provide high-speed internet access over a wide area. It is based on the IEEE 802.16 family of standards and is often referred to as “Wi-Fi on steroids” because it offers higher data rates and broader coverage than traditional Wi-Fi. In this article, we will discuss every point about Worldwide Interoperability for Microwave Access.

**What is WiMax?**

WiMax stands for **Worldwide Interoperability for Microwave Access**. This technology is based on IEEE 802.16. It is used to provide higher data rates with increased coverage. It is based on [MAN (Metropolitan Area Network)](https://www.geeksforgeeks.org/man-full-form-in-computer-networking/) technology. Its range is up to 50 Km. It may provide speeds up to 70 Mbps and it can operate in Non-Line-of-Sight. This technology is fast, convenient, and cost-effective.

**Architecture of WiMax**

* **Physical Layer:** This layer specifies frequency band, synchronization between transmitter and receiver data rate, and multiplexing scheme. This layer is responsible for encoding and decoding of signals and manages bit transmission and reception. It converts[MAC layer](https://www.geeksforgeeks.org/ieee-802-11-mac-frame/) frames into signals to be transmitted. Modulation schemes that are used on this layer include QPSK, QAM-16, and QAM-64.
* **MAC Layer:** This layer provides an interface between the convergence layer and the physical layer of the WiMax protocol stack. It provides point-to-multipoint communication and is based on [CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).](https://www.geeksforgeeks.org/carrier-sense-multiple-access-csma/) The MAC layer is responsible for transmitting data in frames and controlling access to shared wireless media. The MAC protocol defines how and when a subscriber may initiate a transmission on the channel.
* **Convergence Layer:** This layer provides the information of the external network. It accepts a higher layer [protocol data unit (PDU)](https://www.geeksforgeeks.org/protocol-data-unit-pdu/)and converts it to a lower-layer PDU. It provides functions depending on the service being used.

Wi-Fi is wireless networking technology enabling various devices like computers, smartphones, and other equipment to connect to the Internet and communicate with each other without a cable. It creates a network where these devices can exchange information. These established connections through a wireless router act as an intermediary between the WiFi-compatible devices and the Internet. This technology allows seamless internet access and device communication in homes, offices, and in public spaces.

**What is Wi-Fi?**

WiFi is a wireless technology that allows electronic devices to connect to the internet and communicate with each other without a physical cable. This uses radio waves to transmit the data between a WiFi router and compatible devices like smartphones, computers, and smart home gadgets. These WiFi networks are common in homes, offices, and public spaces providing convenient internet access and local connectivity. This technology has become an essential part of modern digital life enabling wireless internet browsing, file sharing, and device communication in various settings.

**What is a Wireless Access Point?**

The WAP means a wireless access point is the networking device that allows WiFi-enabled devices to connect to the wired network. It acts as the central hub broadcasting the Wi-Fi signal that devices can detect and join. Access points are commonly used to extend the range of existing networks, create separate network segments, or provide Wi-Fi connectivity in large spaces like offices, schools or public areas. They can be standalone devices or integrated into a router and they enable multiple devices to access network resources and the internet wirelessly within their coverage area.

**Applications of Wi-Fi**

* Using Wi-Fi we can access the internet in any Wi-Fi-capable device wirelessly. We can stream or cast audio or video wirelessly on any device using Wi-Fi for our entertainment.
* We can share files, data, etc between two or more computers or mobile phones using Wi-Fi, and the speed of the data transfer rate is also very high. Also, we can print any document using a Wi-Fi printer, this is very much used nowadays.
* We can use Wi-Fi as [**HOTSPOTS**](https://www.geeksforgeeks.org/difference-between-wifi-and-hotspot/) also, it points Wireless Internet access for a particular range of area. Using Hotspot the owner of the main network connection can offer temporary network access to Wi-Fi-capable devices so that the users can use the network without knowing anything about the main network connection. Wi-Fi adapters are mainly spreading radio signals using the owner network connection to provide a hotspot.
* Using Wi-Fi or [WLAN](https://www.geeksforgeeks.org/difference-between-wlan-and-wi-fi/) we can construct simple wireless connections from one point to another, known as Point to point networks. This can be useful to connect two locations that are difficult to reach by wire, such as two buildings of corporate business.
* One more important application is **VoWi-Fi**, which is known as **voice-over Wi-Fi**. Some years ago telecom companies are introduced VoLTE (Voice over Long-Term Evolution ). Nowadays they are introduced to VoWi-Fi, by which we can call anyone by using our home Wi-Fi network, only one thing is that the mobile needs to connect with the Wi-Fi. Then the voice is transferred using the Wi-Fi network instead of using the mobile SIM network, so the call quality is very good. Many mobile phones are already getting the support of VoWi-Fi.
* In an office, all the computers are interconnected using Wi-Fi. For Wi-Fi, there are no wiring complexities. Also, the speed of the network is good. For Wi-Fi, a project can be presented to all the members at a time in the form of an excel sheet, ppt, etc. For Wi-Fi, there is no network loss as in cable due to cable break.
* Also using W-Fi a whole city can provide network connectivity by deploying routers at a specific area to access the internet. Already schools, colleges, and universities are providing networks using Wi-Fi because of its flexibility. Wi-Fi is used as a *positioning system* also, by which we can detect the positions of Wi-Fi hotspots to identify a device location.

