CCA-102: Data Communications

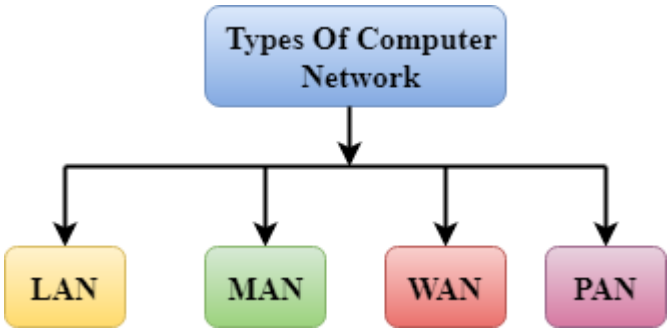
ASSIGNMENT

Q1.What are the different types of networks?

Computer Network Types

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

A computer network can be categorized by their size. A **computer network** is mainly of **four types**:



- LAN(Local Area Network)
- PAN(Personal Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

LAN(Local Area Network)

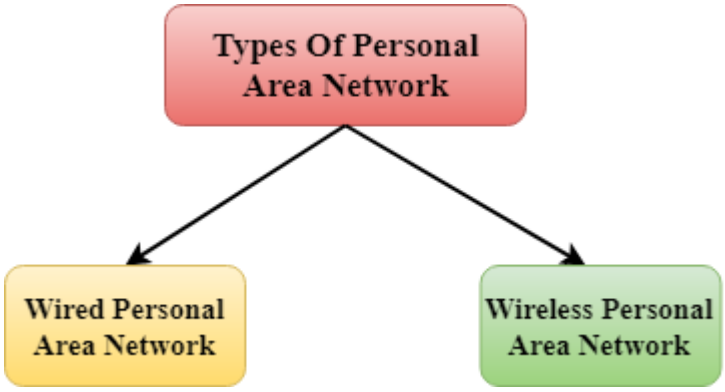
- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

PAN(Personal Area Network)

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.

- **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of **30 feet**.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

There are two types of Personal Area Network:



- Wired Personal Area Network
- Wireless Personal Area Network

Wireless Personal Area Network: Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.

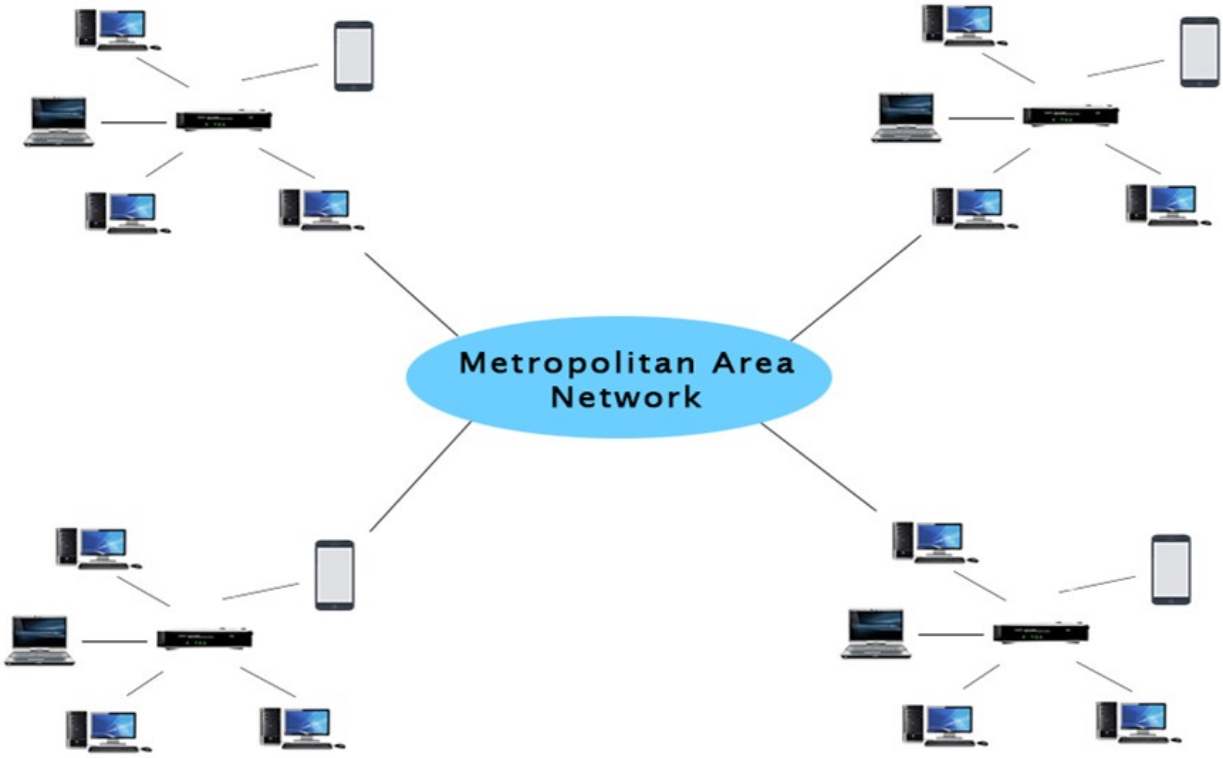
Wired Personal Area Network: Wired Personal Area Network is created by using the USB.

Examples Of Personal Area Network:

- **Body Area Network:** Body Area Network is a network that moves with a person. **For example**, a mobile network moves with a person. Suppose a person establishes a network connection and then creates a connection with another device to share the information.
- **Offline Network:** An offline network can be created inside the home, so it is also known as a **home network**. A home network is designed to integrate the devices such as printers, computer, television but they are not connected to the internet.
- **Small Home Office:** It is used to connect a variety of devices to the internet and to a corporate network using a VPN

MAN(Metropolitan Area Network)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- It has a higher range than Local Area Network(LAN).



