Internet programming and web technologies(20A35502T)

**Unit 1 internet overview**

**Internet Overview:**

The Internet, sometimes called simply "the Net,"

**Definition**:

The internet is a globally connected network system facilitating worldwide communication and access to data resources through a vast collection of private, public, business, academic and government networks.

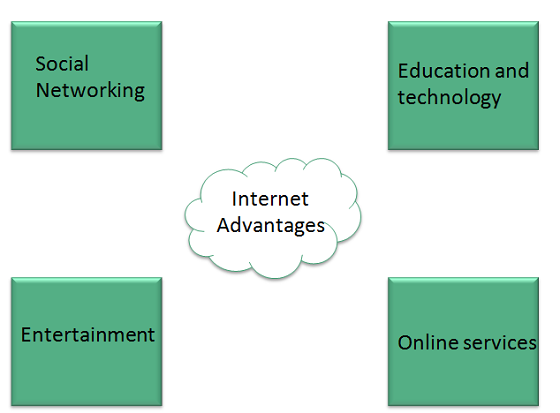
**Evolution:**

The concept of Internet was originated in 1969 and has undergone several technological & Infrastructural changes as follows:

* The origin of Internet devised from the concept of **Advanced Research Project Agency Network (ARPANET).**
* **ARPANET** was developed by United States Department of Defense.
* Basic purpose of ARPANET was to provide communication among the various bodies of government.
* Initially, there were only four nodes, formally called **Hosts.**
* In 1972, the **ARPANET** spread over the globe with 23 nodes located at different countries and thus became known as **Internet.**
* By the time, with invention of new technologies such as TCP/IP protocols, DNS, WWW, browsers, scripting languages etc., Internet provided a medium to publish and access information over the web.

**Advantages:**

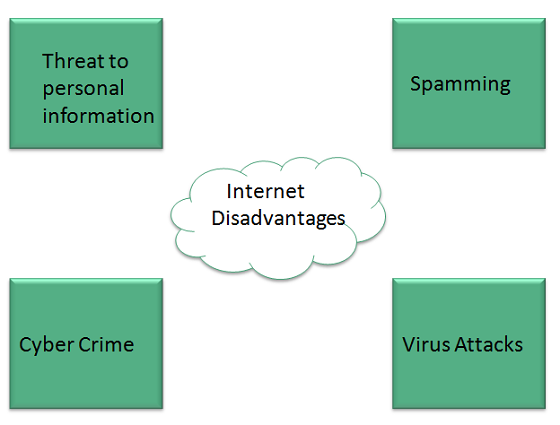
some of the advantages of Internet:



* Internet allows us to communicate with the people sitting at remote locations. There are various apps available on the wed that uses Internet as a medium for communication. various social networking sites such as:
  + Facebook
  + Twitter
  + Google+
  + Orkut, ..etc.
* Any kind of information can be surfed over the internet. Information regarding various topics such as Technology, Health & Science, Social Studies, Geographical Information, Information Technology, Products etc can be surfed with help of a search engine.
* Apart from communication and source of information, internet also serves a medium for entertainment. Following are the various modes for entertainment over internet.
  + Online Television
  + Online Games
  + Songs
  + Videos
  + Social Networking Apps
* Internet allows us to use many services like:
  + Internet Banking
  + Matrimonial Services
  + Online Shopping
  + Online Ticket Booking
  + Online Bill Payment
  + Data Sharing
  + E-mail
* Internet provides concept of **electronic commerce**, that allows the business deals to be conducted on electronic systems

## Disadvantages:

## Some of the disadvanatges of Internet are:



* There are always chances to loose personal information such as name, address, credit card number. Therefore, one should be very careful while sharing such information. One should use credit cards only through authenticated sites.
* Another disadvantage is the **Spamming**. Spamming corresponds to the unwanted e-mails in bulk. These e-mails serve no purpose and lead to obstruction of entire system.
* **Virus** can easily be spread to the computers connected to internet. Such virus attacks may cause system to crash or important data may get deleted.
* There are various websites that do not provide the authenticated information. This leads to misconception among many people.

**Networks:**

A network is a set of devices (often referred to as *nodes)* connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

**Network Criteria :**

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

**Performance:**

Performance can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.

Performance is often evaluated by two networking metrics: throughput and delay.

**Reliability:**

network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

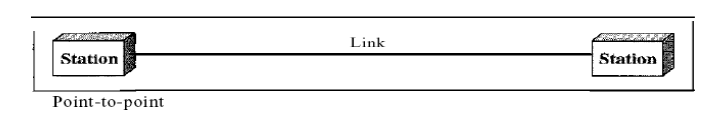
**Security:**

Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

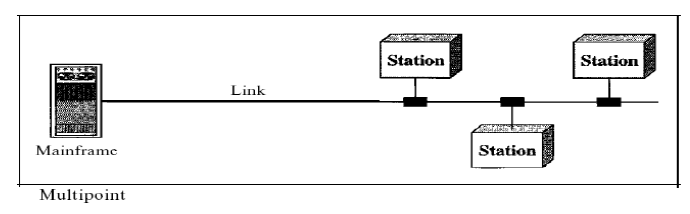
**Types of Connection:**

* There are two possible types of connections: point-to-point and multi point

Point-to-Point:

A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.

Multipoint:

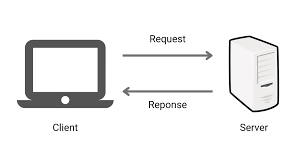


A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatiallyshared connection. If users must take turns, it is a timesharedconnection.

**Types of computer network architecture:**

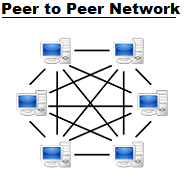
Computer network design falls under two broad categories:

1. Client-server architecture



* First, the client sends their request via a network-enabled device
* Then, the network server accepts and processes the user request
* Finally, the server delivers the reply to the client

2. Peer-to-peer architecture



## In Peer-to-Peer (P2P) architecture, connected computers have equal powers and privileges. There is no central server for coordination. Each device in the computer network can act as either client or server. Each peer may share some of its resources, like memory and processing power, with the entire computer network. For example, some companies use P2P architecture to host memory-consuming applications, such as 3-D graphic rendering, across multiple digital devices.

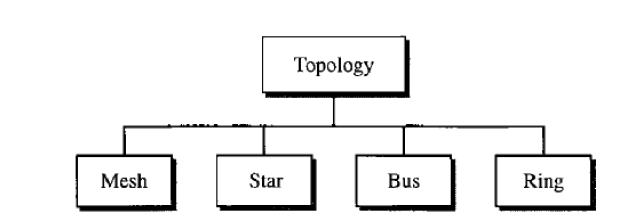
## Network topology:

The arrangement of nodes and links is called network topology.

(or)

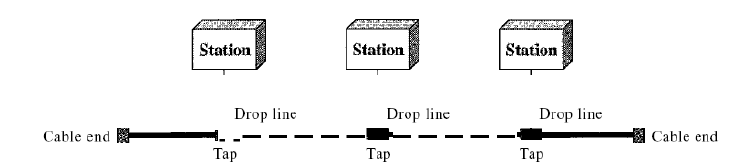
Topologyrefers to the way in which a network is laid out physically.

The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible: bush, star , ring , and mesh topology



### Bus topology:

Each node is linked to one other node only. Data transmission over the network connections occurs in one direction.



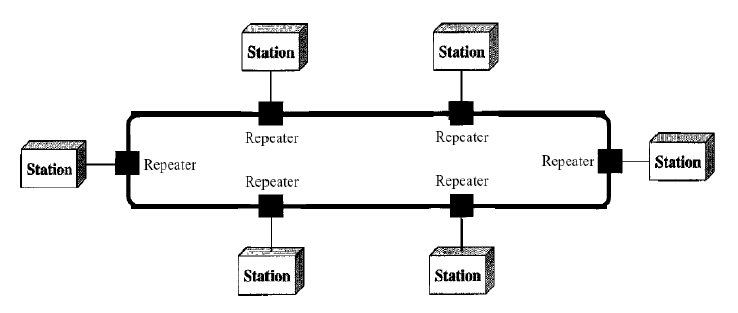
Nodes are connected to the bus cable by drop lines and taps.

Advantages of a bus topology : It include ease of installation.

Backbone cable can be laid along the most efficient path.

Disadvantages: It include difficult reconnection and fault isolation.

### Ring topology:



In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.

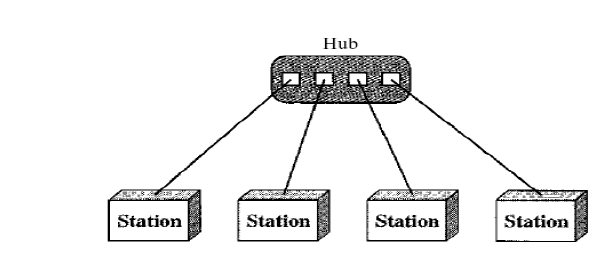
Each device in the ring incorporates a repeater.

Advantage : Data can flow bi-directionally.

Disadvantage : Single node failure can bring down the entire network.

### Star topology:

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub.

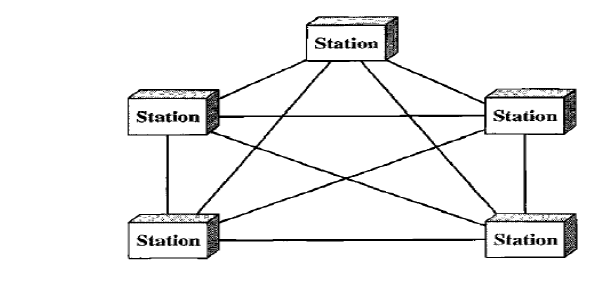


Advantage: 1. star topology performs better as data doesn’t have to go through each node.

