

# **CCA-102: Data Communications**

## **ASSIGNMENT**

# 1. What are the different types of networks?

**Ans.**

**A computer network is a system in which multiple computers are connected to share information and resources.** Computer network varies with each other based on their functionality, geography, ownership, and communication media used.

So, in this blog, we are going to learn about various types of computer networks based on geographical areas they cover, functionality, ownership, and communication media used.

**A computer network can be divided into the following types, based on the geographical area that they cover, they are:**

1. **LAN(Local Area Network)**
2. **MAN(Metropolitan Area Network)**
3. **WAN(Wide Area Network)**

Now, let us study these networks one by one:

## **LAN (Local Area Network)**

A local area network is a network, which is designed to operate over a very small geographical or physical area such as an office, building, a group of buildings, etc.

Generally, it is used to connect two or more personal computers through a communication medium such as coaxial, twisted-pair cables, etc. A LAN can use either wired or wireless mode of communication. The LAN which entirely uses wireless media for communication can be termed as **WLAN (Wireless Local Area Network)**.

Local Area Networks came under existence in around 1970s. IEEE developed the specifications for LAN. The speed of this network varies from 10mbps (Ethernet network) to 1gbps (FDDI or Gigabit Ethernet).

In other words, a LAN connects a relatively small number of machines in a relatively close geographical area. Bus, Ring, and Star topology are generally used in a local area network. In LAN, one computer can become a server in a star topology, serving all other computers called clients. Two different buildings can be connected very easily in LAN using a 'Bridge'.

Ethernet LAN is the most commonly used LAN. The speed of a Local Area Network also depends on the topology used. **For example**, a LAN using bus topology has a speed of 10mbps to 100mbps, while in ring topology it is around 4mbps to 16mbps. LAN's are generally privately owned networks.

#### **Following are the functionalities of a Local Area Network:**

1. **File Serving:** In LAN, a large storage disk acts as a central storage repository.
2. **Print Serving:** Printers can be shared very easily in a LAN by various computers.
3. **Academic Support:** A LAN can be used in the classroom, labs, etc. for educational purposes.
4. **Manufacturing Support:** LAN can support the manufacturing and industrial environment.
5. **High Reliability:** Individual workstations might survive the network in case of failures.

#### **Following are the advantages of a LAN:**

1. File transfer and file access
2. Resource or peripherals sharing
3. Personal computing
4. Document distribution

5. Easy to design and troubleshoot
6. Minimum propagation delay
7. High data rate transfer
8. Low error rate
9. Easily scalable(devices can be added or removed very easily)

**Following are the disadvantages of a LAN:**

1. Equipment and support may be costly
2. Some hardware devices may not inter-operate properly

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

A Metropolitan Area Network is a bigger version of LAN that uses similar technology as LAN. It spans over a larger geographical area such as a town or an entire city.

It can be connected using an optical fiber cable as a communication medium. Two or more LAN's can also be connected using routers to create a MAN. When this type of network is created for a specific campus, then it is termed as CAN (Campus Area Network).

The MAN spans over a geographical area of about 50km. The best example of MAN is the cable television network that spans over the whole city.

A MAN can be either a public or privately owned network. Generally, a telephone exchange line is most commonly used as a communication medium in MAN. The protocols that are used in MAN are RS-232, Frame Relay, ISDN, etc.

**Uses of MAN are as follows:**

1. MAN can be used for connecting the various offices of the same organization, spread over the whole city.

2. It can be used for communication in various governmental departments.

**Following are the advantages of using MAN:**

1. Large geographical area cover as compared to LAN
2. High-speed data connectivity
3. The Propagation delay of MAN is moderate

**Following are the disadvantages of MAN:**

1. It is hard to design and maintain a MAN
2. MAN is less fault-tolerant
3. It is costlier to implement
4. Congestions are more in a MAN

## **WAN (Wide Area Network)**

A Wide Area Network is the largest spread network. It spans over very large-distances such as a country, continent or even the whole globe. Two widely separated computers can be connected very easily using WAN. For Example the Internet.

A WAN may include various Local and Metropolitan Area Network. The mode of communication in a WAN can either be wired or wireless. Telephone lines for wired and satellite links for wireless communication can be used in a wide area network.

In other words, WAN provides long distance transmission of data, voice, image, and video, over a large geographical area. A WAN may span beyond 100km range. It may be privately or publicly owned.

The protocols used in WAN are ISDN (Integrated Service Digital Network), SMDS (Switched Multi-Megabit Data Service), SONET(Synchronous Optical

Network), HDLC(High Data Link Control), SDLC(Synchronous Data Link Control), etc.

The advantage of WAN is that it spans over a very large geographical area, and connects a huge mass of people.

**Following are the disadvantages of WAN:**

1. The propagation delay is more in a WAN
2. The data rate is low
3. The error rate is high
4. It is very complex to design a WAN

These are the types of network according to geographical area.

***Following are the types of network, based on functionality:***

- **Client-Server Network:** Client-Server network is a network in which a client runs the program and access data that are stored on the server. In this kind of network, one computer becomes the server, serving all other computers called clients.
- **Peer-to-Peer Network:** Peer-to-Peer network facilitates the flow of information from one peer to another without any central server. In other words, each node on a server acts as both client and server.

***Following are the types of network, based on Ownership:***

- **Private Network:** A private network is a network in which various restrictions are imposed to secure the network, to restrict unauthorized access. This type of network is privately owned by a single or group of people for their personal use. Local Area Network (LAN) can be used as a private network.
- **Public Network:** A public network is a network that has the least or no restrictions on it. It can be freely accessed by anyone, without any restrictions. This type of network is publicly owned by the government

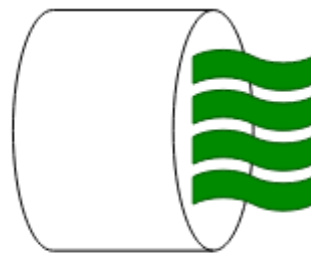
or NGOs. Metropolitan Area Network (MAN) and Wide Area Network (WAN) can be used as a public network.

## **2.Explain the Shielded twisted pair (STP) and Unshielded twisted pair (UTP)**

**Ans.**

### **UTP:**

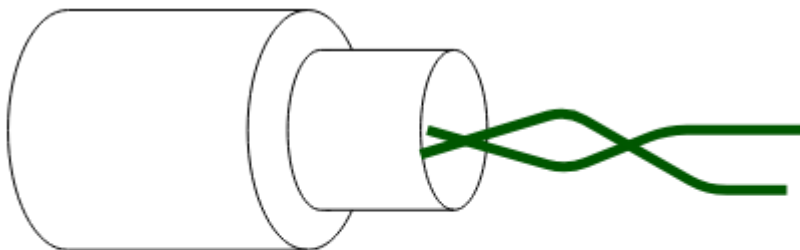
UTP is the type of twisted pair cable. It stands for Unshielded twisted pair. Both Data and voice both are transmitted through UTP because its frequency range is suitable. In UTP grounding cable is not necessary also in UTP much more maintenance are not needed therefore it is cost effective.



**Unshielded Twisted Pair**

### **STP:**

STP is also the type of twisted pair which stands for Shielded twisted pair. In STP grounding cable is required but in UTP grounding cable is not required. in Shielded Twisted Pair (STP) much more maintenance are needed therefore it is costlier than Unshielded Twisted Pair (UTP).



**Shielded Twisted Pair**

## **Difference between Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP) cables:**

S.NO	UTP	STP
1.	UTP stands for Unshielded twisted pair.	STP stands for Shielded twisted pair.
2.	In UTP grounding cable is not necessary.	While in STP grounding cable is required.
3.	Data rate in UTP is slow compared to STP.	Data rate in STP is high.
4.	The cost of UTP is less.	While STP is costlier than UTP.
5.	In UTP much more maintenance are not needed.	While in STP much more maintenance are needed.
6.	In UTP noise is high compared to STP.	While in STP noise is less.
7.	In UTP the generation of crosstalk is also high compared to STP.	While in STP generation of crosstalk is also less.
8.	In UTP, attenuation is high in comparison to STP.	While in STP attenuation is low.