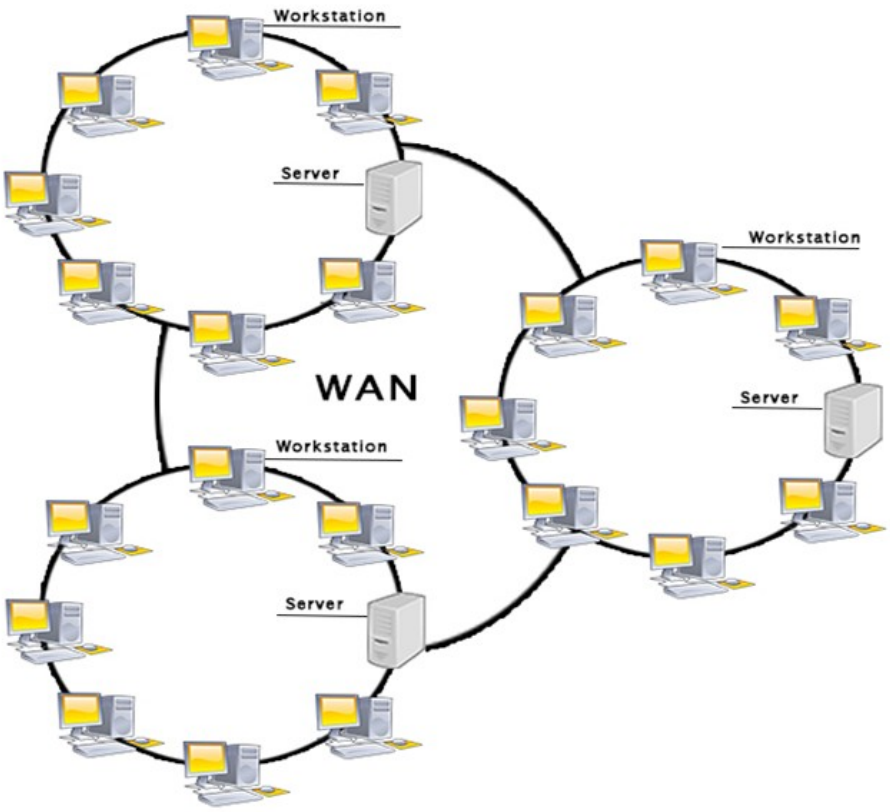
Uses Of Metropolitan Area Network:

- MAN is used in communication between the banks in a city.
- It can be used in an Airline Reservation.
- It can be used in a college within a city.
- It can also be used for communication in the military.

WAN(Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.

- A Wide Area Network is widely used in the field of Business, government, and education.



Examples Of Wide Area Network:

- **Mobile Broadband:** A 4G network is widely used across a region or country.
- **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
- **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

Advantages Of Wide Area Network:

Following are the advantages of the Wide Area Network:

- **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with

them through WAN. The internet provides a leased line through which we can connect with another branch.

- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.
- **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- **Global business:** We can do the business over the internet globally.
- **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

Disadvantages of Wide Area Network:

The following are the disadvantages of the Wide Area Network:

- **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
- **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

Internetwork

- An internetwork is defined as two or more computer network LANs or WAN or computer network segments are connected using devices, and they are configured by a local addressing scheme. This process is known as **internetworking**.
- An interconnection between public, private, commercial, industrial, or government computer networks can also be defined as **internetworking**.
- An internetworking uses the **internet protocol**.
- The reference model used for internetworking is **Open System Interconnection(OSI)**.

Types Of Internetwork:

1. **Extranet:** An extranet is a communication network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. It is used for information sharing. The access to the extranet is restricted to only those users who have login credentials. An extranet is the lowest level of internetworking. It can be categorized as **MAN**, **WAN** or other computer networks. An extranet cannot have a single **LAN**, atleast it must have one connection to the external network.

2. **Intranet:** An intranet is a private network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. An intranet belongs to an organization which is only accessible by the **organization's employee** or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

Intranet advantages:

- **Communication:** It provides a cheap and easy communication. An employee of the organization can communicate with another employee through email, chat.
- **Time-saving:** Information on the intranet is shared in real time, so it is time-saving.

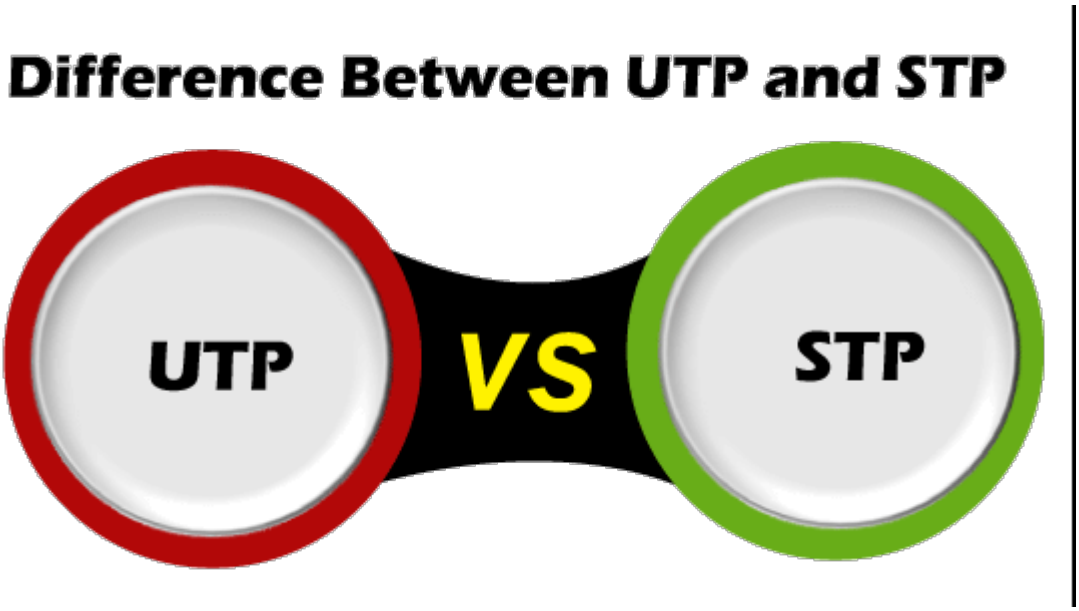
- **Collaboration:** Collaboration is one of the most important advantage of the intranet. The information is distributed among the employees of the organization and can only be accessed by the authorized user.
- **Platform independency:** It is a neutral architecture as the computer can be connected to another device with different architecture.
- **Cost effective:** People can see the data and documents by using the browser and distributes the duplicate copies over the intranet. This leads to a reduction in the cost.

Q2.Explain the Shielded twisted pair (STP) and Unshielded twisted pair (UTP)

Shielded twisted pair cable (STP) has the individual pairs of wires wrapped in foil, which are then wrapped again for double protection. Unshielded twisted pair cable (UTP) has each pair of wires twisted together. Those wires are then wrapped in tubing without any other protection.

Difference between UTP and STP

Before going through the difference between UTP and STP cable, we need to learn the term **twisted pair cable**. A twisted pair cable is a widely used cable for transmitting data and information over certain distances. A twisted pair cable consists of two separate insulated copper wires that are twisted together within a wrapping shield and run parallel with each other. Furthermore, it helps to reduce the crosstalk or electromagnetic induction between the pair of wires. A twisted pair cable is divided into two parts as **STP** and **UTP**.



UTP (Unshielded Twisted Pair)

UTP is an unshielded twisted pair cable used in computer and telecommunications mediums. Its frequency range is suitable for transmitting both data and voice via a UTP cable. Therefore, it is widely used in the telephone, computers, etc. It is a pair of insulated copper wires twisted together to reduce noise generated by external interference. It is a wire with no additional shielding, like aluminium foil, to protect its data from the exterior.

Advantages of the UTP:

1. It is a less costly and less expensive unshielded wire from another network medium.
2. It is designed to reduce crosstalk, RFI, and EMI.
3. Its size is small, and hence the installation of the UTP is easier.
4. It is mostly useful for short-distance network connections like home and small organizations.
5. It is the most commonly used networking cable in the market. It is considered as faster copper-based data transmission cable.
6. It is suitable for transmitting both data and voice via UTP cable.