2. It is also more reliable.

Disadvantage: star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead

### Mesh topology:



Every node is connected to many other nodes. In a full mesh topology, every node is connected to every other node in the network.

Advantages:

1. The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.

2. A mesh topology is robust.

Disadvantages:

1. Disadvantage of a mesh are related to the amount of cabling because every device must be connected to every other device, installation and reconnection are difficult.

2. Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate

**Categories of Networks:**

What are the types of enterprise computer networks?

Depending on the organization's size and requirements, there are three common types of enterprise private networks:

Local area network (LAN):



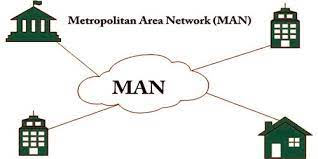
A LAN is an interconnected system limited in size and geography. It typically connects computers and devices within a single office or building. It is used by small companies or as a test network for small-scale prototyping.

LANs are distinguished from other kinds of networks by three characteristics:

(1) Their size,

(2) Their transmission technology, and

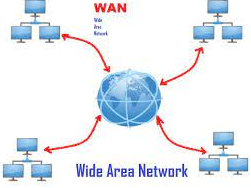
(3) Their topology

Metropolitan Area Network (MAN):

### A metropolitan area network, or MAN, covers a city. The best-known example of a MAN is the cable television network available in many cities.

### A MAN is implemented by a standard called DQDB (Distributed Queue Dual Bus)

Wide area networks (WAN):



An enterprise network spanning buildings, cities, and even countries, is called a wide area network (WAN). While local area networks are used to transmit data at higher speeds within close proximity, WANs are set up for long-distance communication that is secure and dependable.

SD-WAN or software-defined WAN is virtual WAN architecture controlled by software technologies. An SD-WAN offers more flexible and dependable connectivity services that can be controlled at the application level without sacrificing security and quality of service.

Service provider networks

Service provider networks allow customers to lease network capacity and functionality from the provider. Network service providers may consist of telecommunications companies, data carriers, wireless communications providers, Internet service providers, and cable television operators offering high-speed Internet access.

Cloud networks

Conceptually, a cloud network can be seen as a WAN with its infrastructure delivered by a cloud-based service. Some or all of an organization’s network capabilities and resources are hosted in a public or private cloud platform and made available on demand. These network resources can include virtual routers, firewalls, bandwidth, and network management software ,with other tools and functions available as required.

Businesses today use cloud networks to accelerate time-to-market, increase scale, and manage costs effectively. The cloud network model has become the standard approach for building and delivering applications for modern enterprises.

**Advantages of Computer Network:**

• Better communication

• Better connectivity

• Better sharing of Resources

• Bring people together

**WWW (World Wide Web):**

* The World Wide Web, abbreviated as WWW or W3 and commonly known as the Web, is a system of interlinked hypertext documents accessed via the Internet.
* The World Wide Web (abbreviated WWW or the Web) is an information space where documents and other web resources are identified by Uniform Resource Locators (URLs), interlinked by hypertext links, and can be accessed via the Internet.
* With a web browser, one can view web pages that may contain text, images, videos, and other multimedia and navigate between them via hyperlinks.

History of the World Wide Web:



* The World Wide Web was invented by a British scientist, Tim Berners-Lee in 1989. He was working at CERN at that time. Originally, it was developed by him to fulfill the need of automated information sharing between scientists across the world, so that they could easily share the data and results of their experiments and studies with each other.

 data networks, and hypertext into a user-friendly and effective global information system.

WORLD WIDE WEB WORKS:

WWW is a collection of websites connected to the internet so that people can search and share information. It works as follows:

* The computer of a user who requests documents from a server is known as a client. Browser, which is installed on the user' computer, allows users to view the retrieved documents.
* The servers store and transfer web pages or information to user's computers on the network when requested by the users. A web server is a software program which serves the web pages requested by web users using a browser.

**Protocol:**

A protocol is a set of rules and guidelines for communicating data. Rules are defined for each step and process during communication between two or more computers. Networks have to follow these rules to successfully transmit data.

 Many Internet Web browsers allow users to access files using most of the protocols.

**Why do we need protocols**

 the sender and receiver of data are parts of different networks, located in different parts of the world having different data transfer rates. protocols are used to manage the flow control of data, access control of the link being shared in the communication channel.

**Types of internet protocols:**

The Internet Protocols are of different types having different uses.

## There are 9 important types of Internet Protocols. Those are:

## Internet Protocol (IP)

## Transmission Control Protocol (TCP)

## User Datagram Protocol (UDP)

## File Transfer Protocol (FTP)

## Trivial File Transfer Protocol (TFTP)

## Telnet

## Hyper Text Transfer Protocol (HTTP)

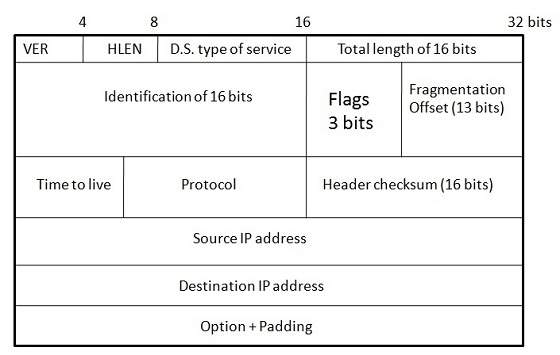
## Point to point protocol (PPP)

## Simple network management protocol (SNMP)

## 1. Internet Protocol (IP):

Internet Protocol is **connectionless** and **unreliable** protocol. It ensures no guarantee of successfully transmission of data.

Internet protocol transmits the data in form of a datagram as shown in the following diagram:



In order to make it reliable, it must be paired with reliable protocol such as TCP at the transport layer.

**Points to remember:**

* The length of datagram is variable.
* The Datagram is divided into two parts: **header** and **data.**
* The length of header is 20 to 60 bytes.
* The header contains information for routing and delivery of the packet.

## 2. Transmission Control Protocol (TCP)

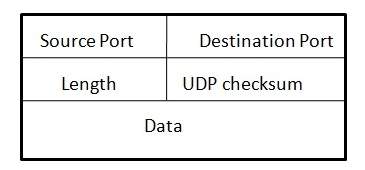
TCP is a connection oriented protocol and offers end-to-end packet delivery. It acts as back bone for connection. It exhibits the following key features:

* Transmission Control Protocol (TCP) corresponds to the Transport Layer of OSI Model.
* TCP is a reliable and connection oriented protocol.
* TCP offers:
  + Stream Data Transfer.
  + Reliability.
  + Efficient Flow Control
  + Full-duplex operation.
  + Multiplexing.

## 3. User Datagram Protocol (UDP):

UDP is connectionless and unreliable protocol. It doesn’t require making a connection with the host to exchange data. Since UDP is unreliable protocol, there is no mechanism for ensuring that data sent is received.

UDP transmits the data in form of a datagram. The UDP datagram consists of five parts as shown in the following diagram:



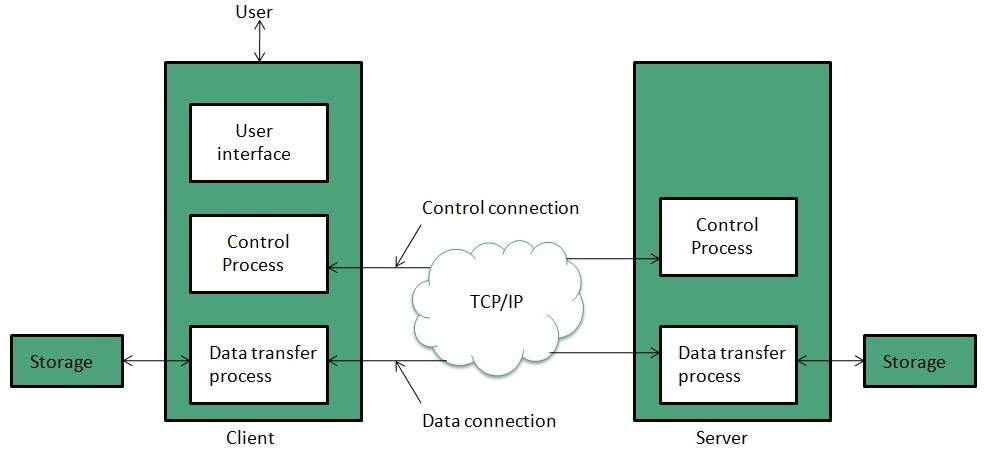
**Points to remember:**

* UDP is used by the application that typically transmit small amount of data at one time.
* UDP provides protocol port used i.e. UDP message contains both source and destination port number, that makes it possible for UDP software at the destination to deliver the message to correct application program.

4. File Transfer Protocol(FTP):

FTP is used to copy files from one host to another. FTP offers the mechanism for the same in following manner:

* FTP creates two processes such as Control Process and Data Transfer Process at both ends i.e., at client as well as at server.
* FTP establishes two different connections: one is for data transfer and other is for control information.
* **Control connection** is made between **control processes** while **Data Connection** is made between Data Transfer Process
* FTP uses **port 21** for the control connection and **Port 20** for the data connection.