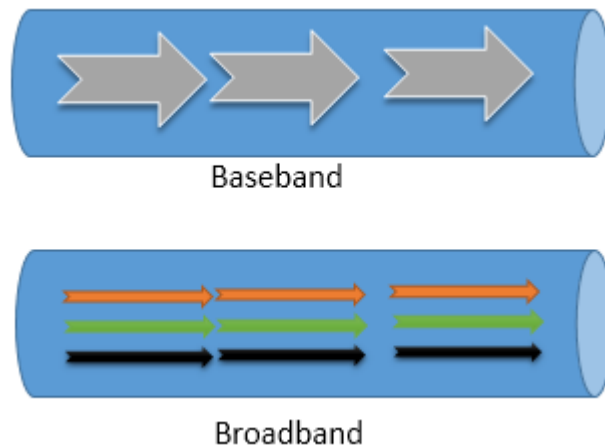
## **3. What is difference between baseband and broadband transmission?**

### **Ans.**

Both baseband and broadband describe how data is transmitted between two nodes. Baseband technology transmits a single data signal/stream/channel at a time while broadband technology transmits multiple data signals/streams/channels simultaneously at the same time.

The following image shows an example of both technologies.





To understand the basic differences between both technologies, consider the baseband as a railway track and the broadband as a highway. Like, at a time, only one train can go on a railway track, in the baseband transmission only one data signal can be transmitted at a time.

Unlike a railway track on a highway, multiple vehicles can go simultaneously. For example, on a 3 lanes highway, 3 vehicles can go at the same time. Same as a highway, in the broadband transmission, multiple data signals can be transmitted at the same time.

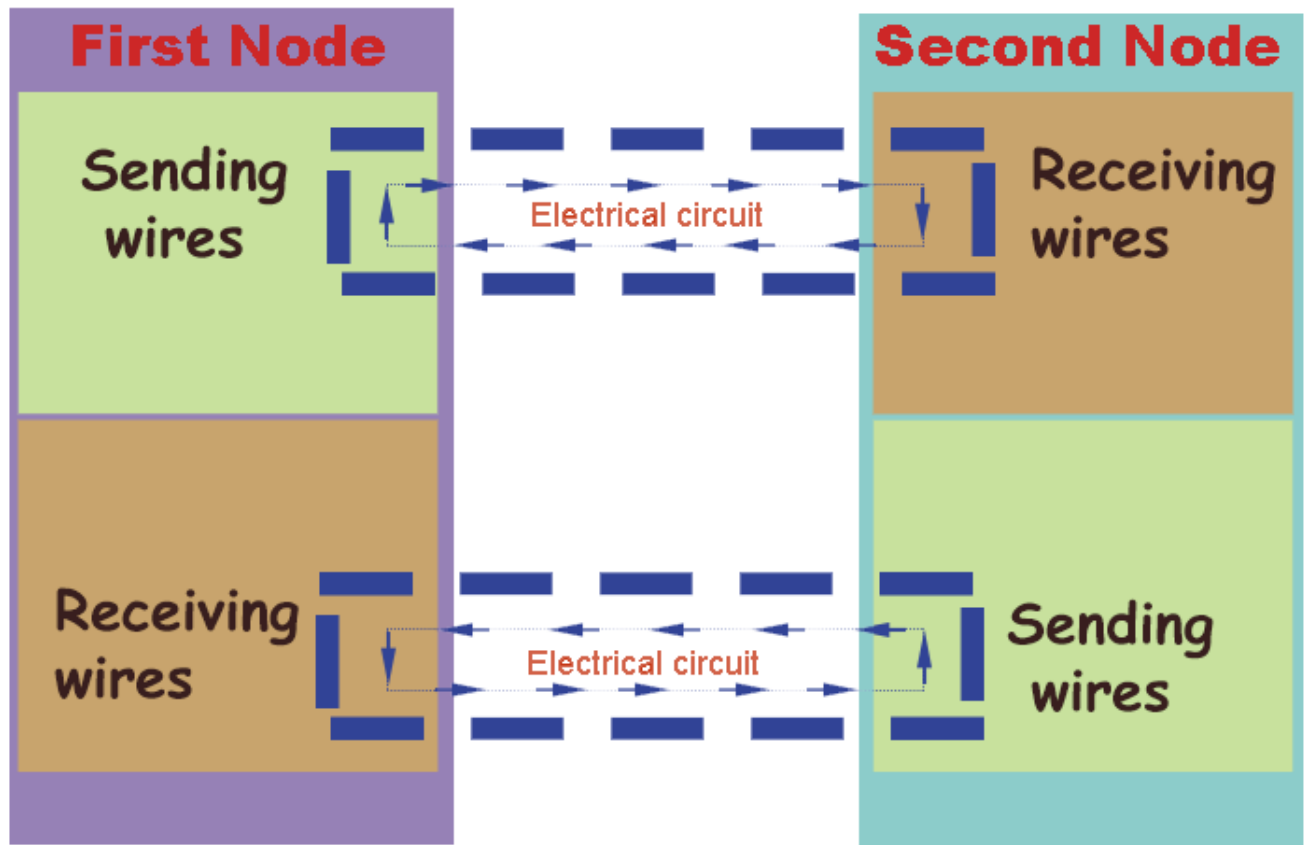


Technical differences between the baseband and broadband transmissions

Baseband technology uses digital signals in data transmission. It sends binary values directly as pulses of different voltage levels. Digital signals can be regenerated using repeaters in order to travel longer distances before weakening and becoming unusable because of attenuation.

Baseband supports bidirectional communication. It means, this technology can send and receive data simultaneously. To support bidirectional communication, this technology uses two separate electric circuits together; one for sending and another for receiving.

The following image shows an example of this.



Although baseband transmits only a single data stream at a time, it is possible to transmit signals of multiple nodes simultaneously. This is done by combining all the signals into a single data stream. To combine the signals of multiple nodes, a technology known as multiplexing is used. Baseband supports the Time Division Multiplexing (TDM).

To learn the types of multiplexing and how the multiplexing is done, you can check this [tutorial](#).

### Multiplexing and Demultiplexing Explained with Types

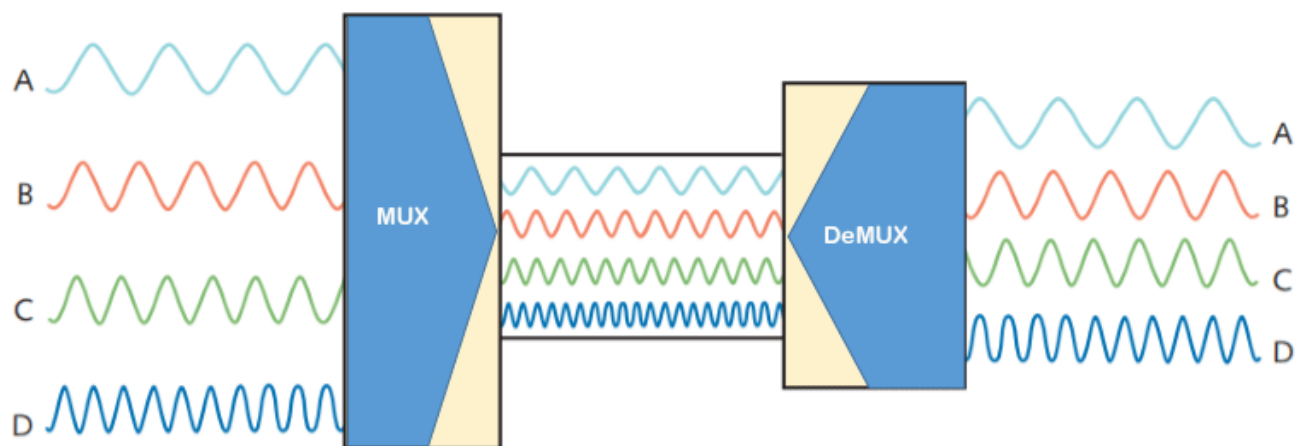
Baseband technology is mainly used in Ethernet networks to exchange data between nodes. This technology can be used on all three popular cable media types of Ethernet; coaxial, twisted-pair, fiber-optic.

### Broadband transmission

Broadband technology uses analog signals in data transmission. This technology uses a special analog wave known as the **carrier wave**. A carrier wave does not contain any data but contains all properties of the analog signal. This technology mixes data/digital signal/binary values into the carrier wave and sends the carrier wave across the channel/medium.

To transmit data of multiple nodes simultaneously, this technology supports the Frequency Division Multiplexing. FDM (Frequency Division Multiplexing) divides the channel (medium or path) into several sub-channels and assigns a sub-channel to each node. Each sub-channel can carry a separate carrier wave.

The following image shows an example of this process.