Disadvantage of the UTP:

1. It can only be used in length segment up to 100 meters.
2. It has limited bandwidth for transmitting the data.
3. It does not provide a secure connection for data transmitting over the network.

STP (Shielded twisted pair):

A shielded twisted pair is a type of twisted pair cable that contains an extra wrapping foil or copper braid jacket to protect the cable from defects like cuts, losing bandwidth, noise, and signal to the interference. It is a cable that is usually used underground, and therefore it is costly than UTP. It supports the higher data transmission rates across the long distance. We can also say it is a cable with metal sheath or coating that surround each pair of the insulated conductor to protect the wire from external users and prevent electromagnetic noise from penetrating.

Features of Shielded twisted pair cable:

1. **Frequency:** It has higher frequency data transmission as compared to the UTP.
2. **Thickness:** It is a thick shielded twisted pair cable as it contains the wrapping of plastic material to the copper conductor.
3. **Grounding practices:** The uses of shielded twisted pair cable are underground for a longer distance.
4. **Installation** of the shielded wire is more difficult than the UTP (Unshielded twisted pair) cable.

Advantages of the STP cable

1. It has lower noise and attenuation than UTP.
2. It is shielded with a plastic cover that protects the STP cable from a harsh environment and increases the data transmission rate.
3. It reduces the chances of crosstalk and protects from external interference.
4. A modular connection helps to terminate the connection of the STP cable.

Disadvantages of the STP cable

1. It is the most expensive wire from UTP cables.
2. It requires more maintenance to reduce the loss of data signals.

3. There is no segment improvement in length despite its thick and heavier connection.
4. It is used only as a grounded wire.

Difference between UTP and STP

Following are the differences of the UTP and STP, as follows:

UTP	STP
It is an unshielded twisted pair.	It is a shielded twisted pair.
UTP cable is a twisted pair cable with wires that are twisted together.	It is enclosed within a foil or mesh shield.
The price of UTP is lower as compared to the STP.	The price of STP is much costlier than UTP.
It does not require a grounding cable.	It requires a grounding cable.
In UTP, the electromagnetic interference is more than the STP while transferring the signal to the transmission media.	It reduces electromagnetic interference while transferring the signal to the transmission media.
UTP has high crosstalk.	STP has low crosstalk.
Transferring speed of the data signal is slow as compared to the STP.	Transferring speed of the data signal is high as compared to the UTP.
Installation of UTP cables is easy as they are lighter, small in size, and flexible.	Installation of STP cable is quite difficult as compared to the UTP. Its size is heavy, bigger, and stiffer.
It does not require much maintenance.	It requires more maintenance.
UTP cables are noisier.	STP cables are less noisy.
However, the UTP cable is used to establish the	Generally, it is used to establish the connection

connection within a short distance, like a home or small industry.	for enterprises over a long distance.

Q3.What is difference between baseband and broadband transmission?

Difference between Baseband and Broadband Transmission

Baseband and ***broadband*** are the two main types of ***signalling techniques***. These terminologies were created to categorize various types of signals based on signal formats or modulation techniques. The broadband transmission sends many signals at once and utilizes analogue signals, whereas baseband transmission sends just one signal at a time and uses digital signals.

In this article, you will learn about the difference between ***Baseband*** and ***Broadband transmission***. But before discussing the differences, you must know about Baseband and Broadband transmission with their advantages and disadvantages.

Baseband Transmission

It is a method of transmission where a single signal is either transmitted or received in the type of discrete pulses of a single frequency across a communication medium like a cable. The baseband signal's frequency is not changed, and the signal's bandwidth is almost 0. Baseband systems do not use frequency shifting, so only one signal uses the entire bandwidth of the system at once. Therefore, any remaining bandwidth is wasted.

In this technology, several devices in a network interact with one another by sending and receiving data on a single communication channel that is shared by all connected devices and utilizing the channel's full bandwidth. The data is either transmitted or received at any time. All the devices in the network must be able to understand the same type of signal. However, ***Time Division Multiplexing (TDM)*** enables sharing of the same media.

The baseband signal is frequently utilized in wired ***Local Area Networks (LANs)*** that are based on Ethernet.

Advantages and Disadvantages of Baseband Transmission

There are various advantages and disadvantages of baseband transmission. Some advantages and disadvantages of baseband transmission are as follows:

Advantages

1. It has a simple structure.
2. It is easy to install.
3. Its maintenance is simple and easy.
4. It has low-cost installation.

Disadvantages

1. It may be only utilized for voice and data.
2. It has a short coverage and a limited range.
3. It works only on a limited distance.

Broadband Transmission

Broadband Transmission sends data in the form of analog signals, allowing signals to be sent at multiple frequencies simultaneously. This broadband transmission is unidirectional. In other words, the data is only transmitted in one direction at the same time. As a result, it may send or receive data but not perform both operations at the same time.

Broadband transmission utilizes ***Frequency Division Multiplexing (FDM)***. The bandwidth in FDM is split into a number of frequency bands, each of which transmits a different signal. A multiplexer separates the numerous signals at the receiving end. It is typically more expensive to maintain and install due to the extra hardware involved. However, they cover more distance than baseband transmission. Broadband transmission is typically utilized via cable TV, several types of ***Digital Subscriber Lines (DSL), Asynchronous Transfer Mode (ATM)***, and ***Power Line communication***.

Advantages and Disadvantages of Broadband Transmission

There are various advantages and disadvantages of broadband transmission. Some advantages and disadvantages of broadband transmission are as follows:

Advantages

1. The main advantage of broadband transmission is its speed. It offers a fast speed for data transmission.
2. It has a large bandwidth provision for data transmission.
3. The data transmission may take place for a large distance.

Disadvantages

1. It needs some extra hardware for data transmissions like Multiplexers and De-multiplexers.
2. The broadband transmission maintenance and cost are high.

Key differences between Baseband and Broadband Transmission

Here, you will learn about the key differences between ***Baseband*** and ***Broadband Transmission***. Some of the main differences between Baseband and Broadband Transmission are as follows:

1. Baseband transmission is a data transmission technique in which one signal needs the whole bandwidth of the channel to transfer the data. In contrast, broadband transmission is a transmission technology in which many signals with different frequencies send data across a single channel at the same time.
2. Manchester and differential Manchester encoding are used in baseband. In contrast, broadband transmission does not utilize any digital encoding, but it utilizes the PSK (Phase shift keying) encoding.