## 5. Trivial File Transfer Protocol (TFTP):

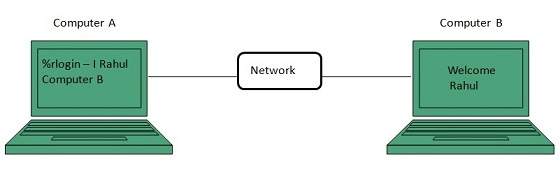
**Trivial File Transfer Protocol** is also used to transfer the files but it transfers the files without authentication. Unlike FTP, TFTP does not separate control and data information. Since there is no authentication exists, TFTP lacks in security features therefore it is not recommended to use TFTP.

**Key points**

* TFTP makes use of UDP for data transport. Each TFTP message is carried in separate UDP datagram.
* The first two bytes of a TFTP message specify the type of message.
* The TFTP session is initiated when a TFTP client sends a request to upload or download a file.
* The request is sent from an ephemeral UDP port to the **UDP port 69**of an TFTP server.

## 6. Telnet:

Telnet is a protocol used to log in to remote computer on the internet. There are a number of Telnet clients having user friendly user interface. The following diagram shows a person is logged in to computer A, and from there, he remote logged into computer B.



7. Hyper Text Transfer Protocol (HTTP)

HTTP is a communication protocol. It defines mechanism for communication between browser and the web server. It is also called request and response protocol because the communication between browser and server takes place in request and response pairs.

### HTTP Request

HTTP request comprises of lines which contains:

* Request line
* Header Fields
* Message body

**Key Points**

The first line i.e., the **Request line** specifies the request method i.e., **Get** or **Post.**

* The second line specifies the header which indicates the domain name of the server from where index.htm is retrieved.

### HTTP Response

Like HTTP request, HTTP response also has certain structure. HTTP response contains:

* Status line
* Headers
* Message body

## 8. Point to point protocol (PPP):

Point to point protocol provides connections for the host to the network or between two routers. It has also a security mechanism.

Point to point protocol is well known as a protocol for connecting telephone lines using modems on both ends. It is widely used to connect computers to the internet.

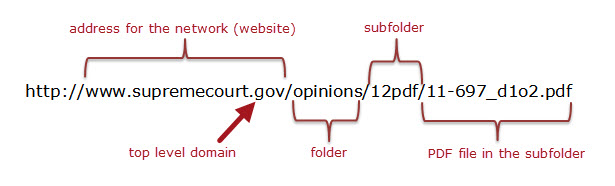
## 9. Simple network management protocol (SNMP):

A simple protocol that defines messages related to network management. Through the use of a simple network management protocol (SNMP) any host on the LAN can configure network devices such as routers.

**Web Organization and Addressing:**

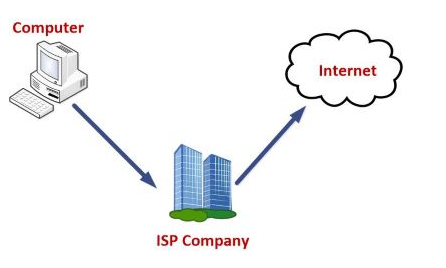
The web address contains information about the location of the webpage.

 a web address organizes information about a webpage's location in a predictable way.



**Internet Service Provider (ISP):**

The term Internet service provider (ISP) refers to a company that provides access to the Internet to both personal and business customers.



ISPs can be divided into many types, some of which are as follows:

**Dial-up Internet access:** It is the oldest technology to provide Internet access by modem to modem connection using telephone lines. In this method, the user's computer is connected to a modem with a telephone line. This method has become outdated today due to slow connection speed. However, in remote areas, this method can be used where the broadband network is not available.

**DSL:** DSL, which stands for 'digital subscriber line' is an advanced version of the dial-up Internet access method. It uses high frequency to execute a connection over the telephone network and allows the internet and the phone connection to run on the same telephone line. This method offers an Asymmetric Digital Subscriber (ADSL), where the upload speed is less than the download speed, and a Symmetric Digital Subscriber Line (SDSL), which offers equal upload and download speeds. Out of these two, ADSL is more popular among users and is popularly known as DSL.

**Wireless Broadband (WiBB):** It is a modern broadband technology for Internet access. It allows high-speed wireless internet within a large area. To use this technology, you are required to place a dish on the top of your house and point it to the transmitter of your Wireless Internet Service Provider (WISP).

**Wi-Fi Internet:** It is the short form for "wireless fidelity," which is a wireless networking technology that provides wireless high-speed Internet connections using radio waves. To use the internet, you are required to be within the range of wi-fi network. It is commonly used in public places such as hotels, airports, restaurants to provide internet access to customers.

**ISDN:** It is a short form of Integrated Services Digital Network. It is a telephone system network which integrates a high-quality digital transmission of voice and data over the same standard phone line. It offers a fast upstream and downstream Internet connection speed and allows both voice calls and data transfer.

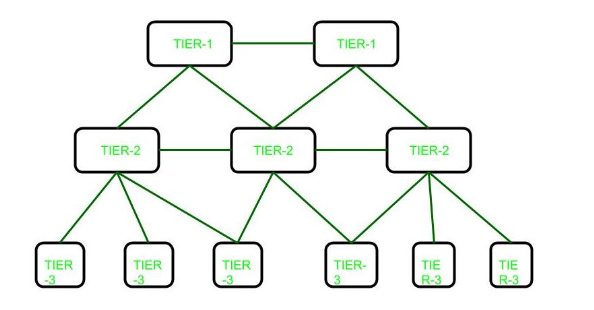
**Ethernet:** It is a wired LAN (Local Area Network) where computers are connected within a primary physical space. It enables devices to communicate with each other via a protocol (a set of rules or common network language). It may provide different speeds such as 10 Mbps, 100 Mbps and 10 Gbps.

**List of ISP**

* Reliance Jio
* Vodafone Idea
* Airtel
* BSNL
* Hathway

# Internet Service Provider (ISP) hierarchy:

**Internet Service Provider (ISP)**is a company which provides internet connection to end user, but there are basically three levels of ISP. There are 3 levels of Internet Service Provider (ISP): Tier-1 ISP, Tier-2 ISP, and Tier-3 ISP.



* **Tier-1 ISP:**   
  These ISPs are at the top of the hierarchy and they have a global reach they do not pay for any internet traffic through their network instead lower-tier ISPs have to pay a cost for passing their traffic from one geolocation to another which is not under the reach of that ISPs. Generally, ISPs at the same level connect to each other and allow free traffic passes to each other. Such ISPs are called peers. Due to this cost is saved. They build infrastructure, such as the Atlantic Internet sea cables, to provide traffic to all other Internet service providers, not to end users.

Examples**:**   
Some examples of tier 1 Internet providers: Cogent Communications, Hibernia Networks, AT&T

* **Tier-2 ISP:**   
  These ISPs are service provider who connects between tier 1 and tier 3 ISPs. They have regional or country reach and they behave just like Tier-1 ISP for Tier-3 ISPs.

Examples**:**   
Examples of tier 2 ISPs: Vodafone,Easynet,BT

* **Tier-3 ISP:**   
  These ISPs are closest to the end users and helps them to connect to the internet by charging some money. These ISPs work on purchasing model. These ISPs have to pay some cost to Tier-2 ISPs based on traffic generated.

Examples**:**   
Examples of Tier-3 ISPs:

Comcast,

Deutsche Telekom,

Verizon Communications

**Advantages:**

* The customer need not then bother with either the technicalities or finances of investing and inventing a web browser to work with. An ISP can readily do all of this for its customers.
* Many ISPs, being professional companies, provide its clientele with high-speed internet and that is not possible if one decides to sidesteps these companies.
* ISPs offer a very high degree of reliability and availability
* The ISPs are secure – they offer a tremendous deal of protection against viruses and use only the latest software patches whilst operating and thereby, maintaining the integrity of the browser.
* User do not need to invest in user’s own web server.
* ISP’s should give the best uptime guarantee.

#### **Disadvantages:**

* Because of the range of options available in the market and due to cut-throat competition, some of the ISPs have been accused of violating the customers’ trust by way of inflated pricing, data losses, etc. It is true that using an ISP makes the customer entirely dependent on it.
* If an Internet Service Provider is stretched thin because of hosting too many sites on a shared server, it can compromise the quality of the customers’ data by way of slow download rates and poor performance of websites.
* User need to trust user’s ISP for uptime and security.
* ISP can directly affect user if the it gets blacklisted.

**DNS:**

The Domain Name System (DNS) Server is a server that is specifically used for matching website hostnames (like[example.com](http://example.com/))to their corresponding Internet Protocol or IP addresses. The DNS server contains a database of public IP addresses and their corresponding domain names.

Every device connected to the internet has a unique IP address that helps to identify it, according to the IPv4 or IPV6 protocols. The same goes for web servers that host websites.( DNS matches a website name to their corresponding IP address.)

DNS servers help us avoid memorization of such long numbers in IP addresses as they automatically translate the website names we enter into the browser address bar into these numbers so that the servers can load the right web pages.

**DNS Work**

The act of entering the domain name is referred to as a DNS query and the process of finding the corresponding IP address is known as DNS resolution.