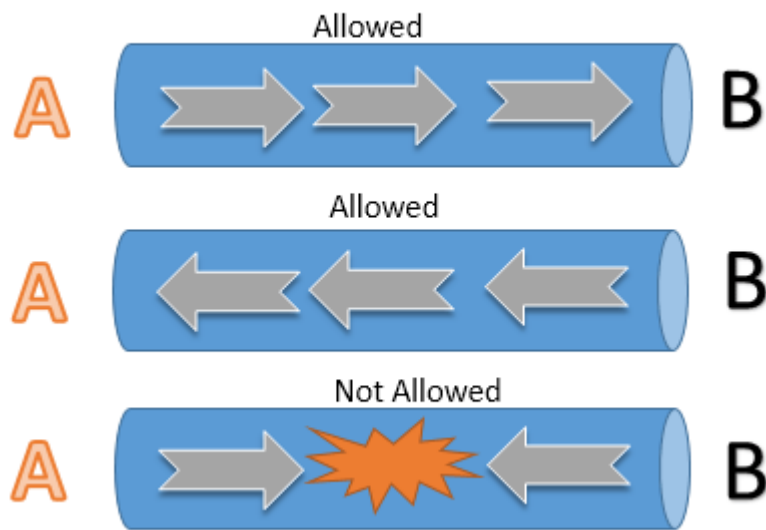


Analog signals can be regenerated using amplifiers in order to travel longer distances.

Broadband supports only unidirectional communication. It means, nodes connected at both ends of a medium can send or receive data but can't perform both actions simultaneously. Only one action is allowed at a time.

For example, two nodes A and B are connected through a cable that uses broadband technology to transmit signals. When node A transmits signals, node B receives the transmitted signals and when node B transmits signals, node A receives the transmitted signals.

The following image shows this example.



Broadband is typically used in an environment that transmits audio, video, and data simultaneously. For example, Cable TV Networks, Radio stations, and Telephone companies. Usually radio waves, coaxial, fiber-optic cables are used for broadband transmission.

Key differences between baseband and broadband transmissions

Baseband transmission	Broadband transmission
Transmit digital signals	Transmit analog signals
To boost signal strength, use repeaters	To boost signal strength, use amplifiers
Can transmit only a single data stream at a time	Can transmit multiple signal waves at a time
Support bidirectional communication simultaneously	Support unidirectional communication only
Support TDM based multiplexing	Support FDM based multiplexing
Use coaxial, twisted-pair, and fiber-optic cables	Use radio waves, coaxial cables, and fiber optic cables
Mainly used in Ethernet LAN networks	Mainly used in cable and telephone networks

#### 4. What is the difference between a hub, modem, router and a switch?

**Ans.**

## Hub

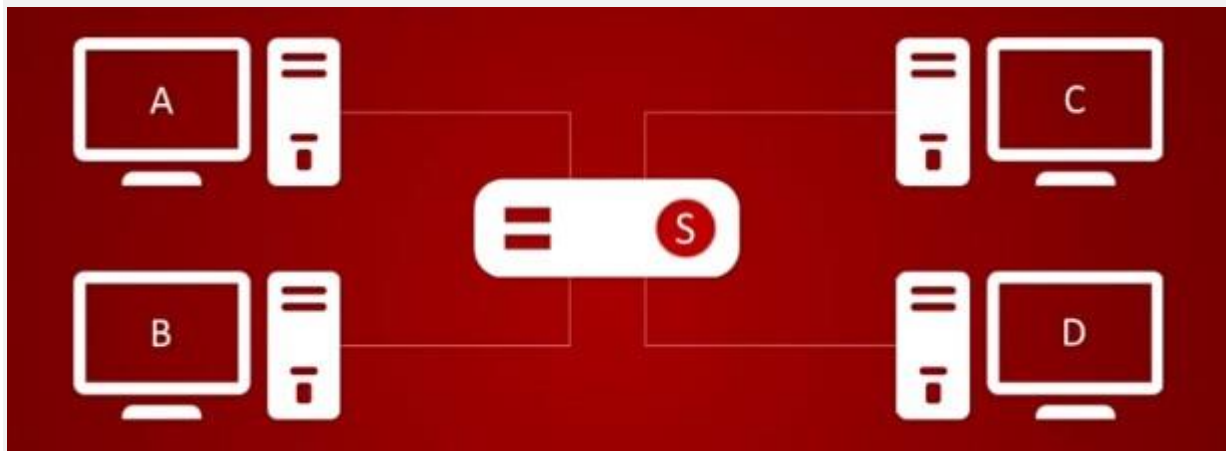
A hub is to send out a message from one port to other ports. For example, if there are three computers of A, B, C, the message sent by a hub for computer A will also come to the other computers. But only computer A will respond and the response will also go out to every other port on the hub. Therefore, all the computers can receive the message and computers themselves need to decide whether to accept the message



## Switch

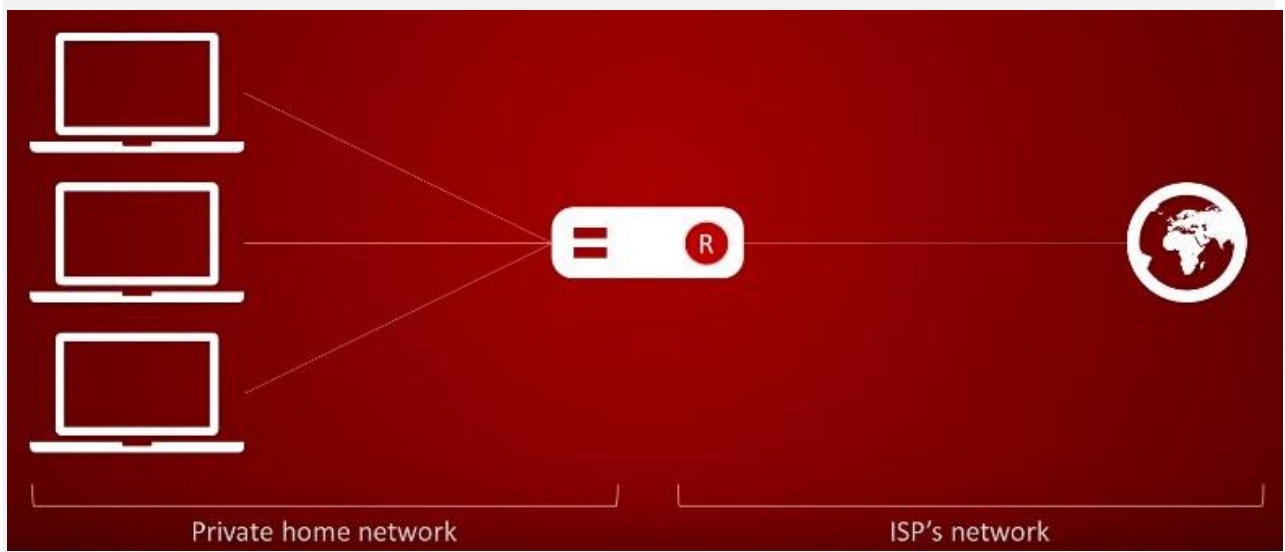
A switch is able to handle the data and knows the specific addresses to send the message. It can decide which computer is the message intended for and send the message directly to the right computer.

The efficiency of switch has been greatly improved, thus providing a faster network speed.



## Router

Router is actually a small computer that can be programmed to handle and route the network traffic. It usually connects at least two networks together, such as two LANs, two WANs or a LAN and its ISP network. Routers can calculate the best route for sending data and communicate with each other by protocols.



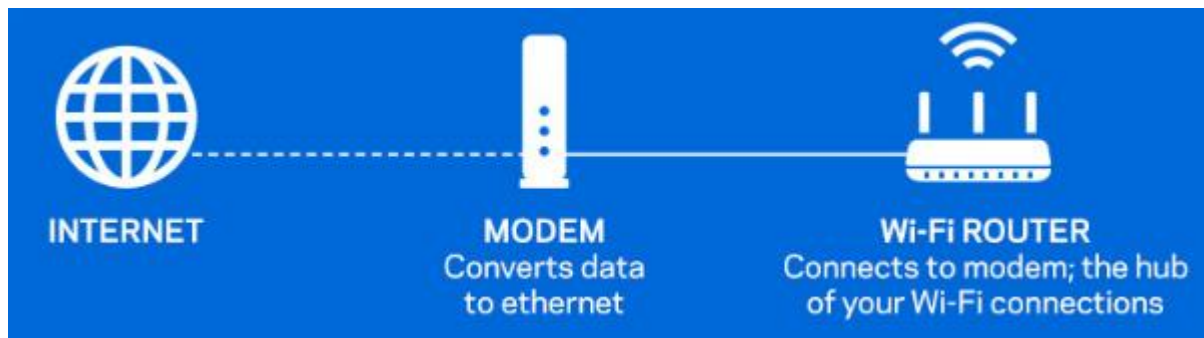
## modem



Nowadays, we don't just use the Internet, we rely on it. When the connection is slow—or worse, nonexistent—your whole day could be ruined. But have you ever stopped to think about how that connection works? From Wi-Fi router to mobile devices, the components that make up your home network all speak different digital languages, but your modem is the translator. It takes the signals that come from your Internet Service Provider, or ISP, and translates them into an Internet connection for

your Wi-Fi router to broadcast. On a basic level, your modem gives you access to the Web, but it can also make a huge difference in the efficiency of your home Wi-Fi.