Features	Baseband Transmission	Broadband Transmission
Definition	It is a data transmission technique in which one signal needs the whole bandwidth of the channel to transfer the data.	It is a transmission technology in w many signals with different frequencies data across a single channel at the time.
Signal Type	It utilizes digital signals.	It utilizes analog signals.
Signal transmission	The signals may be transmitted in both directions.	The signal may transmit only one direc
Direction Type	It is bidirectional in nature.	It is unidirectional in nature.
Multiplexing	It uses Time Division Multiplexing (TDM).	It uses Frequency Division Multiple (FDM).
Topology	It operates with bus topology.	It operates with both bus and tree topol
Number of Channels	It utilizes the same channel for sending and receiving data.	It utilizes two channels, one transmission and the second for reception.
Distance Covered	Signals are only capable of travelling	Signals may be transmitted across

	limited distances. Attenuation is needed for long distances.	distances without attenuation.
Installation and Maintenance	It is simple and easy to install and maintain.	It is complex to install and maintain.
Cost	It is less expensive to design.	It is costly to design.
Encoding Technique	Manchester and differential Manchester encoding are used in baseband.	It doesn't utilize any digital encoding, l utilizes the PSK (Phase shift ke encoding.
Impedance	It contains a 50-ohm impedance.	It contains a 70-ohm impedance.
Transfer medium	It utilizes coaxial cables, wires, and twisted-pair cables as the transfer medium for digital signals.	It sends digital signals via coaxial c optical fibre cables, and radio waves.
Application	It is usually found in Ethernet.	It is usually found in telephone netv and cables.

3. Baseband transmission signals travel over shorter distances because attenuation is most noticeable at higher frequencies, which causes a signal to travel short distances without losing power. In contrast, the signals in broadband transmissions may travel across larger distances.
4. The baseband transmission utilizes digital signalling for signal transmission. In contrast, broadband transmission utilizes analog signalling for transmitting analog signals.
5. Another distinction between broadband and baseband transmission is the direction of signal transmission. Baseband transmission allows signals to be sent in both directions simultaneously. In contrast, broadband transmission allows signals to be sent in only one way.
6. Baseband transmission utilizes the bus topology. In contrast, broadband transmission utilizes both bus and tree topologies.

7. Baseband transmission utilizes time division multiplexing. In contrast, broadband transmission utilizes frequency division multiplexing.
8. Baseband transmission is simple and easy to install and maintain. In contrast, broadband transmission is complex to install and maintain.
9. Baseband transmission is less expensive to design. In contrast, broadband transmission is costly to design.
10. Baseband transmission contains a 50-ohm impedance. In contrast, broadband transmission contains a 70-ohm impedance.

Head-to-head comparison between Baseband and Broadband Transmission

Here, you will learn the head-to-head comparisons between Baseband and Broadband Transmission. The main differences between Baseband and Broadband Transmission are as follows:

Conclusion

The two main categories of signalling are baseband and broadband transmissions. Baseband transmission utilizes the digital signal or electrical impulse that may be transported in a physical medium like wires. On the other hand, broadband transmission utilizes analogue signalling, which uses optical or electromagnetic wave signals. The baseband transmission utilizes the complete channel's bandwidth to broadcast a signal. In contrast, broadband transmission divides the channel's bandwidth into varying frequency ranges to transmit many signals simultaneously,

Q4.What is the difference between a hub, modem, router and a switch?

A modem is used to connect to the Internet. A router acts as a gateway to the computer network and is placed between a modem and a switch or hub. A switch connects devices such

as a desktop, laptop, and access point to the router. An access point connects a device wirelessly.

The Differences Between a Modem, a Router, a Switch and a Hub

Device	What is does
Modem:	Stands for "modulating-demodulating": modems are hardware devices that allow a computer or another device, such as a router or switch, to connect to the Internet. They convert or "modulate" an analog signal from a telephone or cable wire to digital data (1s and 0s) that a computer can recognize. Simply send traffic from point A to piont B without further manipulation.
Routers:	Are responsible for sending data from one network to another. Work at Layer 3 (Network) of the OSI model, which deals with IP addresses. Typically, routers today will perform the functionality of both a router and a switch - that is, the router will have multiple ethernet ports that devices can plug into.
Switches:	They use the MAC address of a device to send data only to the port the destination device is plugged into. Work at Layer 2 (Data Link) of the OSI model, which deals with MAC addresses.
Hubs:	Unlike switches, hubs broadcast data to all ports, which is inefficient, so hubs are basically a multiport repeaters.

Note: it is also useful to know the following terms:

- Default gateway - a piece of software usually located on a router, a firewall, a server, etc, that enables traffic to flow in and out of the network. Gateways act as a junction between multiple networks.

- DHCP (Dynamic Host Configuration Protocol) - a protocol that automatically provides and assigns IP addresses, default gateways, DNS servers and other network parameters to client devices. Most routers/switches have the ability to provide DHCP server support.

In case you have several devices on your network that support DHCP, you need to make sure that only one of them is configured with DHCP. Having several devices with DHCP enabled will lead to a DHCP Race Condition - also known as Conflicting DHCP Servers.

Note: modern voice system will require your network to have a router in it. Despite the fact that some modems have integrated router features, they barely capable of maintaining voice systems functionality. You may want to have both modem and router in your network (modem will need to be launched in bridged mode).

Q5.When you move the NIC cards from one PC to another PC, does the MAC address gets transferred as well?

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 the NIC card was replace by another one.

Q6. When troubleshooting computer network problems, what common hardware-related problems can occur?

Most common hardware related problems are Pa BX, LAN Card, WLAN Card and Wi-Fi AP if it is wireless, Cables, Switches, Routers and Wireless Controllers. Most problems are hardware related, a faulty power cable or power supply unit. Sometimes RAM needs to be upgraded or VGA cable is not properly connected.

Q7.In a network that contains tow servers and twenty work stations, where is the best place to install an Anti-virus program?

The best solution is to install anti-virus on all the computers in the network.

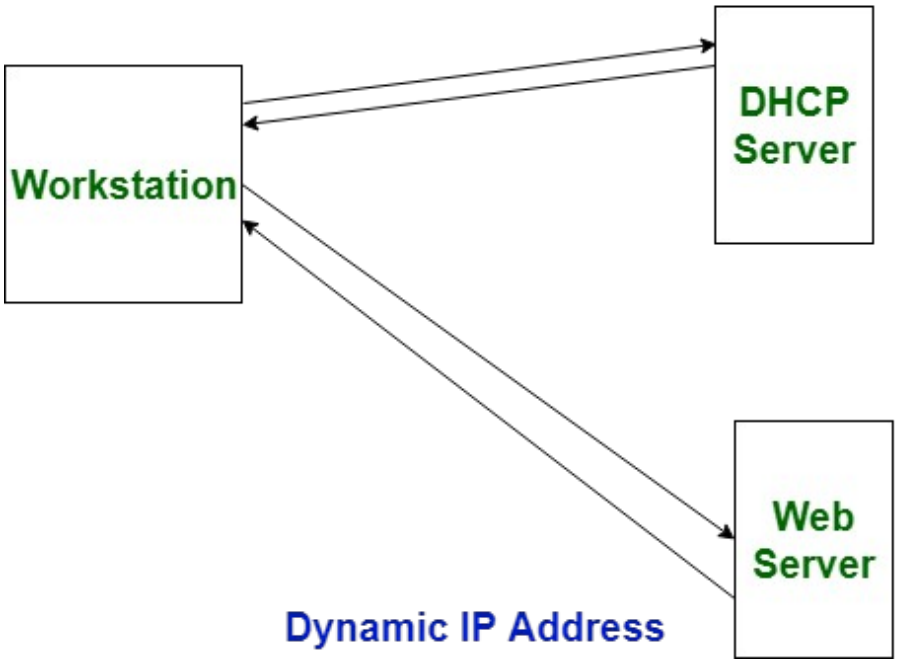
An anti-virus program must be installed on all servers and workstations to ensure protection. That's because individual users can access any workstation and introduce a computer virus when plugging in their removable hard drives or flash drives.