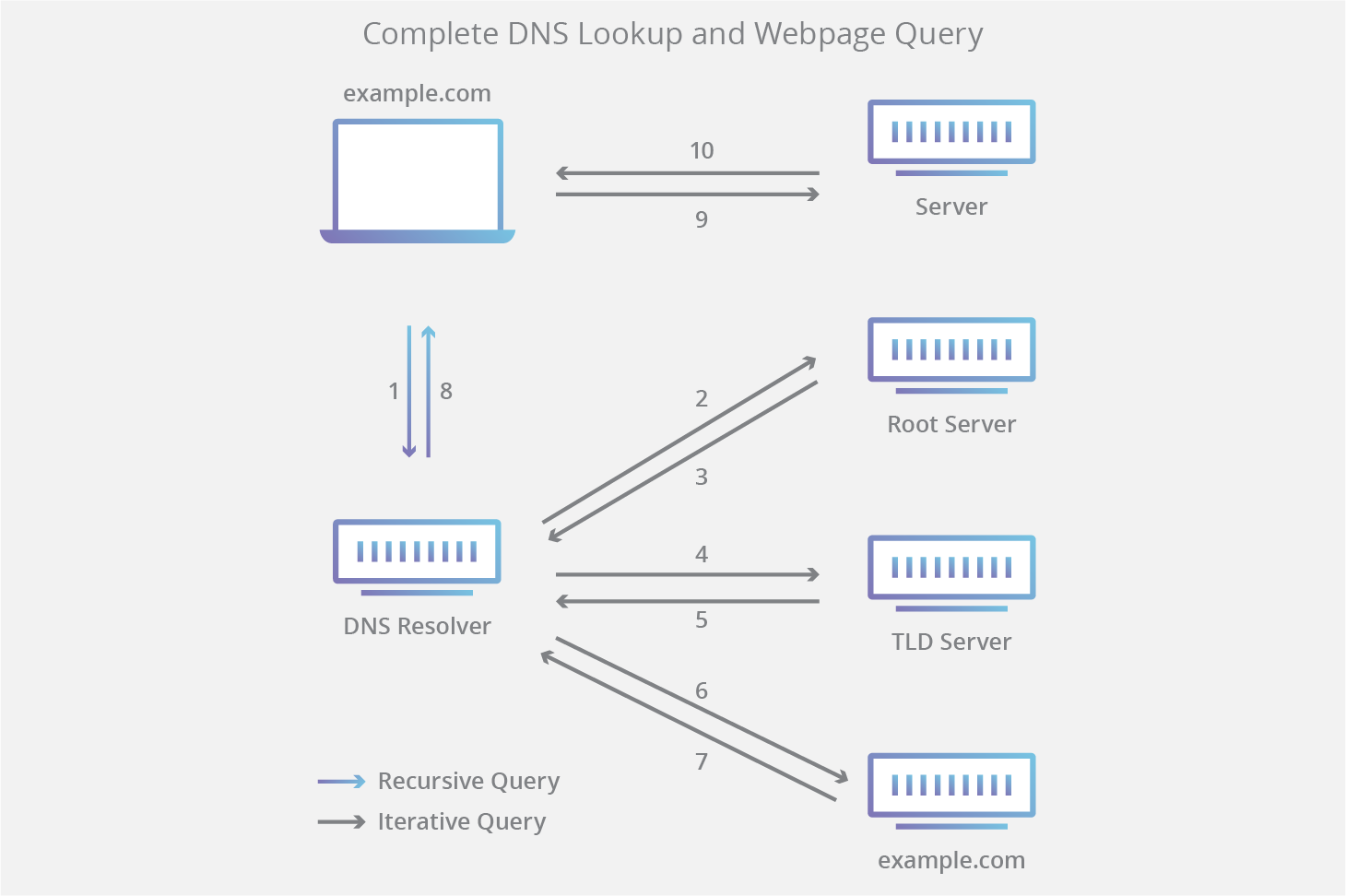
DNS queries can be of three types: recursive query, iterative query or non-recursive query.

1. Recursive query – These are queries where a DNS server has to respond with the requested resource record. If a record cannot be found, the DNS client has to be shown an error message.
2. Iterative query – These are queries for which the DNS client will continue to request a response from multiple DNS servers until the best response is found, or an error or timeout occurs. If the DNS server is unable to find a match for the query, it will refer to a DNS server authoritative for a lower level of the domain namespace. This referral address is then queried by the DNS client and this process continues with additional DNS servers.
3. Non-recursive query – these are queries which are resolved by a DNS resolver when the requested resource is available, either due to the server being authoritative or because the resource is already stored in cache.

The Different Types of DNS Server

There are four servers that work together to deliver an IP address to the client:

1. **DNS recursor:**  The DNS recursor (also referred to as the DNS resolver) is a server that receives the query from the DNS client, and then interacts with other DNS servers to hunt down the correct IP. Once the resolver receives the request from the client, the resolver then actually behaves as a client itself, querying the other three types of DNS servers in search of the right IP.
2. **Root name server :** The resolver queries the root nameserver. The root server is the first step in translating (resolving) human-readable domain names into IP addresses. The root server then responds to the resolver with the address of a [top-level domain (TLD)](https://www.cloudflare.com/learning/dns/top-level-domain/) DNS server (such as .com or .net) that stores the information for its domains.
3. **Top Level Domain (TLD) nameserver :** The resolver queries the TLD server. The TLD server responds with the IP address of the domain’s authoritative nameserver. The recursor then queries the authoritative nameserver, which will respond with the IP address of the origin server.
4. **Authoritative nameserver**:  In the last step, the authoritative DNS nameserver will return the IP address back to the DNS recursor and DNS recursor send that IP address back to client. Using this IP address, the client can then initiate a query directly to the origin server, and the origin server will respond by sending website data that can be interpreted and displayed by the web browser.



Benefits of a DNS server

There are many benefits to be seen when using a DNS server. The most significant include:

* DNS servers help you locate websites by typing the domain as opposed to its IP address
* They add an extra layer of security to your network
* Without DNS servers, online transactions would be impossible
* If a website changes its IP address, the DNS server will pick this up and automatically update its database so users are unaffected.
* DNS servers are fast at what they do, meaning less downtime for users.

## What to Do if DNS Server Isn’t Responding

there are lots of ways to try and resolve this.

1. Switch web browser. If the problem occurs while on Google Chrome, try Firefox, or Opera instead.
2. Turn off your firewall temporarily. While firewalls are extremely important when it comes to protecting your computer against unwanted DNS attacks, they do have a habit of interfering with your network connection. Once turned off, revisit the page you had problems connecting to. If the website loads ok, then you know the firewall settings need adjusting.
3. Clear your DNS settings. The final step to try when experiencing DNS server issues is to clear your DNS cache.

**Connection Types:**

Many type of connections can be used for internet access.

All the connections have their own speed range that can be used for different purposes like for home, or for personal use.

**Different types of internet connections are:**

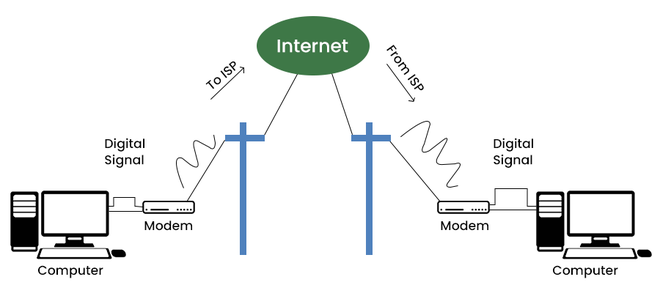
1. Dial-Up Connection
2. Broadband Connection
3. DSL
4. Cable Connection
5. Satellite Connection
6. Wireless Connection
7. Cellular
8. ISDN

**1.Dial-Up Connection:**

A dial-up connection is established between your computer and the ISP server using a modem.

A dial-Up Connection is a cheap and traditional connection that is not preferred these days as this type of connection is very slow.

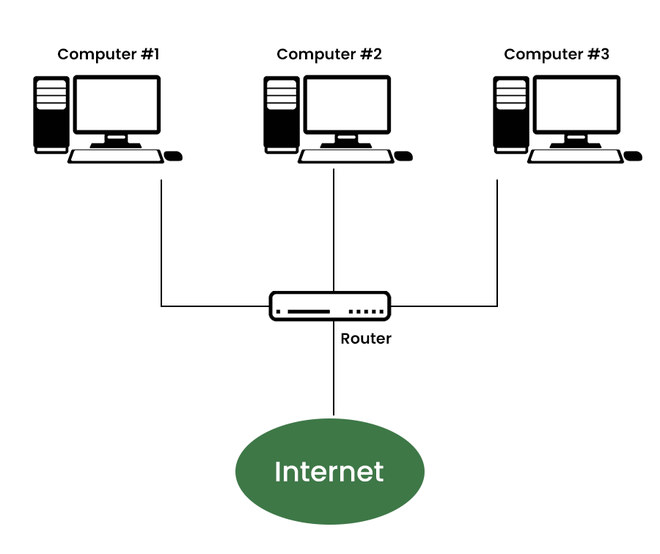
To access the internet connection in the dial-up connection we need to dial a phone number on the computer and that’s why it requires a telephone connection. It requires a modem to set up a dial-up connection, which works as interference between your computer and the telephone line. In this connection, we can use either an internet connection or telephone at a time.



**2.Broadband connection:**

Broadband refers to high-speed internet access that is faster than traditional dial-up access. It is provided through either cable or telephone composition. It does not require any telephone connection that’s why here we can use telephone and internet connection simultaneously. In this connection, more than one person can access the internet connection simultaneously.

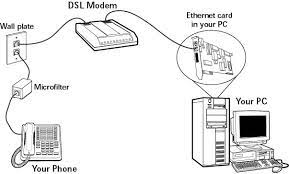
It is a wide bandwidth data transmission that transports several signals and traffic types. In this connection, the medium used is coaxial cable, optical fiber cable, radio, or twisted pair cable.