## How a Modem Works



The modem receives information from your ISP through the phone lines, optical fiber, or coaxial cable in your home (depending on your service provider) and converts it into a digital signal. The router's job is to push this signal out to connected devices, either through wired Ethernet cables or Wi-Fi, so that all of your devices can hop on board and access the Internet. Your router and ISP can't communicate directly because they speak different languages—or rather, they transmit different signal types—which is why the modem's role as a translator is so important.

### 5. When you move the NIC cards from one PC to another PC, does the MAC address gets transferred as well?

**Ans.** Yes, that's because MAC addresses are hard-wired into the NIC circuitry, not the PC. This also means that a PC can have a different MAC address when another one replaced the NIC card

### 6. When troubleshooting computer network problems, what common hardware-related problems can occur?.

**Ans.**

A large percentage of a network is made up of hardware. Problems in these areas can range from malfunctioning hard drives, broken NICs and even hardware startups. Incorrectly hardware configuration is also one of those culprits to look into.

### 7. In a network that contains two servers and twenty workstations, where is the best place to install an Anti-virus program?

**Ans.**



An anti-virus program must be installed on all servers and workstations to ensure protection. That's because individual users can access any workstation and introduce a computer virus when plugging in their removable hard drives or flash drives.

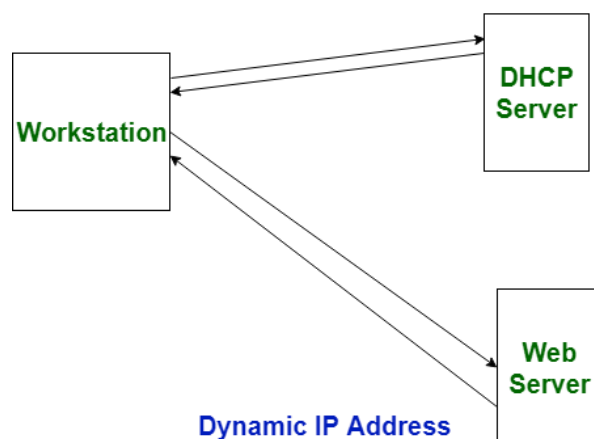
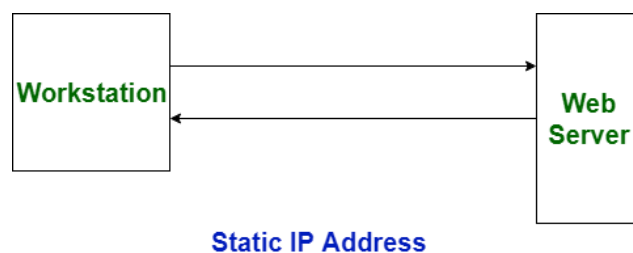
### 8. Define Static IP and Dynamic IP? Discuss the difference between IPV4 and IPV6.

Ans

## Difference between Static and Dynamic IP address

**IP** stands for **Internet Protocol**. IP address may be a distinctive numerical symbol allotted to every device on a network to spot each affiliation unambiguously.

The distinction between Static and Dynamic IP address lies inside the length of allotted scientific discipline address. The static scientific discipline address is fastened scientific discipline address that is manually allotted to a tool for a protracted amount of your time. On the opposite hand, the Dynamic scientific discipline address oft changes whenever user boots his/her machine, and it's mechanically allotted.



## **Difference between Static and Dynamic IP address:**

S.NO	Static IP Address	Dynamic IP address
1.	It is provided by ISP(Internet Service Provider).	While it is provided by DHCP (Dynamic Host Configuration Protocol).
2.	Static ip address does not change any time, it means if a static ip address is provided then it can't be changed or modified.	While dynamic ip address change any time.
3.	Static ip address is less secure.	While in dynamic ip address, there is low amount of risk than static ip address's risk.
4.	Static ip address is difficult to designate.	While dynamic ip address is easy to designate.
5.	The device designed by static ip address can be trace.	But the device designed by dynamic ip address can't be trace.
6.	Static ip address is more stable than dynamic ip address.	While dynamic ip address is less stable than static ip address.
7.	The cost to maintain the static ip address is higher than dynamic ip address.	While the maintaining cost of dynamic ip address is less than static ip address.
8.	It is used where computational data is less confidential.	While it is used where data is more confidential and needs more security.

## What is IPv4?

IPv4 was the first version of IP. It was deployed for production in the ARPANET in 1983. Today it is most widely used IP version. It is used to identify devices on a network using an addressing system.

The IPv4 uses a 32-bit address scheme allowing to store  $2^{32}$  addresses which is more than 4 billion addresses. Till date, it is considered the primary Internet Protocol and carries 94% of Internet traffic.

## What is IPv6?

It is the most recent version of the Internet Protocol. Internet Engineer Taskforce initiated it in early 1994. The design and development of that suite is now called IPv6.

Basis for differences	IPv4	IPv6
Size of IP address	IPv4 is a 32-Bit IP Address.	IPv6 is 128 Bit IP Address.
Addressing method	IPv4 is a numeric address, and its binary bits are separated by a dot (.)	IPv6 is an alphanumeric address whose binary bits are separated by a colon (:). It also contains hexadecimal.
Number of header fields	12	8
Length of header field	20	40
Checksum	Has checksum fields	Does not have checksum fields
Example	12.244.233.165	2001:0db8:0000:0000:0000:ff00:0042:7879
Type of Addresses	Unicast, broadcast, and multicast.	Unicast, multicast, and anycast.
Number of classes	IPv4 offers five different classes of IP Address. Class A to E.	IPv6 allows storing an unlimited number of IP Address.
Configuration	You have to configure a newly installed system before it can communicate with other systems.	In IPv6, the configuration is optional, depending upon on functions needed.
VLSM support	IPv4 support VLSM (Virtual Length Subnet Mask).	IPv6 does not offer support for VLSM.
Fragmentation	Fragmentation is done by the sender.	Fragmentation is done by the sender.

Basis for differences	IPv4	IPv6
	by sending and forwarding routes.	
Routing Information Protocol (RIP)	RIP is a routing protocol supported by the routed daemon.	RIP does not support IPv6. It uses static routes.
Network Configuration	Networks need to be configured either manually or with DHCP. IPv4 had several overlays to handle Internet growth, which require more maintenance efforts.	IPv6 support autoconfiguration capabilities.
Best feature	Widespread use of NAT (Network address translation) devices which allows single NAT address can mask thousands of non-routable addresses, making end-to-end integrity achievable.	It allows direct addressing because of vast address Space.
Address Mask	Use for the designated network from host portion.	Not used.
SNMP	SNMP is a protocol used for system management.	SNMP does not support IPv6.
Mobility & Interoperability	Relatively constrained network topologies to which move restrict mobility and interoperability capabilities.	IPv6 provides interoperability and mobility capabilities which are embedded in network devices.
Security	Security is dependent on applications - IPv4 was not designed with security in mind.	IPSec(Internet Protocol Security) is built into the IPv6 protocol, usable with a proper key infrastructure.
Packet size	Packet size 576 bytes required, fragmentation optional	1208 bytes required without fragmentation
Packet fragmentation	Allows from routers and sending host	Sending hosts only
Packet header	Does not identify packet	Packet head contains Flow Label field that

Basis for differences	IPv4	IPv6
	flow for QoS handling which includes checksum options.	specifies packet flow for QoS handling
DNS records	Address (A) records, maps hostnames	Address (AAAA) records, maps hostnames
Address configuration	Manual or via DHCP	Stateless address autoconfiguration using Internet Control Message Protocol version 6 (ICMPv6) or DHCPv6
IP to MAC resolution	Broadcast ARP	Multicast Neighbour Solicitation
Local subnet Group management	Internet Group Management Protocol (IGMP)	Multicast Listener Discovery (MLD)
Optional Fields	Has Optional Fields	Does not have optional fields. But Extension headers are available.
IPSec	Internet Protocol Security (IPSec) concerning network security is optional	Internet Protocol Security (IPSec) Concerning network security is mandatory
Dynamic host configuration Server	Clients have approach DHCP (Dynamic Host Configuration server) whenever they want to connect to a network.	A Client does not have to approach any such server as they are given permanent addresses.
Mapping	Uses ARP (Address Resolution Protocol) to map to MAC address	Uses NDP (Neighbour Discovery Protocol) to map to MAC address
Compatibility with mobile devices	IPv4 address uses the dot-decimal notation. That's why it is not suitable for mobile networks.	IPv6 address is represented in hexadecimal, colonated notation. IPv6 is better suited to mobile networks.