Q8. Define Static IP and Dynamic IP? Discuss the difference between IPV4 and IPV6.

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 often changes

whenever user boots his/her machine, and it's mechanically allotted.

Static IP Address



Dynamic IP Address

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	While dynamic ip address change

S.NO	Static IP Address	Dynamic IP address
	time, it means if a static ip address is provided then it can't be changed or modified.	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

S.NO	Static IP Address	Dynamic IP address
		security.

The address through which any computer communicates with our computer is simply called an Internet Protocol Address or IP address. For Example, If we want to load a web page or we want to download something, we require the address for delivery of that particular file or webpage. That address is called an IP Address.

Types of IP Address

1. IPv4 (Internet Protocol Version 4)
2. IPv6 (Internet Protocol Version 6)

IPv4

IPv4 address consists of two things that are the network address and the host address. It stands for **Internet Protocol version four.** It was introduced in 1981 by DARPA and was the first deployed version in 1982 for production on SATNET and on the ARPANET in January 1983.

IPv4 addresses are 32-bit integers that have to be expressed in Decimal Notation. It is represented by 4 numbers separated by dots in the range of 0-255, which have to be converted to 0 and 1, to be understood by Computers. For Example, An IPv4 Address can be written as **189.123.123.90.**

IPv4 Address Format

IPv4 Address Format is a 32-bit Address that comprises binary digits separated by a dot (.).

IPv4 Address Format

IPv6

IPv6 is based on IPv4 and stands for Internet Protocol version 6. It was first introduced in December 1995 by Internet Engineering Task Force. IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency. IPv6 is written as a group of 8 hexadecimal numbers separated by colon (:). It can be written as 128 bits of 0s and 1s.

IPv6 Address Format

IPv6 Address Format is a 128-bit IP Address, which is written in a group of 8 hexadecimal numbers separated by colon (:).

IPv6 Address Format

Benefits of IPv6

The recent Version of IP IPv6 has a greater advantage over IPv4. Here are some of the mentioned benefits:

- **Larger Address Space:** IPv6 has a greater address space than IPv4, which is required for expanding the IP Connected Devices. IPv6 has 128 bit IP Address rather and IPv4 has a 32-bit Address.
- **Improved Security:** IPv6 has some improved security which is built in with it. IPv6 offers security like Data Authentication, Data Encryption, etc. Here, an Internet Connection is more Secure.
- **Simplified Header Format:** As compared to IPv4, IPv6 has a simpler and more effective header Structure, which is more cost-effective and also increases the speed of Internet Connection.
- **Prioritize:** IPv6 contains stronger and more reliable support for QoS features, which helps in increasing traffic over websites and increases audio and video quality on pages.
- **Improved Support for Mobile Devices:** IPv6 has increased and better support for Mobile Devices. It helps in making quick connections over other Mobile Devices and in a safer way than IPv4.

For more, you can refer to, the Advantages of IPv6.

Difference Between IPv4 and IPv6

IPv4	IPv6
IPv4 has a 32-bit address length	IPv6 has a 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end, connection integrity is Unachievable	In IPv6 end-to-end, connection integrity is Achievable
It can generate 4.29×10^{9} address space	The address space of IPv6 is quite large it can produce 3.4×10^{38} address space
The Security feature is dependent on the application	IPSEC is an inbuilt security feature in the IPv6 protocol
Address representation of IPv4 is in decimal	Address Representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation is performed only by the sender

IPv4	IPv6
In IPv4 Packet flow identification is not available	In IPv6 packet flow identification are Available and uses the flow label field in the header
In IPv4 checksum field is available	In IPv6 checksum field is not available
It has a broadcast Message Transmission Scheme	In IPv6 multicast and anycast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
IPv4 has a header of 20-60 bytes.	IPv6 has a header of 40 bytes fixed
IPv4 can be converted to IPv6	Not all IPv6 can be converted to IPv4
IPv4 consists of 4 fields which are separated by addresses dot (.)	IPv6 consists of 8 fields, which are separated by a colon (:)
IPv4's IP addresses are divided into five different	IPv6 does not have any classes of the IP address.

IPv4	IPv6
classes. Class A , Class B, Class C, Class Da , Class E.	
IPv4 supports VLSM(Variable Length subnet mask).	IPv6 does not support VLSM.
Example of IPv4: 66.94.29.13	Example of IPv6: 2001:0000:3238:DFE1:0063:0000:0000:FEFB

Q9. Discuss TCP/IP model in detail.

The TCP/IP model is a four-layer model that divides network communications into four distinct categories or layers. The model is often referred to as the TCP/IP stack. The four important layers are the application layer, the transport layer, the network layer, and the link layer.

The TCP/IP model refers to the Transmission Control Protocol/Internet Protocol Model. This model is a part of the network domain designed specifically for overseeing efficient and error-free transmission of data.

The model works on a four-layered architecture model, where each layer implicit the required network protocols on the data to be transmitted, which remodels the data to the most optimum structure for efficient transmission over the network.

In this tutorial on what is TCP/IP model is, you will understand the working of each layer in detail to better understand the functioning of the model.

The History of TCP/IP

The Internet Protocol Suite, or TCP/IP for short, is the set of protocols that make up the network layer of the Internet.

- TCP/IP was developed during the Cold War as a way for the U.S. Department of Defense to connect computers within their networks and with each other across national boundaries. It's been used since the late 1960s when it was formalized by DARPA and later adopted by government agencies and universities worldwide as a common networking standard.
- The first version of TCP/IP was ARPANET (1975), which stands for Advanced Research Projects Administration Network. The name changed to TCP/IP in 1983, when it became an open standard that could be used on any network.
- To give researchers access to each other's equipment, they needed to send messages quickly over long distances without having them re-transmitted by any intermediate nodes along the way. This necessity led to the development of the Transmission Control Protocol (TCP) and Internet Protocol (IP). These protocols were intended for machine-to-machine connections, such as between computers over local area networks or wide-area networks.

Features of the TCP/IP Model

Below mentioned are some of the features that make the TCP/IP model stand out in the network concepts:

- The TCP/IP model is among one of the most important network concepts that contributed to the working of ARPANET.
- The TCP/IP model comprises four layers: the network access layer, the internet layer, the transport layer, and the application layer (going from bottom to top).
- The network model is implemented during network and communication-related issues.
- Communication between different modes of network devices is possible through the application of various layers.
- The layers in the model provide maintenance of communication channels, flow control, and reliability check format, among other applications in the form of protocols.