**3.DSL:**

DSL stands for Digital Subscriber Line. It provides an internet connection through the telephone line(network). DSL is a form of broadband communication that is always on, there is no need to dial a phone number to connect. DSL connection uses a router to transport data and the speed of this connection range between 128k to 8Mbps depending on the service offered. A DSL connection can translate data at 5 million bytes per second, or 5mbps.

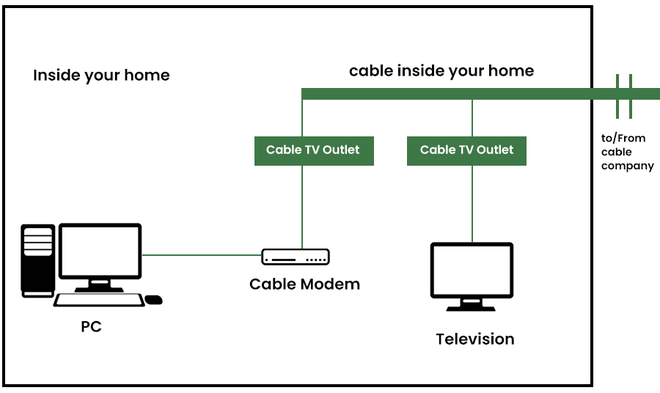
DSL service can be delivered simultaneously with wired telephone service on the same telephone line due to high-frequency bands for data.



**4.Cable Connection:**

It is a form of broadband access cable modem that can provide extremely fast access to the internet. The speed of this connection varies which can be different for uploading data transmission or downloading.

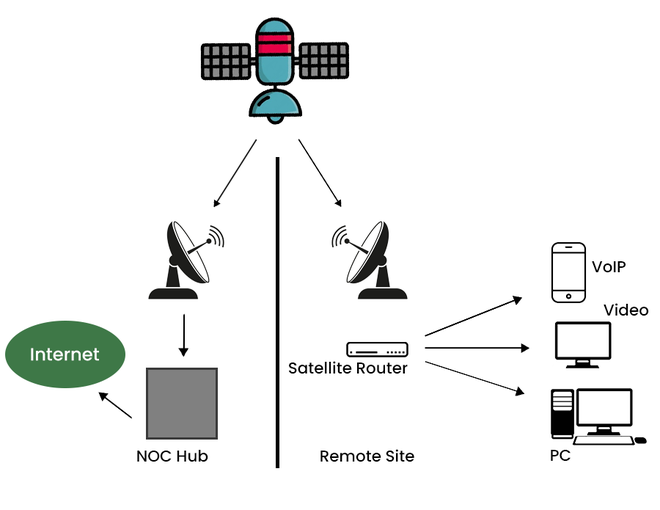
It uses a cable modem to provide an internet connection and operates over cable TV lines. The speed of cable connection ranges from 512k to 20Mbps.h



**5.Satellite Connection:**

This type of connection is provided mainly in rural areas where a broadband connection is not yet offered. It accesses the internet via a satellite that is in Earth’s orbit.

The signal travels from a long distance that is from earth to satellite and back again which provides a delayed connection. Satellite connection speeds range from 512k to 2.0Mbps.



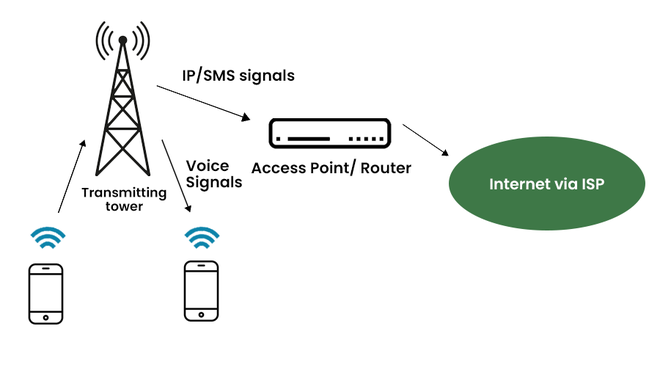
**6.Wireless Connection**

As the name suggests wireless connection does not use telephone lines or cables to connect to the internet. The wireless connection uses a radio frequency band to connect to the internet. It is also an always-on connection and this connection can be accessed from anywhere and speed may vary for different locations. It ranges from 5Mbps to 20Mbps.

## 

**7.Cellular Connection:**

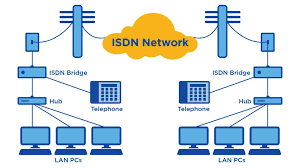
Cellular technology provides wireless Internet access through cell phones. Speed may vary depending on the service provider. The most common are 3G and 4G which means from 3rd generation and 4th generation respectively. The speed of the 3G cellular network is around 2.0Mbps and the 4G cellular network is around 21Mbps the goal of the 4G network is to achieve peak mobile speeds of 100Mbps but the current speed of the 4G network is about 21Mbps.



**8.ISDN :**

ISDN stands for Integrated Service Digital Network and it is a circuit-switched telephone network system, but it also provides access to packet-switched networks that transmits both voice and data over a digital line. It provides a packet-switched connection for data in increments of 64 kilobit/s.

ISDN connection provides better speeds and higher quality than traditional connections. It provided a maximum of 128kbit/s bandwidth in both upstream and downstream directions.



**Internet Addresses:**

Internet addresses are **made up of a network address and a host (or local) address**. This two-part address allows a sender to specify the network as well as a specific host on the network. A unique, official network address is assigned to each network when it connects to other Internet networks.

The Internet addressing scheme consists of Internet Protocol (IP) addresses and two special cases of IP addresses: broadcast addresses and loopback addresses.

Internet addresses can be in one of two formats: IPv4 (IP version 4) or IPv6 (IP version 6).

IPv4 internet addresses are 32-bit quantities. The AF\_INET address family communicates through IPv4 addresses. IPv6 internet addresses are 128-bit quantities The AF\_INET6 address family communicates through IPv6 addresses

**Types Of IP Address-**

IP Addresses may be of the following two types-



**1. Static IP Address-**

Static IP Address is an IP Address that once assigned to a network element always remains the same.

They are configured manually.

Some ISPs do not provide static IP addresses.

Static IP Addresses are more costly than dynamic IP Addresses

**2. Dynamic IP Address-**

Dynamic IP Address is a temporarily assigned IP Address to a network element.

It can be assigned to a different device if it is not in use.

DHCP or PPPoE assigns dynamic IP addresses.

**IP Address Format-**

IP Address is a 32 bit binary address written as 4 numbers separated by dots.

The 4 numbers are called as **octets** where each octet has 8 bits.

The octets are divided into 2 components- Net ID and Host ID.



1. **Network ID** represents the IP Address of the network and is used to identify the network.

2. **Host ID** represents the IP Address of the host and is used to identify the host within the network.

IP Address Example-

Example of an IP Address is-

00000001.10100000.00001010.11110000

(Binary Representation)

OR

1.160.10.240

(Decimal Representation)

There are two systems in which IP Addresses are classified-



**Classful Addressing**

In Classful Addressing System, IP Addresses are organized into following 5 classes-



**1. Class A-** If the 32 bit binary address starts with a bit 0, then IP Address belongs to class A.

In class A IP Address,

The first 8 bits are used for the Network ID.

The remaining 24 bits are used for the Host ID.



**Total Number of IP Addresses-**

Total number of IP Addresses available in class A

= Numbers possible due to remaining available 31 bits = 2**31**

**Total Number of Networks-**

Total number of networks available in class A

= Numbers possible due to remaining available 7 bits in the Net ID – 2

= 27 – 2 = 126

**Total Number of Hosts-**

Total number of hosts that can be configured in class A

= Numbers possible due to available 24 bits in the Host ID – 2 = 224 – 2

(The reason of subtracting 2 is explained later.)

**Range Of 1st Octet-** We have-

Minimum value of 1st octet = **0**0000000 = 0

Maximum value of 1st octet = **0**1111111 = 127

From here,

Range of 1st octet = [0, 127]

But 2 networks are reserved and unused.

So, Range of 1st octet = [1, 126]

**Use-** Class A is used by organizations requiring very large size networks like NASA, Pentagon etc.

**2. Class B-** If the 32-bit binary address starts with bits 10, then IP Address belongs to class B.

In class B IP Address,

The first 16 bits are used for the Network ID.

The remaining 16 bits are used for the Host ID.



**Total Number of IP Addresses-**

Total number of IP Addresses available in class B

= Numbers possible due to remaining available 30 bits = 230

**Total Number of Networks**-

Total number of networks available in class B

= Numbers possible due to remaining available 14 bits in the Net ID = 214

**Total Number of Hosts**-

Total number of hosts that can be configured in class B

= Numbers possible due to available 16 bits in the Host ID – 2 = 216 – 2

**Range Of 1st Octet-** We have**-**

Minimum value of 1st octet = **10**000000 = 128

Maximum value of 1st octet = **10**111111 = 191

So, Range of 1st octet = [128, 191]

**Use-** Class B is used by organizations requiring medium size networks like IRCTC, banks etc.

**3. Class C-** If the 32-bit binary address starts with bits 110, then IP Address belongs to class C. In class C IP Address,

The first 24 bits are used for the Network ID

The remaining 8 bits are used for the Host ID.