## 9. Discuss TCP/IP model in detail.

Ans

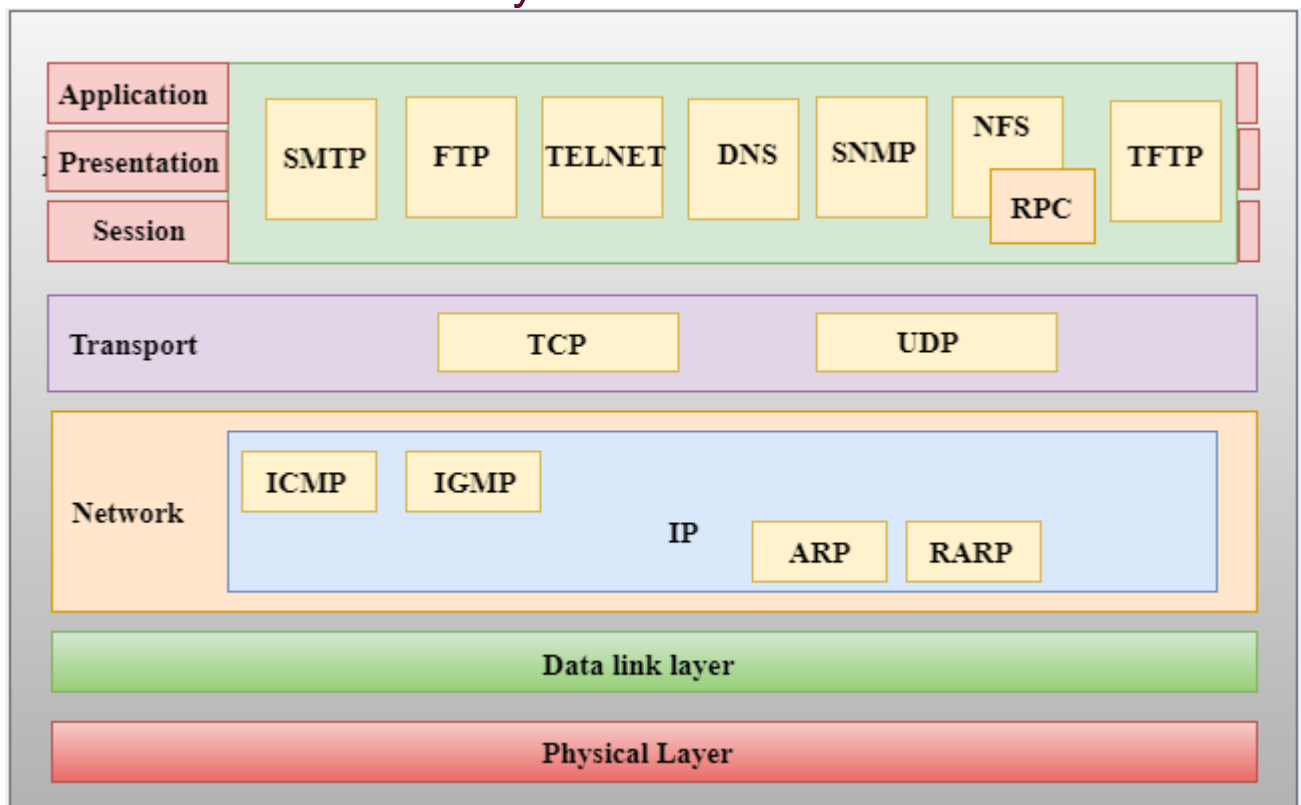
### TCP/IP model

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.

- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

## Functions of TCP/IP layers:



## Network Access Layer

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.

- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

## Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Following are the protocols used in this layer are:

**IP Protocol:** IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

## ARP Protocol

- ARP stands for **Address Resolution Protocol**.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- **The two terms are mainly associated with the ARP Protocol:**
  - **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
  - **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

## ICMP Protocol

- **ICMP** stands for Internet Control Message Protocol.
  - It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
  - A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
  - An ICMP protocol mainly uses two terms:
    - **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
    - **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.
  - The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
  - ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.
-

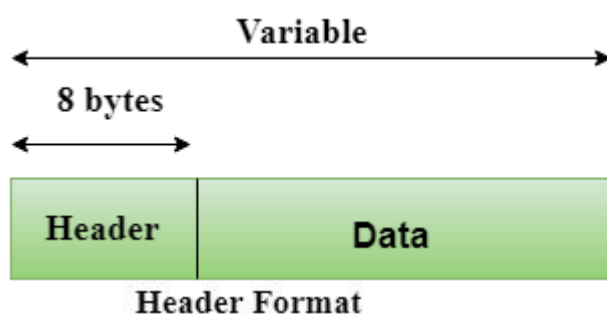


## Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol.**

- **User Datagram Protocol (UDP)**
  - It provides connectionless service and end-to-end delivery of transmission.
  - It is an unreliable protocol as it discovers the errors but not specify the error.
  - User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
  - **UDP consists of the following fields:**
    - Source port address:** The source port address is the address of the application program that has created the message.
    - Destination port address:** The destination port address is the address of the application program that receives the message.
    - Total length:** It defines the total number of bytes of the user datagram in bytes.
    - Checksum:** The checksum is a 16-bit field used in error detection.
  - UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.



Source port address 16 bits	Destination port address 16 bits
Total length 16 bits	Checksum 16 bits

- **Transmission Control Protocol (TCP)**
  - It provides a full transport layer services to applications.

- It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
  - TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
  - At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
  - At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.
- 

## Application Layer

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

### Following are the main protocols used in the application layer:

- **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.
- **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.

- **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
- **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
- **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

## 10.What is a Web Browser (Browser)? Give some example of browsers.

Ans

# Web Browser

---

A web browser, or simply "browser," is an [application](#) used to access and view [websites](#). Common web browsers include Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, and Apple Safari.

The primary function of a web browser is to render [HTML](#), the code used to design or "mark up" [webpages](#). Each time a browser loads a web page, it processes the HTML, which may include text, [links](#), and references to images and other items, such as [cascading style sheets](#) and [JavaScript](#) functions. The browser processes these items, then renders them in the browser window.

Early web browsers, such as Mosaic and Netscape Navigator, were simple applications that rendered HTML, processed form input, and supported [bookmarks](#). As websites have evolved, so have web browser requirements. Today's browsers are far more advanced, supporting multiple types of HTML (such as [XHTML](#) and HTML 5), dynamic JavaScript, and [encryption](#) used by secure websites.

The capabilities of modern web browsers allow [web developers](#) to create highly interactive websites. For example, [Ajax](#) enables a browser to dynamically update information on a webpage without the need to reload the page. Advances in CSS allow browsers to display a [responsive website](#) layouts and a wide array of visual effects. [Cookies](#) allow browsers to remember your settings for specific websites.

While web browser technology has come a long way since Netscape, browser compatibility issues remain a problem. Since browsers use different rendering engines, websites may not appear the same across multiple browsers. In some cases, a website may work fine in one browser, but not function properly in another. Therefore, it is smart to [install](#) multiple browsers on your computer so you can use an alternate browser if necessary.

Some examples of browsers can be found below.

## 5 Popular Browsers

### 1. Google Chrome

Chrome, created by internet giant Google, is the most popular browser in the USA, perceived by its computer and smartphone users as fast, secure, and reliable. There are also many options for customization in the shape of useful extensions and apps that can be downloaded for free from the Chrome Store. Chrome also allows easy integration with other Google services, such as Gmail. Due to the success of the "Chrome" brand name, Google has now extended it to other products, for example, Chromebook, Chromebox, Chromecast, and Chrome OS.

### 2. Apple Safari

Safari is the default on Apple computers and phones, as well as other Apple devices. It's generally considered to be an efficient browser, its slick design being in keeping with the ethos of Apple. Originally developed for Macs, Safari has become a significant force in the mobile market due to the domination of iPhones and iPads. Unlike some of the other browsers listed, Safari is exclusive to Apple, it doesn't run on Android devices, and the Windows version of Safari is no longer supported by important security updates from Apple.