Now go ahead and continue with the next topic in this tutorial on ‘what is the TCP/ IP model’, which includes the layers of the TCP/IP model.

Layers of the TCP/IP Model

In this section, you will understand the different layers of the model and their functionality in the network concept:

The TCP/IP model is divided into four different layers:

- Application layer
- Transport layer
- Internet layer
- Network Access layer

Each layer performs a specific task on the data that is being transmitted over the network channel, and data moves from one layer to another in a preset pattern as mentioned below:

The above model represents the flow of data when it is being transmitted from the sender side. In the case of data being received, the layers of the model work in reverse order.

Now, take a look at each of the layers in detail:

Application Layer

This is the topmost layer which indicates the applications and programs that utilize the TCP/IP model for communicating with the user through applications and various tasks performed by the layer, including data representation for the applications executed by the user and forwards it to the transport layer.

The application layer maintains a smooth connection between the application and user for data exchange and offers various features as remote handling of the system, e-mail services, etc.

Some of the protocols used in this layer are:

- HTTP: Hypertext transfer protocol is used for accessing the information available on the internet.
- SMTP: Simple mail transfer protocol, assigned the task of handling e-mail-related steps and issues.
- FTP: This is the standard protocol that oversees the transfer of files over the network channel.

Now, move on to the next layer,

Transport Layer

This layer is responsible for establishing the connection between the sender and the receiver device and also performs the task of dividing the data from the application layer into packets, which are then used to create sequences.

It also performs the task of maintaining the data, i.e., to be transmitted without error, and controls the data flow rate over the communication channel for smooth transmission of data.

The protocols used in this layer are:

- TCP: Transmission Control Protocol is responsible for the proper transmission of segments over the communication channel. It also establishes a network connection between the source and destination system.
- UDP: User Datagram Protocol is responsible for identifying errors, and other tasks during the transmission of information. UDP maintains various fields for data transmission such as:
- Source Port Address: This port is responsible for designing the application that makes up the message to be transmitted.
- Destination Port Address: This port receives the message sent from the sender side.
- Total Length: The total number of bytes of the user datagram.
- Checksum: Used for error detection of the message at the destination side.

Moving on to the next layer, you have:

Internet Layer

The Internet layer performs the task of controlling the transmission of the data over the network modes and enacts protocols related to the various steps related to the transmission of data over the channel, which is in the form of packets sent by the previous layer.

This layer performs many important functions in the TCP/IP model, some of which are:

1. It is responsible for specifying the path that the data packets will use for transmission.
2. This layer is responsible for providing IP addresses to the system for the identification matters over the network channel.

Some of the protocols applied in this layer are:

- IP: This protocol assigns your device with a unique address; the IP address is also responsible for routing the data over the communication channel.

- ARP: This protocol refers to the Address Resolution Protocol that is responsible for finding the physical address using the IP address.

The last layer in the network model is the network access layer.

Network Access Layer

This layer is the combination of data-link and physical layer, where it is responsible for maintaining the task of sending and receiving data in raw bits, i.e., in binary format over the physical communication modes in the network channel.

- It uses the physical address of the system for mapping the path of transmission over the network channel.
- Till this point in this tutorial on what is TCP/IP model, you understood the basic idea behind the model and details about its layers, now compare the model with another network model.

TCP/IP Work

The TCP/IP protocol suite is the set of communication protocols used to connect hosts on the Internet. TCP/IP allows computers on the same network to identify and communicate with each other. TCP/IP is a two-layer protocol, with the transport layer (TCP) responsible for reliable end-to-end communication and the Internet layer (IP) accountable for routing packets from the host to the host.

- At the transport layer, TCP provides a reliable byte-stream service to applications. TCP guarantees the delivery of data and that data will be delivered in the same order in which it was sent. TCP uses several mechanisms to provide this service, including sequence numbers, acknowledgments, and timeouts.
- At the Internet layer, IP is responsible for routing datagrams (packets) from host to host. IP does not guarantee the delivery of datagrams, but it tries to deliver them as best. If a datagram cannot be delivered, IP will return an error message to the source host.

The TCP/IP protocol suite is the most commonly used protocol suite on the Internet today, and it is also the protocol suite used by most LANs and WANs.

TCP/IP Important

TCP/IP is essential because it provides an architecture that allows for virtually instantaneous communication across all types of network media, such as copper,

fiber, or wireless. It does this using the Internet Protocol Suite, which encompasses both the TCP and UDP protocols.

In turn, the TCP Protocol governs how packets move from one place to another on a network, and the UDP Protocol governs how packets move within a single machine or between two devices on a local area network (LAN). Without TCP/IP, there would be no way for computers to communicate over the internet.

Functions of TCP/IP Layers

The TCP/IP model is a four-layer model that divides network communications into four distinct categories or layers. The model is often referred to as the TCP/IP stack. The four important layers are the application layer, the transport layer, the network layer, and the link layer.

- The Application Layer: The application layer is closest to the end user. And this is the layer that users interact with directly, including protocols such as HTTP, FTP, and SSH. This layer is responsible for providing applications with access to the network.
- The Transport Layer: The transport layer ensures that data is delivered reliably and efficiently from one point to another. This layer handles data transmission between hosts, including protocols like TCP and UDP.
- The Internet Layer: The network layer is responsible for routing data through the web. This layer delivers data packets from one host to another, including the IP protocol.
- The Link Layer: The link layer provides reliable data links between the two nodes — for example, protocols like ethernet and Wi-Fi.

Protocols Used

There are four main protocols used in TCP/IP: the Transmission Control Protocol (TCP), the User Datagram Protocol (UDP), the Internet Protocol (IP), and the Internet Control Message Protocol (ICMP).

- TCP ensures that data is delivered reliably and in order.
- UDP is used for applications where data doesn't need to be delivered reliably or needs to be delivered quickly without the overhead of TCP.
- IP is the protocol that routes data from one computer to another.
- ICMP is used for error-checking and for managing traffic congestion.

All four of these protocols are essential for the proper functioning of the internet. They work together to ensure that data is delivered quickly, reliably, and in the appropriate order.

There are some other protocols also notable, and there are,

- Address Resolution Protocol (ARP)
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Simple Mail Transfer Protocol (SMTP)
- Domain Name System (DNS)

TCP Characteristics

- TCP is a connection-oriented protocol that establishes a connection between two nodes before transmitting any data. All data sent over a TCP connection is checked for accuracy and retransmitted until the data is received correctly. This reliability makes TCP well-suited for applications that require a high degree of error-checking and for large data transfers. And also, TCP operates at the lowest level of the OSI model, transmitting data in segments, which are then reassembled into whole frames by the receiver.
- TCP also provides congestion control, which helps prevent network congestion by regulating the rate at which data is sent.
- Additionally, TCP can control the flow of data, allowing data to be sent at different rates depending on the application's needs.

Advantages and Disadvantages of the TCP/IP Model

With tons of benefits, there are also some potholes here with these models.

Advantages of TCP/IP:

- Scalability: The TCP/IP model is highly scalable and can accommodate small and large networks.
- Reliability: The model is robust and reliable, making it suitable for mission-critical applications.