**Total Number of IP Addresses-**

Total number of IP Addresses available in class C

= Numbers possible due to remaining available 29 bits= 229

**Total Number of Networks**-

Total number of networks available in class C

= Numbers possible due to remaining available 21 bits in the Net ID = 221

**Total Number of Hosts-**

Total number of hosts that can be configured in class C

= Numbers possible due to available 8 bits in the Host ID – 2 = 28 – 2

**Range Of 1st Octet**-We have-

Minimum value of 1st octet = **110**00000 = 192

Maximum value of 1st octet = **110**111111 = 223

So, Range of 1st octet = [192, 223]

**Use-**Class C is used by organizations requiring small to medium size networks.

For example- engineering colleges, small universities, small offices etc.

**4. Class D-** If the 32-bit binary address starts with bits 1110, then IP Address belongs to classD.

Class D is not divided into Network ID and Host ID.



**Total Number of IP Addresses**-

Total number of IP Addresses available in class D= Numbers possible due to remaining available 28 bits = 228

**Range Of 1st Octet** We have-

Minimum value of 1st octet = **1110**0000 = 224

Maximum value of 1st octet = **1110**1111 = 239

So, Range of 1st octet = [224, 239]

**Use**-

Class D is reserved for multicasting.

In multicasting, there is no need to extract host address from the IP Address.

This is because data is not destined for a particular host.

**5. Class E-** If the 32-bit binary address starts with bits 1111, then IP Address belongs to class E

Class E is not divided into Network ID and Host ID.



**Total Number of IP Addresses**-

Total number of IP Addresses available in class E

= Numbers possible due to remaining available 28 bits = 228

**Range Of 1st Octet-**We have-

Minimum value of 1st octet = **1111**0000 = 240

Maximum value of 1st octet = **1111**1111 = 255

So, Range of 1st octet = [240, 255]

**Use**- Class E is reserved for future or experimental purposes.

**Rules for assigning Host ID:**

The Host ID is used to determine the host within any network. The Host ID is assigned based on the following rules:

o The Host ID must be unique within any network.

The Host ID in which all the bits are set to 0 cannot be assigned as it is used to represent the network ID of the IP address.

o The Host ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

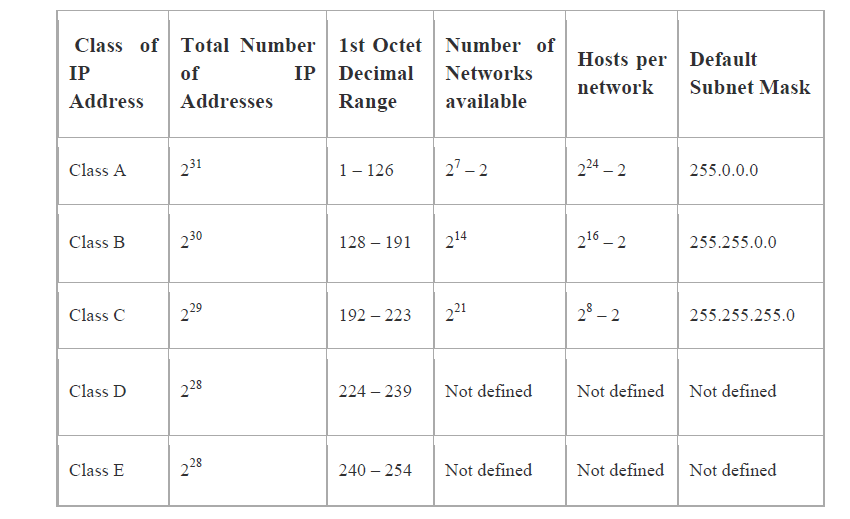
**Rules for assigning Network ID**:

If the hosts are located within the same local network, then they are assigned with the same network ID. The following are the rules for assigning Network ID:

o the network ID cannot start with 127 as 127 is used by Class A.

o The Network ID in which all the bits are set to 0 cannot be assigned as it is used to specify a particular host on the local network.

o The Network ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.



**Classless Addressing**

Classless Addressing is an improved IP Addressing system.

It makes the allocation of IP Addresses more efficient.

It replaces the older classful addressing system based on classes.

It is also known as **Classless Inter Domain Routing (CIDR)**.

**CIDR Block-**

When a user asks for specific number of IP Addresses,

CIDR dynamically assigns a block of IP Addresses based on certain rules.

This block contains the required number of IP Addresses as demanded by the user.

This block of IP Addresses is called as a **CIDR block**.

**Rules For Creating CIDR Block**- **A CIDR block is created based on the following 3 rules-**

**Rule-01**: All the IP Addresses in the CIDR block must be contiguous.

**Rule-02:**

The size of the block must be presentable as power of 2.

Size of the block is the total number of IP Addresses contained in the block.

Size of any CIDR block will always be in the form 21, 22, 23, 24, 25 and so on.

|  |
| --- |
| **Rule-03:** First IP Address of the block must be divisible by the size of the block. REMEMBER  If any binary pattern consisting of (m + n) bits is divided by 2n, then-  Remainder is least significant n bits  Quotient is most significant m bits  So, any binary pattern is divisible by 2n, if and only if its least significant n bits are 0.  Examples-  Consider a binary pattern-  01100100.00000001.00000010.01000000  (represented as 100.1.2.64)  It is divisible by 25 since its least significant 5 bits are zero.  It is divisible by 26 since its least significant 6 bits are zero.  It is not divisible by 27 since its least significant 7 bits are not zero.  **CIDR Notation-**  CIDR IP Addresses look like- **a.b.c.d / n**  They end with a slash followed by a number called as IP network prefix.  IP network prefix tells the number of bits used for the identification of network.  Remaining bits are used for the identification of hosts in the network.  **Subnetting in Networking-**  In networking,  The process of dividing a single network into multiple sub networks is called as **subnetting**.  The sub networks so created are called as **subnets**.  Example**-**Following diagram shows the subnetting of a big single network into 4 smaller subnets- |



**Advantages-** The two main advantages of subnetting a network are-

It improves the security.

The maintenance and administration of subnets is easy.

**Subnet ID-**

Each subnet has its unique network address known as its **Subnet ID**.

The subnet ID is created by borrowing some bits from the Host ID part of the IP Address.

The number of bits borrowed depends on the number of subnets created

**Types of Subnetting-**

Subnetting of a network may be carried out in the following two ways-



**1. Fixed Length Subnetting-** Fixed length subnetting also called as **classful subnetting** divides the network into subnets where-

All the subnets are of same size.

All the subnets have equal number of hosts.

All the subnets have same subnet mask.

**2. Variable Length Subnetting-** Variable length subnetting also called as **classless subnetting** divides the network into subnets where-

All the subnets are not of same size.

All the subnets do not have equal number of hosts.

All the subnets do not have same subnet mask.

**Disadvantages of Subnetting**-

**1. Subnetting leads to loss of IP Addresses.**

During subnetting,

We have to face a loss of IP Addresses.

This is because two IP Addresses are wasted for each subnet.

One IP address is wasted for its network address.

Other IP Address is wasted for its direct broadcasting address.

**2. Subnetting leads to complicated communication process**

After subnetting, the communication process becomes complex involving the following 4 steps-

1. Identifying the network

2.Identifying the sub network

3. Identifying the host

4. Identifying the process

**Subnet Mask Use-** Subnet mask is used to determine to which network the given IP Address belongs to. Host use its subnet mask to determine whether the other host it wants to communicate with is present within the same network or not.

If the destination host is present within the same network, then source host sends the packet directly to the destination host.

If the destination host is present in some other network, then source host routes the packet to the default gateway (router).

Router then sends the packet to the destination host.

**Note:**

There are four different types of IP addresses: public, private, static, and dynamic. While the public and private are indicative of the location of the network—private being used inside a network while the public is used outside of a network—static and dynamic indicate permanency.

# **Browser:**

# A browser is a software program that is used to explore, retrieve, and display the information available on the World Wide Web.

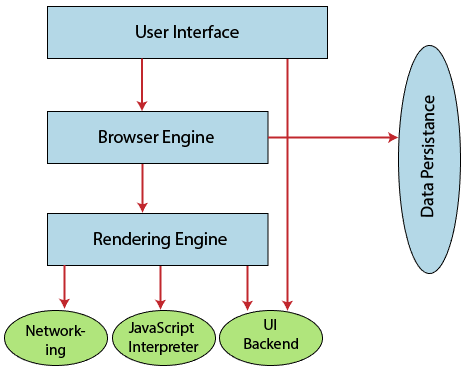
### **Features of Web Browser:**

Most Web browsers offer common features such as:

1. Refresh button
2. Stop button
3. Home button
4. Web address bar
5. Bookmarks

### **Component of a Web browser**

The primary components of a browser are shown in the below image:



1. **User Interface:** The user interface is an area where the user can use several options like address bar, back and forward button, menu, bookmarking, and many other options to interact with the browser.
2. **Browser Engine:** It connects the UI (User Interface) and the rendering engine as a bridge. It queries and manipulates the rendering engine based on inputs from several user interfaces.
3. **Rendering Engine:** It is responsible for displaying the requested content on the browser screen. It translates the HTML, XML files, and images, which are formatted by using the CSS. It generates the layout of the content and displays it on the browser screen. Although it can also display the other types of content by using different types of plugins or extensions. such as:
   * Internet Explorer uses **Trident**
   * Chrome & Opera 15+ use **Blink**
   * Chrome (iPhone) & Safari use **Webkit**
   * Firefox & other Mozilla browsers use **Gecko**
4. **Networking:** It retrieves the URLs by using internet protocols like HTTP or FTP. It is responsible for maintaining all aspects of Internet communication and security. Furthermore, it may be used to cache a retrieved document to reduce network traffic.
5. **JavaScript Interpreter:** As the name suggests, JavaScript Interpreter translates and executes the JavaScript code, which is included in a website. The translated results are sent to the rendering engine to display results on the device screen.
6. **UI Backend:** It is used to draw basic combo boxes and Windows (widgets). It specifies a generic interface, which is not platform-specific.
7. **Data Storage:** The data storage is a persistence layer that is used by the browser to store all sorts of information locally, like cookies. A browser also supports different storage mechanisms such as IndexedDB, WebSQL, localStorage, and FileSystem. It is a database stored on the local drive of your computer where the browser is installed. It handles user data like cache, bookmarks, cookies, and preferences.