### 3. Microsoft Internet Explorer and Edge

Although it has been discontinued, Internet Explorer is worthy of mention as it was the go-to browser in the early days of the internet revolution, with usage share rising to 95% in 2003. However, its relatively slow start-up speed meant that many users turned to Chrome and Firefox in the years that followed. In 2015, Microsoft announced that Microsoft Edge would replace Internet Explorer as the default browser on Windows 10, making Internet Explorer 11 the final version to be released. At the time of writing, the market share of Microsoft Edge remains lower than Internet Explorer, which is still used by many people around the world.

## 4. Mozilla Firefox

Unlike Chrome, Safari, Internet Explorer, and Microsoft Edge, Firefox is an open-source browser, created by community members of the Mozilla Foundation. It is perhaps the most customizable of the main browsers, with many add-ons and extensions to choose from. In late 2003, it had a usage share of 32.21% before gradually losing out to competition from Google Chrome. It currently remains a strong competitor in the "desktop" field but has a lower market share in the mobile arena, where Google Chrome and Apple Safari tend to dominate.

## 5. Opera

Another web browser worthy of mention is Opera, which is designed for Microsoft Windows, Android, iOS, macOS, and Linux operating systems. It has some interesting features and is generally considered to be a reliable option by many users. Many of its earlier features have gone on to be incorporated into rival browsers. It also has a distinct user interface. At the time of writing, Opera has a usage of just 2.28% but remains influential, albeit from the fringes.

# 11.What is a search engine? Give example.

**Ans**

## What Is a Search Engine?

Also known as a web search engine and an internet search engine, a search engine is a (usually web-based) computer program that collects and organizes content from all over the internet. The user enters a query composed of keywords or phrases, and the search engine responds by providing a list of results that best match the user's query. The results can take the form of links to websites, images, videos, or other online data.

## How Do Search Engines Work?

The work of a search engine can be broken down into three stages. Firstly, there is the process of discovering the information. Secondly, there is the organization of the information so that it can be effectively accessed and presented when users search for something. Thirdly, the information must be assessed to present search engine users with relevant answers to their queries.

These three stages are usually called crawling, indexing, and ranking.

### Crawling

Search engines use pieces of software called web crawlers to locate publicly available information from the internet, which is why this process is known as crawling. Web crawlers can also sometimes be referred to as search engine spiders. The process is

complicated, but essentially the crawlers/spiders find the web servers (also known as just servers for short) which host the websites and then proceed to investigate them.

A list of all the servers is created, and it is established how many websites are hosted on each server. The number of pages each website has, as well as the nature of the content, for example, text, images, audio, video, is also ascertained. The crawlers also follow any links that the website has, whether internal ones that point to pages within the site, or external ones that point to other websites and use them to discover more pages.

## **Indexing**

Information found by the crawlers is organized, sorted, and stored so that it can later be processed by the algorithms for presentation to the search engine user. This is known as indexing. Not all the page information is stored by the search engine, instead, it's just the essential information needed by the algorithms to assess the relevance of the page for ranking purposes.

## **Ranking**

When a query is entered into a search engine, the index is scoured for relevant information and then sorted into a hierarchical order by an algorithm. This ordering of the search engine results pages (SERPS) is known as ranking.

Different search engines use different algorithms, and so give different results. Over the years, algorithms have become more and more complex as they attempt to present more relevant and accurate answers in response to the queries of search engine users.

# **10 Examples of Search Engines**

## **1. Google**

Google is the biggest search engine in the world by far. It handles over 5 billion searches each day and has a market share of over 90% at the time of writing (August 2019). Developed originally by Larry Page and Sergey Brin in 1997, Google has become so successful that it has become synonymous with search engine services, even entering the dictionary as a verb, with people using expressions such as: "I googled it" when they've searched for something online.

## **2. Bing**

The origins of Microsoft's Bing can be found in the technology company's earlier search engines, MSN Search, Windows Live Search, and Live Search. Bing was launched in 2009 with high hopes that it could usurp its rival Google, but despite attracting many fans, things haven't quite worked out that way. Even so, Bing is the third largest search engine worldwide after Google and Baidu. It is available in 40 different languages.

### **3. Yahoo!**

Yahoo! Search is another big player in the search engine world. However, for much of its history it has supplied the user interface, but relied on others to power the searchable index and web crawling. From 2001 to 2004, it was powered by Inktomi and then Google. From 2004, Yahoo! Search was independent until a deal was struck with Microsoft in 2009 whereby Bing would power the index and crawling.

### **4. Ask.com**

Originally known as Ask Jeeves, Ask.com is a little different from Google and Bing, as it uses a question and answer format. For a number of years, Ask.com was focused on becoming a direct rival to the big search engines, but nowadays, answers are supplied from its vast archive and users contributions, along with the help of an unnamed and outsourced third-party search provider.

### **5. Baidu**

Founded in the year 2000 by Robin Li and Eric Xu, Baidu is the most popular search engine in China, and the fourth most visited website in the world, according to [Alexa rankings](#). Baidu has its origins in RankDex, a search engine previously developed by Robin Li in 1996. As well as its Chinese search engine, Baidu also offers a mapping service called Baidu Maps and more than 55 other internet-related services.

### **6. AOL.com**

AOL, now styled as Aol. and originally known as America Online, was a big player in the early days of the internet revolution, providing a dial-up service for millions of Americans in the late 1990's. Despite AOL's decline as broadband gradually replaced dial-up, the AOL search engine is still used by a significant minority of searchers. On June 23, 2015, AOL was acquired by Verizon Communications.

### **7. DuckDuckGo**

DuckDuckGo (DDG) has a number of features that distinguish it from its main competitors. It has a strong focus on protecting searchers' privacy, so rather than profiling users and presenting them with personalized results, it provides the same search results for any given search term. There's also an emphasis on providing quality rather than quantity when it comes to search results. DDG's interface is very clean and not overladen with adverts.

### **8. WolframAlpha**

WolframAlpha markets itself as a computational knowledge engine. Instead of answering the queries of searchers with a list of links, it responds with mathematical and scientific answers for their questions, using externally sourced "curated data". WolframAlpha was launched in 2009 and has become a valuable tool for academics and researchers.

## 9. Yandex

Launched in 1997, Yandex is Russia's largest search engine, and the country's fourth most popular website. Outside of Russia, the search engine also has a major presence in Ukraine, Belarus, Kazakhstan, and other countries of the Commonwealth of Independent States. As well as search, Yandex offers many other internet-related products and services, including maps and navigation, music, eCommerce, mobile applications, and online advertising.

## 10. Internet Archive

The Internet Archive provides free public access to a wide range of digital materials. A nonprofit digital library based in San Francisco, it's a great tool for tracing the history domains and seeing how they have evolved over the years. Besides websites, you can also find software applications and games, movies/videos, music, moving images, and a huge collection of public-domain books. The Internet Archive also campaigns for a free and open internet.

# 12. What is the Internet & WWW? What are the uses of internet in our daily life?

Ans

### WWW and Internet

The terms World Wide Web (WWW) and the Internet are so often used interchangeably that the fundamental difference between the two is easily forgotten.

In simple words, WWW is just a common point of connectivity for information sharing that is facilitated by a global network of computers.

The internet, on the other hand, is a connection between computers and countless other devices that form a huge network of systems.

#### Differences between WWW and Internet

WWW (World Wide Web)	Internet
The World Wide Web is the common system for navigating the internet. It is not the only system that can be used for such access, but it is by far the most common one.	The internet is a public network of network with a maze of wired and wireless connections between separate groups of servers computers and countless devices from around the world
The World Wide Web is distinguished from other systems through its use of HTTP (Hypertext Transfer Protocol). It can be safely said that the HTTP is the language of the World Wide Web	Along with Internters, there also exist the Intranets, which is the same type of information network but more privatized in order to control access.



WWW is more software-oriented as compared to the Internet	Internet is primarily hardware-based.
The HTTP along with being the language of the World Wide Web also governs it by dealing with linking of files, documents and other resources	The internet is governed by a set of rules and regulations collectively known as Internet Protocol (IP). The IP deals with data transmitted through the internet.
The invention of the World Wide Web can be credited to Sir Tim Berners Lee. During his work at the European Organization for Nuclear Research in 1989, he had developed the basic idea of the WWW to merge the evolving technologies of computers, data networks and hypertext into a powerful and easy to use global information system.	The first workable prototype of the Internet was the ARPANET (Advanced Research Project Agency Network) in the late 1960s. After its adoption on January 1st 1983, researchers began to develop a “network of networks” which evolved into the modern form of the Internet

## Importance Of Internet Technology For Easy Life



Today, the internet has become unavoidable in our daily life. Appropriate use of the internet makes our life easy, fast and simple. The internet helps us with facts and figures, information and knowledge for personal, social and economic development. There are many uses of the internet, however, the use of the internet in our daily life depends on individual requirements and goals.