- Flexibility: It is very flexible, allowing for interoperability between different types of networks.
- Security: The various protocols in the model provide robust security measures.
- Cost-effectiveness: TCP/IP is relatively inexpensive to implement and maintain.

Disadvantages of TCP/IP:

- Complexity: The model is quite complex and requires a certain degree of expertise to configure and maintain.
- Vulnerability: Because of its complexity, it is vulnerable to attack.
- Performance: Performance can be degraded due to network congestion and latency.

Uses of TCP/IP

Here are some of the most valuable uses of TCP/IP models:

- World Wide Web: TCP/IP transfers data between web browsers and servers.
- Email: Applications such as Outlook, Thunderbird, and Gmail use TCP/IP protocols to send and receive emails.
- File Transfer: FTP, SFTP, and other file transfer services rely on TCP/IP to move files from one computer to another.
- Networking: TCP/IP links computers together in a network.
- Virtual Private Networks: VPNs use TCP/IP to encrypt data before it travels across a public or private network.
- Internet of Things: Many smart home devices use TCP/IP to communicate and transfer data.
- Voice Over Internet Protocol: VOIP services such as Skype and Google Voice use TCP/IP to transmit calls over the internet.

Conclusion

In this ‘What is TCP/IP model’ tutorial, you understood the network communication details about data, which includes the basic idea behind the working of the model, the functioning of each layer in the model, and also how the data is restructured to achieve efficient transmission over the communication channel.

To better understand the working of each layer and the different steps they take during the data transmission over the network from a professional point of view, you can refer to Simplilearn's Cyber Security Expert course, which will allow you to gain in-depth knowledge about the network functions and working of the model at a whole new level.

Do you have any questions related to this tutorial on 'What is TCP/IP model?' If yes, feel free to mention them in the comments section at the bottom of this page. Our team will help you solve your queries ASAP.

Q10. What is a Web Browser (Browser)? Give some example of browsers.

Web Browser is a common term which is frequently used by people while discussing the Internet. However, the exact definition of a web browser is known by few only.

Web Browser Definition: A software application used to access information on the World Wide Web is called a Web Browser. When a user requests some information, the web browser fetches the data from a web server and then displays the webpage on the user's screen.

It is also important to know in detail about what a web browser is for candidates preparing for Government exams. This is because Computer Knowledge is a common topic for many competitive exams and questions based on web browsers may be asked.

In this article, we shall discuss in detail the different types of web browsers and their development over the years. Also, web browser functions have been given along with some sample questions from the competitive exam perspective.

To learn more about the other Computer Awareness related topics, candidates can check the links given below:

Basics of Cloud Computing	Types of Computer
Computer Virus	Computer Shortcut Keys
Computer Abbreviations	High Level Computer Language

History of Web Browser

Today web browsers are easily accessible and can be used on devices like computer, laptops, mobile phones, etc. but this evolution of making browsers available for easy use took many years.

Given below are some salient points which one must know with regard to the history of web browsers:

- **"WorldWideWeb"** was the first web browser created by Tim Berners Lee in 1990. This is completely different from the World Wide Web we use today
- In 1993, the **"Mosaic"** web browser was released. It had the feature of adding images and an innovative graphical interface. It was the "the world's first popular browser"
- After this, in 1994, Marc Andreessen (leader of Mosaic Team) started working on a new web browser, which was released and was named **"Netscape Navigator"**
- In 1995, **"Internet Explorer"** was launched by Microsoft. It soon overtook as the most popular web browser
- In 2002, **"Mozilla Firefox"** was introduced which was equally as competent as Internet Explorer
- Apple too launched a web browser in the year 2003 and named it **"Safari"**. This browser is commonly used in Apple devices only and not popular with other devices
- Finally, in the year 2008, Google released "Chrome" and within a time span of 3 years it took over all the other existing browsers and is one of the most commonly used web browsers across the world

For those who are willing to know more about the Internet, can visit the linked article.

Other Related Links	
Basics of MS Excel	MS Word
MS PowerPoint	Hardware and Software Questions

Functions of Web Browser

Our dependency on the Internet has massively increased. Stated below are functions of web browsers and how are they useful:

- The main function is to retrieve information from the World Wide Web and making it available for users
- Visiting any website can be done using a web browser. When a URL is entered in a browser, the web server takes us to that website
- To run Java applets and flash content, plugins are available on the web browser
- It makes Internet surfing easy as once we reach a website we can easily check the hyperlinks and get more and more useful data online

- Browsers user internal cache which gets stored and the user can open the same webpage time and again without losing extra data
- Multiple webpages can be opened at the same time on a web browser
- Options like back, forward, reload, stop reload, home, etc. are available on these web browsers, which make using them easy and convenient

Given below are a few difference between articles for candidates to learn more about the different computer features:

Difference Between Internet and WWW	Difference Between Firewall and AntiVirus
Difference Between RAM and ROM	Difference Between Virus and Malware
Difference Between Hardware and Software	Difference Between IPv4 and IPv6

a Web Browser

A web browser is the software installed on your computer or mobile that allows you to view web pages.

The first web browser, World Wide Web, was developed by Tim Berners-Lee in 1990.

It was created to allow researchers at CERN (European Organization for Nuclear Research) to share information about particle physics over the internet.

Since then, many browsers have been developed and are available for you to use.

There are many different types of browsers. Some of them are free and some cost money.

You can find out which is best for you by comparing the features offered by each

browser.

If you're having trouble viewing a website with one web browser, try using another one!

the Examples of Web Browsers

There are 10 Examples of web Browsers, which are given below.

- Internet Explorer.
- Google Chrome.
- Mozilla Firefox.
- Safari.
- Opera.
- Konqueror.
- Lynx.
- Tor Browser.
- UC Browser.
- Brave Browser.

1. Internet Explorer

The Internet Explorer is a web browser that was developed by Microsoft.

It is the second most used web browser in the world, after Google Chrome.

The Internet Explorer is not just a web browser, but also an operating system that can be accessed on Windows-based computers.

The Internet Explorer has been around since the 1990s when it was first released in August of 1995.

This browser remains one of the most popular today, with more than half of all websites using it to access their site according to W3Schools.

The browser remains popular because it offers easy access to news sites and video streaming sites like YouTube and Netflix among many others.

2. Google Chrome

Chrome is an internet browser, but it's also so much more than that.

Chrome helps you get to what you want faster and more smoothly, so you can spend less time searching and more time doing.

It’s created by Google and helps you get to the web faster with features like speed browsing, voice search, and autofill.

Chrome used to be just a browser that people would use to access the internet. That was back in 2008.

Today, Chrome is much more than just a browser; it’s an entire suite of tools designed to make life easier on the web.

3. Mozilla Firefox

Mozilla Firefox is an open-source, free web browser developed by the Mozilla Foundation.

It was created in 2003 and is now one of the major players in the browser world.

Mozilla Firefox offers many advantages over other browsers. For starters, it's much more secure than other browsers because it does not allow third-party installations.