### **List of Internet Browsers**

There are various types of internet browsers, which are as follows:

* **Microsoft Edge:** Microsoft Edge is a web browser that comes pre-installed with Windows 10 operating system and Windows Server 2016. It was introduced to replace the Internet Explorer Web browser, and its code name was Spartan. It offers various types of features such as freestyle writing over Web page displays, refined search, and presentations for e-books and other reading resources.  
  Microsoft Edge was developed under the **Spartan codename** Project. In April 2015, Microsoft changed the project Spartan name as Microsoft Edge. Although Internet Explorer and Edge are included with Windows 10, Edge act as a default browser. It combines new web technology evaluations and enhances the speed of browsing.  
  

Although, Internet Explorer 11 was available in Microsoft Windows operating system, Microsoft Edge has become the default browser in Windows 10. It needs at least 1 gigabyte of memory. It offers several types of features, such as annotation features, a new rendering engine, and easy-to-use icons, etc. Furthermore, it also provides better security as compared to Internet Explorer, and it can be combined with Cortana, Microsoft's virtual personal assistant.

### **Features of Microsoft Edge**

* It provides support for Firefox and Chrome add-ons.
* It has the ability to fill the form automatically.
* It can be integrated with Cortana.
* It provides faster page rendering.
* It has more security features and also allows private browsing.
* It is modern, lightweight, and reduces resource consumption.
* **Opera:** An Opera web browser was first conceived at Telenor company in 1994, later bought by the Opera Software on 1 April 1995. It was designed for desktop and mobile interfaces, but it is more popular now for mobile phones. It is based on Chromium, and it uses the blink layout engine. An opera mini was released for smartphones on 10 August 2005 that could run standard web browsers. It can be downloaded from the google play store or Apple play store.
* **Apple Safari:** Safari is an internet browser available for the Macintosh, and Windows operating systems included the iPhone, iPad, and iPod Touch. It was developed by Apple, Inc. on 30 June 2003. It is the default browser for the operating system in its products, such as OS X for the MacBook and Mac computers and iOS for the iPad and iPhone mobile devices. It is at number four in the browser market after Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome. It uses the WebKit engine, which is used for rendering fonts, displays graphics, determining page layout, and running JavaScript.
* **Google Chrome:** Google Chrome is an open-source internet browser. It is developed by Google on 11 December 2008 for Windows, Linux, Mac OS X, Android, and iOS operating systems.
* **Mozilla Firefox:** The Mozilla Firefox web browser is developed by the Mozilla Foundation and its subordinate company, Mozilla Corporation. It was first released was beta on 23 September 2002. Although it was released as the Mozilla Browser, it was internally code-named Phoenix. The First version 1.0 of Firefox was introduced on 9 November 2004.
* **Internet Explorer:** It is a web browser that is manufactured by Microsoft Corporation, and it is included with the Microsoft Windows operating system. But It was removed in Window 10 in support of Microsoft's new Edge Browser.

**Web Server:**

A web server is a computer programs that delivers (serves) content, such as Web pages, using the Hypertext Transfer protocol (HTTP), over the World Wide Web. The term Web server can also refer to the computer or virtual machine running the program.

**Types of Server**

There are four leading web servers: Apache, IIS, lighttpd and Jagsaw.

**Apache HTTP Server:** This is the most popular web server in the world developed by the Apache Software Foundation. Apache web server is an open source software and can be installed on almost all operating systems including Linux, Unix, Windows, FreeBSD, Mac OS X and more.

**Features of Apache:**

* + Handling of static files
  + Loadable dynamic modules
  + Auto-indexing
  + Compatible with IPv6
  + Supports HTTP/2
  + FTP connections
  + Bandwidth throttling
  + Load balancing
  + Session tracking
  + URL rewriting

Geolocation based on IP address and many more

**Internet Information Services:** The Internet information Server (lIS) is a high performance Web Server from Microsoft. This web server runs on Windows NT/2000 and 2003 platforms (and may be on upcoming new Windows version also). IIS comes bundled with Windows NT/20aO and 2003; Because IIS is tightly integrated with the operating system  so it is relatively easy to administer it.

**Lighttpd:** The lighttpd, pronounced Lightyis also a free web server that is distributed with the FreeBSD operating system. This open source web server is fast, secure and consumes much less CPU power. Lighttpd can also run on Windows, Mac OS X, Linux and Solaris operating systems.

**Jigsaw Server:** Jigsaw (W3C’s Server) comes from the World Wide Web Consortium. It is open source and free and can run on various platforms like Linux, UNIX, Windows, and Mac OS X Free BSD etc. Jigsaw has been written in Java and can run CGI scripts and PHP programs.

**Security and Vulnerability:**

A vulnerability is a weakness that can be exploited by cybercriminals to gain unauthorized access to a computer system. After exploiting a vulnerability, a cyberattack can run malicious code, install malware and even steal sensitive data.

Vulnerabilities can be exploited by a variety of methods, including SQL injection, buffer overflows, cross size scripting(XSS) , and open-source exploit kits that look for known vulnerabilities and security weakness in web applications.

1. SQL INJECTIONS

SQL injection is a type of web application security vulnerability in which an attacker attempts to use application code to access or corrupt database content. If successful, this allows the attacker to create, read, update, alter, or delete data stored in the back-end database. SQL injection is one of the most prevalent types of web application security vulnerabilities.

2. CROSS SITE SCRIPTING (XSS)

Cross-site scripting (XSS) targets an application's users by injecting code, usually a client-side script such as JavaScript, into a web application's output. The concept of XSS is to manipulate client-side scripts of a web application to execute in the manner desired by the attacker. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface websites or redirect the user to malicious sites.

3. BROKEN AUTHENTICATION & SESSION MANAGEMENT

Broken authentication & session management allows a cybercriminal to steal a user’s login data, or forge session data, such as cookies, to gain unauthorized access to websites.

When a visitor signs in to a website, the site uses a proprietary algorithm to generate a unique session ID. The visitor’s device then uses that session ID as a key to their identity for the remainder of their login session. All of this information has to be sent back and forth between the visitor and the server. If that information is not encrypted and is sent as plain text instead, it’s possible for someone to intercept a visitor’s session ID and/or credentials to impersonate that same visitor. This is especially true when operating on a public network (like a coffee shop wifi) that anyone else can access and possibly intercept.

SSL Certificate is used to protect from Broken authentication & session management

4. INSECURE DIRECT OBJECT REFERENCES

Insecure direct object reference is when a web application exposes a reference to an internal implementation object. Internal implementation objects include files, database records, directories and database keys. When an application exposes a reference to one of these objects in a URL, hackers can manipulate it to gain access to a user's personal data.

5. SECURITY MISCONFIGURATION

Security misconfiguration encompasses several types of vulnerabilities all centered on a lack of maintenance or a lack of attention to the web application configuration. A secure configuration must be defined and deployed for the application, frameworks, application server, web server, database server and platform. Security misconfiguration gives hackers access to private data or features and can result in a complete system compromise.

6. CROSS-SITE REQUEST FORGERY (CSRF)

Cross-Site Request Forgery (CSRF) is a malicious attack where a user is tricked into performing an action he or she didn't intend to do. A third-party website will send a request to a web application that a user is already authenticated against (e.g. their bank). The attacker can then access functionality via the victim's already authenticated browser. Targets include web applications like social media, in browser email clients, online banking, and web interfaces for network devices.

Don't get caught with your guard down. Practice safe website security measures and always be ready to protect yourself, and your company's future, from an attack that you might never recover from. The best way to tell if your website or server is vulnerable is to conduct regular security audits.

**Web System Architecture: (Web Application Architecture) :**

The web system architecture describes the interactions between applications, databases, and middleware systems on the web. It ensures that multiple applications work simultaneously.

Components of Web Applications Architectures

components can be categorized into two areas:

1. user interface app components and
2. structural components.

**1. user interface app components**

This includes activity logs, dashboards, notifications, settings, statistics, etc. These components have nothing to do with the operation of a web application architecture. Instead, they are part of the interface layout plan of a web app.

**2. Structural Components –**

The two major structural components of a web app are client and server sides.

* **Client Component -** The client component is developed in CSS, HTML, and JS. As it exists within the user’s web browser, there is no need for operating system or device-related adjustments. The client component is a representation of a web application’s functionality that the end-user interacts with.
* **Server Component -** The server component can be build using one or a combination of [several programming languages](https://hackr.io/blog/best-programming-languages-to-learn) and frameworks, including Java, .Net, NodeJS, PHP, Python, and Ruby on Rails. The server component has at least two parts; app logic and database. The former is the main control center of the web application while the latter is where all the persistent data is stored.

## Types of Web Application Architecture : There are three primary types of web application architecture. Those are:

1. **Single-Page Applications (SPAs)**
2. **Microservices**
3. **Serverless Architectures**

**1. Single-Page Applications (SPAs)**

Single page web applications interact with the user in a more dynamic fashion by providing updated content within the current page, rather than loading entirely new pages from the server with each action from the user.