### 1. Uses of the Internet in Education

The Internet is a great platform for students to learn throughout their lifetime. They can use the internet to learn new things and even acquire degrees through online education programs. Teachers can also use the internet to teach students around the world.

## **2. Internet Use to Speed Up Daily Tasks**

The Internet is very much useful in our daily routine tasks. For example, it helps us to see our notifications and emails. Apart from this, people can use the internet for money transfers, shopping order online food, etc.

## **3. Use of the Internet for Shopping**

With the help of the internet, anybody can order products online. The increase in online shopping has also resulted in companies offering a huge discount for their customers.

## **4. Internet for Research & Development**

The Internet plays a pivotal role in research and development as it is propelled through internet research. The benefit of the internet is enjoyed by small businessmen to big universities.

## **5. Business Promotion and Innovation**

The Internet is also used to sell products by using various e-Commerce solutions. The result is new services and businesses starting every day thereby creating job opportunities and reducing unemployment.

## **6. Communication**

Without a doubt, the internet is the most powerful medium of communication at present. It connects people across different parts of the world free and fast.

## **7. Digital Transactions**

The internet facilitates internet banking, mobile banking, and e-wallets. Since all digital transactions are stored in a database, it helps the government to track income tax details or income reports in the ITR.

## **8. Money Management**

The internet can also be used to manage money. Now, there are many websites, applications, and other tools that help us in daily transactions, transfers, management, budget, etc.

## **9. Tour & Travel**

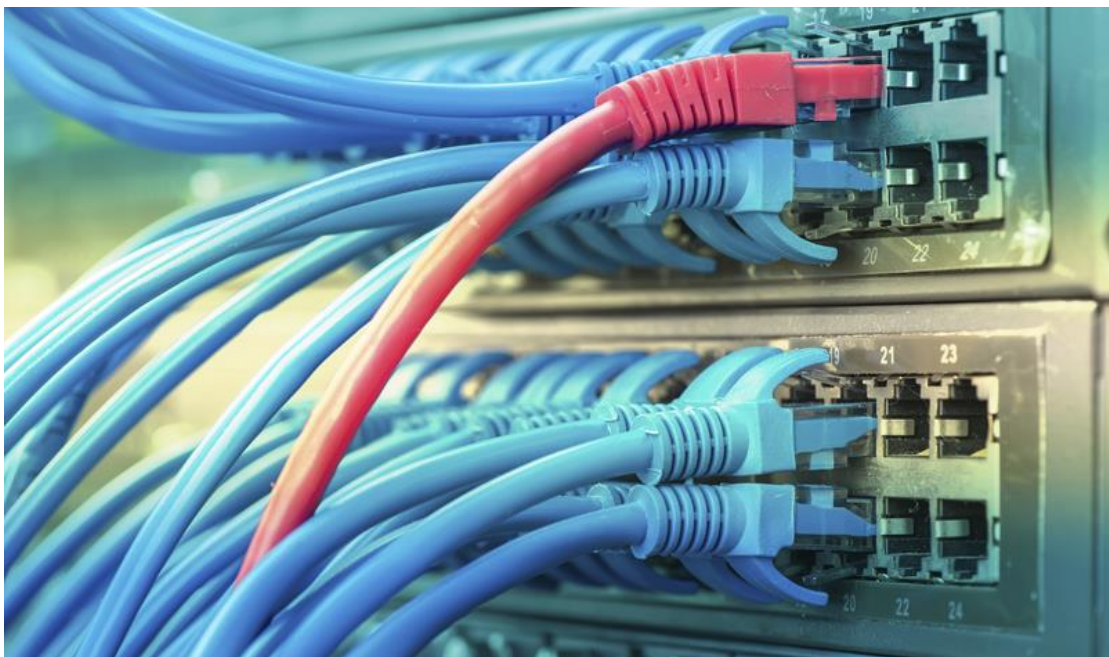
During tour and travel, the use of the internet is highly effective as it serves as a guide. People browse the internet before they start visiting the places. Tour bookings can also be done using the internet.

The influence of the internet in our daily life is huge. It has opened us a magical world of information and we would have never seen the world as it is without the internet. Considering its scope and importance, it would be hard to imagine a world without the internet.

**13. What is an Internet Service Provider? Give some example of ISP in India**

Ans

## What is an Internet Service Provider?



An Internet Service Provider (ISP) is the industry term for the company that is able to provide you with access to the Internet, typically from a computer. If you hear someone talking about the Internet and they mention their “provider,” they’re usually talking about their ISP.

Your ISP makes the Internet a possibility. In other words, you can have a shiny computer with a built-in modem and could have a router for networking, but without a subscription with an ISP, you won’t have a connection to the Internet.

For the typical homeowner or apartment dweller, the ISP is usually a “cable company” that, in addition, or offering a TV subscription, also offers an Internet subscription. You don’t get both for the price of one, however. You can get just cable TV or just high-speed Internet, or both.

An ISP is your gateway to the Internet and everything else you can do online. The second your connection is activated and set up, you'll be able to send emails, go shopping, do research, and more. The ISP is the link or conduit between your computer and all the other "servers" on the Internet. You may feel like you're talking to your mom directly through email, but in reality, it's more "indirectly." Your email goes from your computer to the ISP computers/servers, where it's sent along to its destination through other servers on the network.

Of course, that's its "electronic" path: the transmission is still virtually instantaneous.

Every home or organization with Internet access has an ISP. The good news is, we don't all have to have the same provider to communicate with each other and we don't have to pay anything extra to communicate with someone who has a different ISP.

Whereas just about anyone can have a website, not everyone can be an ISP. It takes money, infrastructure, and a lot of very smart technicians. Your ISP maintains miles of cabling, employs hundreds of technicians, and maintains network services for its hundreds of thousands of subscribers. Depending on where you live, you typically have a choice of ISPs.

## Types of ISPs

In the 1990s, there were three types of ISPs: dial-up services, high-speed Internet (also referred to as "broadband") offered by cable companies, and DSL (Digital Line Subscribers) offered by phone companies. By 2013, dial-up services were rare (even though they were cheap), because they were very slow...and the other ISP options were typically readily available and much, much faster.

## DSL and Cable.

Two of the leading DSL ISPs have been Verizon and AT&T. But in the last few years (from 2013), DSL has been on the decline, while cable-based ISPs, like Comcast and Time Warner, have been growing. Why the change? It's because the phone companies have been getting more into the lucrative smartphone business, and selling annual contracts for cellular service along with...smartphone Internet capabilities.

That's left a lot of the broadband business for the cable companies.

# Fiber Internet: On its way to you?

With DSL dropping out of the picture, there's room for new technology and it's already here in some areas: it's called fiber, or fiber optical, broadband. Supposedly, fiber is hundreds of times FASTER than cable or DSL. That's especially exciting news (if it's true and available) to companies, and gamers and households with a lot of simultaneous wireless usage going on.

Verizon (yes, they are downplaying DSL) now offers FiOS in select areas (put an "f" before "eye" and the "os"-sound in "most"). FiOS stands for fiber optic services, and it claims to have superfast Internet connection speeds.

And for all of us not in the Kansas area, Google launched Google Fiber in 2013, which offers incredibly ultra-fast Internet speed. Other companies (and communities) are teaming up to bring the next generation of broadband to you.

## Top 10 ISP provider in India on the basis of subscribers base.

Rank	ISP	Narrowband	Broadband	Total
1	Jio	0	138,615,904	138,615,904
2	Airtel	32,008,751	62,294,731	94,303,482
3	Vodafone	21,736,495	45,975,013	67,711,508
4	Idea Cellular	8,589,570	29,614,167	38,203,737
5	BSNL	10,915,589	21,242,487	32,158,076
6	Reliance Communications	10,697,647	5,523,074	16,220,721
7	Aircel	7,142,722	9,073,153	16,215,875
8	Tata Teleservices	4,690,205	4,316,099	9,006,304
9	Telenor India	7,969,328	331,339	8,300,667
10	MTNL	484,517	1,408,903	1,893,420

## 14. Discuss the difference between MAC address, IP address and Port address.

Ans

## Difference Between MAC Address and IP Address



MAC and IP are the addresses that uniquely defines a device and a connection in a network. A MAC address is a number assigned to the NIC card by the manufacturer. IP address is a number assigned to the connection in a network. The basic difference between MAC address and IP address is that a **MAC** address uniquely identifies a device that wants to take part in a network.