**Types of Wi-Fi Connections**

**LAN (Local Area Network)**

A LAN operates within a limited area like an office building or home, connecting various devices such as computers, printers, and storage devices. It uses components like switches, routers, and cables, with Wi-Fi being the most common wireless form of LAN. Think of it as a network that serves a single location.

**PAN (Personal Area Network)**

A PAN is the smallest network type, centered around one person’s devices in a specific location, typically connecting personal gadgets like phones, computers, and gaming consoles. [Bluetooth](https://www.geeksforgeeks.org/bluetooth/) is the most well-known wireless [PAN](https://www.geeksforgeeks.org/overview-of-personal-area-network-pan/) technology. These networks are perfect for personal use in homes or small offices.

**MAN (Metropolitan Area Network)**

A MAN covers a larger geographical area than a [LAN](https://www.geeksforgeeks.org/lan-full-form/), typically spanning across a city, college campus, or business complex. It’s designed to connect multiple locations within a metropolitan area, making it ideal for organizations that need to manage systems across several buildings or facilities.

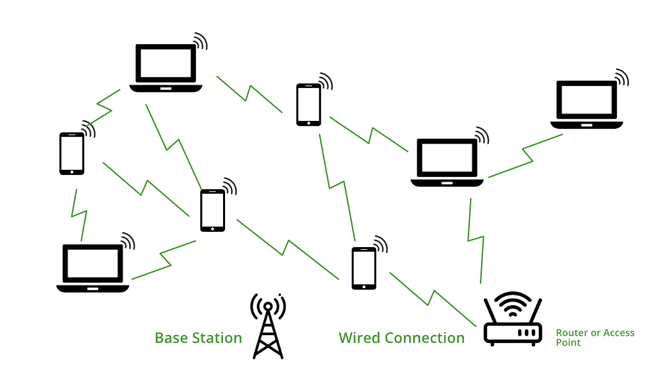
**WAN (Wide Area Network)**

A [WAN](https://www.geeksforgeeks.org/wan-full-form/) is the largest network type, covering vast geographical areas like cities, countries, or even the entire globe – the Internet being the most famous example. It can encompass multiple smaller networks like LAN and [MAN](https://www.geeksforgeeks.org/man-full-form-in-computer-networking/), and cellular networks are the most common type of wireless WAN.

**How does a Wi-Fi work?**

Wi-Fi is a wireless technology for networking, so it uses Electromagnetic waves to transmit networks. We know that there are many divisions of Electromagnetic waves according to their frequency such as X-ray, Gamma-ray, radio wave, microwave, etc, in Wi-Fi, the radio frequency is used. For transmitting Wi-Fi signal there is three medium,

* **Base Station Network or an Ethernet(802.3) Connection:** It is the main host network from where the network connection is provided to the router.
* **Access Point or Router:** it is a bridge between a wired network and a wireless network. It accepts a wired Ethernet connection and converts the wired connection to a wireless connection and spreads the connection as a radio wave.
* **Accessing Devices:** It is our mobile, computer, etc from where we use the Wi-Fi and surfing internet.



*Working of Wi-Fi*

All the electronics devices read data in binary form, also router or our devices, here routers provide radio waves and those waves are receive by our devices and read the waves in binary form. We know how a wave looks like a upper pick of the wave is known as a 1 and the lower pick of the wave is known as the 0 in a binary as mentioned below :

* **SSID (Service Set Identifier):** This 32 character name that identifies the Wi-Fi network and differentiates the one Wi-Fi from a another Wi-Fi. All the devices are attempting to connect a particular [SSID](https://www.geeksforgeeks.org/service-set-identifier-ssid-in-computer-network/). A SSID is the name of a wireless network.
* **WPA-PSK (Wi-Fi Protected Access- Pre-Shared Key):** The program developed by Wi-Fi Alliance Authority to secure a wireless networks with a use of a Pre Shared Key authentication. The WPA has a 3 types such as WPA, WPA2 and a WPA3. It is a way of encrypting a Wi-Fi signal to protect from a unwanted users.