AJAX, short for Asynchronous JavaScript and XML, which is the foundation for page communications making SPAs possible.

**2.Microservices –**

These are small and lightweight services that execute a single functionality.

The Microservices Architecture framework has a number of advantages that allows developers to not only enhance productivity but also speed up the entire deployment process.  
The components making up an application build using the Microservices Architecture aren’t directly dependent on each other. As such, they don’t necessitate to be built using the same programming language.

**3. Serverless Architectures –**

In this type of web application architecture, an application developer consults a third-party cloud infrastructure services provider for outsourcing server as well as infrastructure management.  
The benefit of this approach is that it allows applications to execute the code logic without bothering with the infrastructure-related tasks.  
The Serverless Architecture is best when the development company doesn’t want to manage or support the servers .

### **Models of Web Application Components**

Depending on the total number of servers and databases used for a web application, the model of a web app is decided. It can be any of the following three:

### **1. One Web Server, One Database**

It is the most simple as well as the least reliable web app component model. Such a model uses a single server as well as a single database. A web app builds on such a model will go down as soon as the server goes down. Hence, it isn’t much reliable.

One web server, one database web application component model is not typically used for real web applications. It is mostly used for running test projects as well as with the intent of learning and understanding the fundamentals of the web application.

### **2. Multiple Web Servers, One Database (At a Machine Rather than the Web server)**

The idea with this type of web application component model is that the webserver doesn’t store any data. When the webserver gets information from a client, it processes the same and then writes it to the database, which is managed outside of the server. This is sometimes also referred to as a stateless architecture.

At least 2 web servers are required for this web application component model. This is all for avoiding failure. Even when one of the web servers goes down, the other one will take charge.

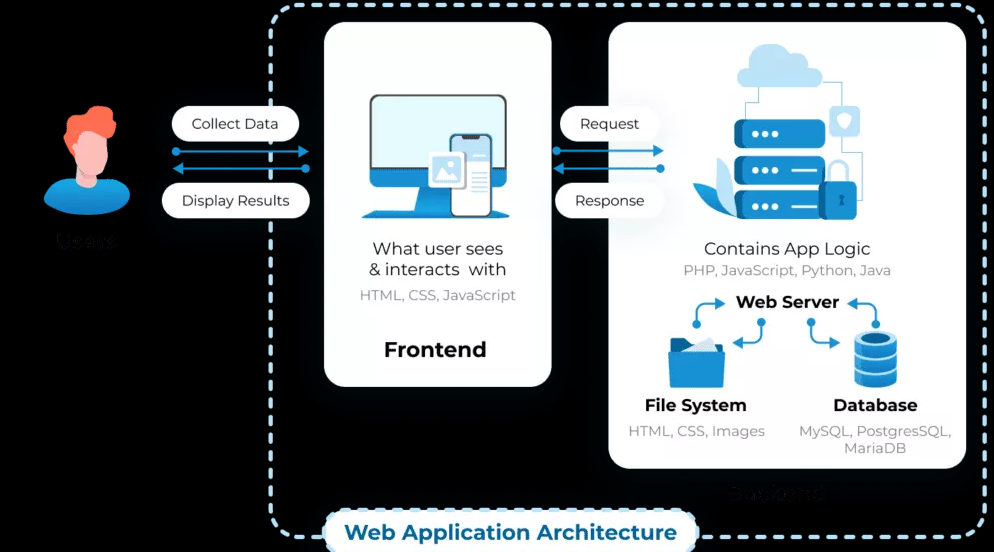
All requests made will be redirected automatically to the new server and the web app will continue execution. Hence, reliability is better as compared to the single server with inherent database model. However, if the database crashes the web app will follow to do the same.

### **3. Multiple Web Server, Multiple Databases**

It is the most efficient web application component model because neither the webservers nor the databases have a single point of failure. There are two options for this type of model. Either to store identical data in all the employed databases or distribute it evenly among them.

Not more than 2 databases are required typically for the former case, while for the latter case some data might become unavailable in the scenario of a database crash. [DBMS normalization](https://hackr.io/blog/dbms-normalization) is used, however, in both scenarios.

When the scale is large i.e. more than 5 web servers or databases or both, it is advised to install load balancers.



**URL:**

URL stands for ***Uniform Resource Locator***that identifies a particular Internet resource. URL helps the user locate a web page, gopher service, library catalogue, image, or text file locations. URLs are the standard addressing system of the www. A complete URL provides the web client with all the information it needs to contact a server and make a request for information.

**Example**: https://www.ecomputernotes.com/software

URLs divided into three essential parts:

1. **Protocol (http ://)** – The information appearing before the colon in any URL indicates the type of information server or [protocol](https://ecomputernotes.com/computernetworkingnotes/computer-network/protocol). For example, http:// indicates that the server to be connected is a www server.
2. **Domain name (www.ecomputernotes.com)** – The second piece of information is the address of the server. In this example, ecomputernotes.com is the name of the machine at PS Exam on the World Wide Web.
3. **Resource name (software.htm)** – The third piece of information is the path to the actual document requested. In this example, the URL indicates that the document in the system directory and is named software.htm.

**Domain Name:**

A domain name is a string of text that maps to a numeric IP address, used to access a website from client software.

[**Structure of domain names**](https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_domain_name#structure_of_domain_names)

A domain name has a simple structure made of several parts (it might be one part only, two, three…), separated by dots and **read from right to left**:



Each of those parts provides specific information about the whole domain name.

[**TLD**](https://developer.mozilla.org/en-US/docs/Glossary/TLD)**(Top-Level Domain).**

TLDs tell users the general purpose of the service behind the domain name. The most generic TLDs (.com, .org, .net) don't require web services to meet any particular criteria.

**Label (or component)**

The labels are what follow the TLD. A label is a case-insensitive character sequence anywhere from one to sixty-three characters in length. The label located right before the TLD is also called a Secondary Level Domain(SLD).A domain name can have many labels

Example: [developer.mozilla.org](https://developer.mozilla.org/), [iot.mozilla.org](https://iot.mozilla.org/), or [bugzilla.mozilla.org](https://bugzilla.mozilla.org/).

## Subdomain

A subdomain is a domain that's part of a larger domain. For example, mail.google.com, www.google.com, and docs.google.com are all subdomains of the domain google.com. Domain owners can create subdomains to provide easy-to-remember addresses for web pages or services within their top-level domain.

**Webserver Administration**

  Web server administrators are system architects responsible for the overall design, implementation, and maintenance of Web servers.

They may or may not be responsible for Web content, which is traditionally the responsibility of the Webmaster.

Specific responsibilities include:

* Coding websites – the most popular languages include HTML and JavaScript
* Collaborating with development teams to program websites
* Setting up tools to monitor website traffic
* Analyzing website traffic to inform design decisions
* Addressing usability issues

**Search Engines**

A search engine is an online answering machine, which is used to search, understand, and organize content's result in its database based on the search query (keywords) inserted by the end-users  (internet user).

The process of organizing content in the form of a list is commonly known as a **Search Engine Results Page (SERP).**

**Google**, **Yahoo!, Bing**, **YouTube**, and **DuckDuckGo** are some popular examples of search engines.

## Advantages of Search Engine

A list of advantages of search engines is given below -

### **1. Time-Saving**

Search engine helps us to save time by the following two ways -

* Eliminate the need to find information manually.
* Perform search operations at a very high speed.

### **2. Variety of information**

The search engine offers various variety of resources to obtain relevant and valuable information from the Internet. By using a search engine, we can get information in various fields such as education, entertainment, games, etc. The information which we get from the search engine is in the form of blogs, pdf, ppt, text, images, videos, and audios.

### **3. Precision**

All search engines have the ability to provide more precise results.

### **4. Free Access**

Mostly search engines such as Google, Bing, and Yahoo allow end-users to search their content for free. In search engines, there is no restriction related to a number of searches, so all end users (Students, Job seekers, IT employees, and others) spend a lot of time to search valuable content to fulfill their requirements.

### **5. Advanced Search**

Search engines allow us to use advanced search options to get relevant, valuable, and informative results. Advanced search results make our searches more flexible as well as sophisticated. For example, when you want to search for a specific site, type **"site:"** without quotes followed by the site's web address.

Suppose we want to search for java tutorial on javaTpoint then type **"java site:www.javatpoint.com"** to get the advanced result quickly.

To search about education institution sites (colleges and universities) for B.Tech in computer science engineering, then use **"computer science engineering site:.edu."** to get the advanced result.

### **6. Relevance**

Search engines allow us to search for relevant content based on a particular keyword. For example, a site "javatpoint" scores a higher search for the term "java tutorial" this is because a search engine sorts its result pages by the relevance of the content; that's why we can see the highest-scoring results at the top of SERP.

## Disadvantages of Search Engine

There are the following disadvantages of Search Engines -

* Sometimes the search engine takes too much time to display relevant, valuable, and informative content.
* Search engines, especially Google, frequently update their algorithm, and it is very difficult to find the algorithm in which Google runs.
* It makes end-users effortless as they all time use search engines to solve their small queries also.

## Search Engine Components are:

Generally there are three basic components of a search engine as listed below:

1. Web Crawler
2. Database
3. Search Interfaces

### **Web crawler**

It is also known as spider or bots**.** It is a software component that traverses the web to gather information.

### **Database**

All the information on the web is stored in database. It consists of huge web resources.

### **Search Interfaces**

This component is an interface between user and the database. It helps the user to search through the database.