On the other hand, an **IP** address uniquely defines a connection of a network with an interface of a device. Let us study some other differences between MAC address and IP address with the help of comparison chart shown below.

Content: MAC address Vs IP address

1. Comparison Chart
2. Definition
3. Key Differences
4. Conclusion

Comparison Chart

BASIS FOR COMPARISON	MAC	IP
Full Form	Media Access Control Address.	Internet Protocol Address.
Purpose	It identifies the physical address of a computer on the internet.	It identifies connection of a computer on the internet.
Bits	It is 48 bits (6 bytes) hexadecimal	IPv4 is a 32-bit (4 bytes) address, and IPv6

BASIS FOR COMPARISON	MAC	IP
	address.	is a 128-bits (16 bytes) address.
Address	MAC address is assigned by the manufacturer of NIC card.	IP address is assigned by the network administrator or Internet Service Provider.
Retrieve Address	ARP protocol can retrieve MAC address of a device.	RARP protocol can retrieve IP address of a device.

#### Definition of Mac Address

Address that uniquely defines a hardware interface is called **MAC (Media Access Control)** Address. MAC address is purchased by the manufacturer, producing interface hardware and assign the MAC addresses sequentially to the interface hardware as they are produced. MAC address is burned into the ROM of **Network Interface Card (NIC)**. NIC is an interface hardware that is used by the computer to become a part of a network.

MAC address is a **48-bit hexadecimal** address. The format of a MAC address is MM:MM:MM:SS:SS:SS, where MM:MM:MM is a 3-byte address of the manufacturer. On the other hand, SS:SS:SS is a serial number of NIC card. MAC Address of each computer on a network is unique. When you change or replace the NIC card of your computer, your MAC address also gets changed.

MAC address is used at the data link layer of OSI/TCP/IP model. **ARP** (Address Resolution Protocol) is a protocol used to receive MAC address of a device.

#### Definition of IP Address

The address provided to a connection in a network is called **IP (Internet Protocol)** address. IP address does not uniquely identify a device on a



network but, it specifies a particular connection in a network. IP address is provided by the administrator of the network or by Internet Service Provider (ISP).

IP address identifies both a network and the host on that network. IP address is used while routing as it specifically identifies a network connection. If your computer is on two networks so, it will have two IP addresses.

**IPv4** address is **32-bit** address whereas **IPv6** is **128-bit** address. Your IP address will get changed each time you connect to the network as it is dynamically allocated to your device when it participates in the network. IP address for a particular connection in a network can be retrieved by **RARP** (Reverse Address Resolution Protocol).

#### Key Differences Between MAC Address and IP Address

1. The full form of MAC address is Media Access Control whereas, the full form of IP address is Internet Protocol address.
2. The IP address identifies a connection to a device in a network. On the other hand, Mac address identifies a device participating in a network.
3. MAC address is 48 bits (6 bytes) hexadecimal address whereas, IP address has two versions, IPv4 a 32-bit address and IPv6 a 128-bit address.
4. MAC address is assigned by the manufacturer of interface hardware. On the other hand, IP address is assigned by the network administrator or Internet Service Provider (ISP).
5. ARP protocol retrieves the MAC address whereas RARP protocol retrieves IP address.

## 15. How do we view my Internet browser's history?

Ans

### How do I view my Internet browser's history?

Today, all major browsers have functionality that allows you to quickly and easily view your



Internet browser's history. However, as multiple devices contain browser history, there are multiple ways to view as well. To proceed, choose your devices from the section below and follow the instructions.

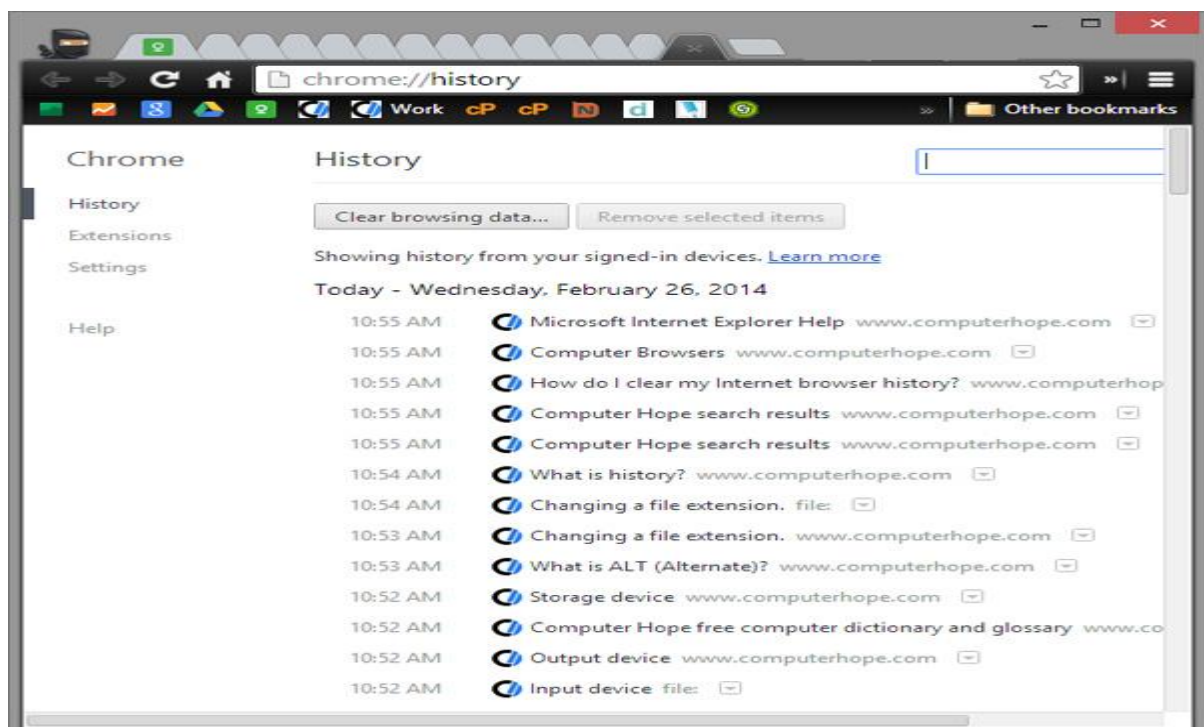
## Desktop or laptop computer

If you are using Windows, Linux, or macOS, there are quick shortcut key combinations that allow you to view your history.

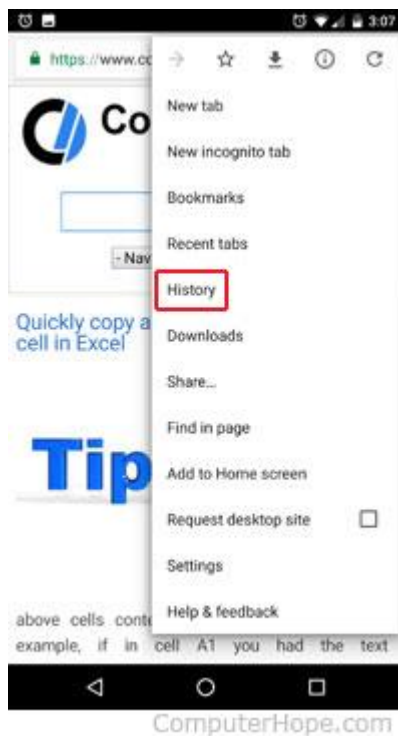
**Windows and Linux users:** [Ctrl](#)+H

**Apple users:** [Command](#) + [Shift](#) + H


Once one of the above shortcut keys is pressed, a history section similar to the example below should appear. In the following screenshot, browsing history is being viewed in Google Chrome.



## Android phone or tablet running Google Chrome



Users who are running Google Chrome on their Android phone or tablet can view their history with the following steps.

1. Open the [Google Chrome](#) Internet browser.
2. In the upper-right corner of the screen **tap** the  **icon**.
3. In the [drop-down menu](#) that appears, select **history** and shown in the image.
4. The following page contains your device's history.

## iPhone or iPad running Safari

Users who are running Safari for iOS on their iPhone or iPad can view their history with the following steps.

1. On your device, open the [Safari](#) Internet browser.

2. In the lower-left corner of the browser window, press and hold the back arrow.
3. The next screen contains your browser's history.