It also has a very clean interface that doesn't come with any bloatware or toolbars that you don't want to use.

Other features include web development tools, pop-up blocking, private browsing, and tabbed browsing.

4. Safari Browser

Safari is a web browser developed by Apple.

As of this writing, it is the only browser that comes installed on all of their devices.

Safari was originally named after the Safari browser that was bundled with Mac OS X v10.2 in 2001.

The Safari browser has been optimized for fast loading and smooth scrolling, both of which are important when using a mobile device.

The latest version of Safari, Safari 11, is available for download on your iPhone or iPad from the App Store.

5. Opera Browser

Opera is a web browser that was created in the late 1990s.

The Opera browser is now available for Windows, Mac, Linux, Android, iOS, and even your Kindle! It’s also one of the most popular browsers in Asia.

Opera has many built-in features that make it easier to browse the web. One of these features is Speed Dial which lets you save pages that you visit often so that they are just one click away.

Another feature is Stash Express which saves every webpage you visit on your Stash so it's never lost again.

And finally, there's Opera Turbo which compresses data before loading it onto your phone or computer.

There are many other features too like news feeds and download manager which make the browsing experience more enjoyable and safer than ever before.

6. Konqueror

Konqueror is an open source web browser for Unix-like operating systems.

It is one of the earliest full-featured browsers, with simple syntax highlighting and HTML previewing in the left window, plus multi-tabbed browsing.

Konqueror has a built-in Document Viewer that will allow you to view PDFs and

other document types.

It also has a built in file manager, so it can be used as a basic OS file browser. Konqueror is so much more than just another browser.

7. Lynx Browser

Lynx is a text-based web browser. It is designed for use with slow computer connections, old computers, or computers with small screens.

It is also good for people who prefer keyboard navigation over the use of a mouse.

Lynx was first released in 1992 by a programmer named Bob Alberti as a shareware package.

The first release had 14 lines of code and featured "a basic, text-only user interface." Over time, Lynx has grown significantly in size and features.

The latest release includes many features seen on modern browsers such as tabbed browsing and JavaScript support.

8. Tor Browser

Tor Browser is a free browser that helps you protect your privacy and security on the internet.

This is accomplished by routing your traffic through a network of volunteer nodes, meaning third parties can't watch your online activity.

Tor Browser is designed to prevent anyone from knowing what you do online, even someone watching at the same café as you.

It also gives you access to sites that are censored in many countries, such as Facebook and Twitter.

It can help you find resources to learn important skills like HTML coding or basic programming languages.

It has been used by journalists, law enforcement officers, activists, and human rights workers around the world to conduct their work with greater safety and protection against surveillance.

9. UC Browser

UC Browser is a light, smart browser that gives users the fastest mobile web browsing experience.

UC Browser uses the latest in web kit technology to offer features like ad-blocking, built-in Google Translate, and voice search for Android phones.

The app also has a smart download feature so you can easily download files on spot.

One of the most talked about features is UC News.

This section offers news in your native language with live feeds from around the world.

10. Brave Browser

Brave is a fast, simple, and secure browser that protects your privacy and blocks ads.

Brave is the first open-source browser with built-in adblocker, malware blocker, tracking protection, autoplay blocker, and private tabs.

Brave aims to provide a faster and safer browsing experience while still supporting publishers through its anonymous ads system.

The Brave browser was created by Brendan Eich, inventor of JavaScript and co-founder of Mozilla & Firefox.

More than 5 million users have downloaded the Brave browser so far to enjoy a faster browsing experience without intrusive advertising or trackers.

Q11. What is a search engine? Give example.

A Search Engine

A search engine is a software program, which is designed to perform web searches on the World Wide Web (www). You can call the search engines as an **answering machine**.

Search engines discover, process and organize internet content and provide it to users when searching for any information.

Here are a few important points:

- A search engine is a platform on which a user can search the internet content.
- **Google, Yahoo, Bing, Baidu**, and **DuckDuckGo** are popular search engines. Google is one of the most used search engines worldwide that is used with the Chrome browser. So, almost everyone is familiar with it.
- According to the research, around 92.16% of searches are happening on Google, 2.18 on Bing, 1.52 on Yahoo, 1.14 on Baidu, and so on.

Examples of search engines

Most of the time, people are confused between search engines and web browsers. For example, they mislead between Google and Chrome. They think Google and Chrome both are search engines or web browsers. But it is not correct. Google is a search engine, while Chrome is a web browser.

For the brief, Google, Yahoo, and Bing are popular search engines. This chapter will describe to you what is a search engine and its example as well.

Q12. What is the Internet & WWW? What bare the uses of internet in our daily life?

Introduction

The **Internet** is an increasingly important part of everyday life for people around the world. But if you've never used the Internet before, all of this new information might feel a bit confusing at first.

Throughout this tutorial, we'll try to answer some basic questions you may have about the Internet and how it's used. When you're done, you'll have

a good understanding of **how the Internet works**, how to **connect to the Internet**, and **how to browse the Web**.

the Internet

The Internet is a **global network** of billions of computers and other electronic devices. With the Internet, it's possible to access almost any information, communicate with anyone else in the world, and do much more.

You can do all of this by connecting a computer to the Internet, which is also called **going online.** When someone says a computer is online, it's just another way of saying it's connected to the Internet.

The **Internet** (or **internet**) is the global system of interconnected computer networks that uses the Internet protocol suite (TCP/IP) to communicate between networks and devices. It is a *network of networks* that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical

networking technologies. The Internet carries a vast range of information resources and services, such as the interlinked hypertext documents and applications of the World Wide Web (WWW), electronic mail, telephony, and file sharing.

The origins of the Internet date back to the development of packet switching and research commissioned by the United States Department of Defense in the late 1960s to enable time-sharing between computers

The primary precursor network, the ARPANET, initially served as a backbone for the interconnection of regional academic and military networks in the 1970s to enable resource sharing. The funding of the National Science Foundation Network as a new backbone in the 1980s, as well as private funding for other commercial extensions, led to worldwide participation in the development of new networking technologies and the merger of many networks.

the linking of commercial networks and enterprises by the early 1990s, as well as the advent of the World Wide Web

marked the beginning of the transition to the modern Internet, and generated a sustained exponential growth as generations of institutional, personal, and mobile computers were connected to the network. Although the Internet was widely used by academia in the 1980s, commercialization incorporated its services and technologies into virtually every aspect of modern life.

Most traditional communication media, including telephone, radio, television, paper mail, and newspapers, are reshaped, redefined, or even bypassed by the Internet, giving birth to new services such as email, Internet telephone, Internet television, online music, digital newspapers, and video streaming websites. Newspaper, book, and other print publishing have adapted to website technology or have been reshaped into blogging, web feeds, and online news aggregators. The Internet has enabled and accelerated new forms of personal interaction through instant messaging, Internet forums, and social networking services. Online shopping has grown exponentially for major retailers, small businesses, and entrepreneurs, as it enables firms to extend their "brick and mortar" presence to serve a larger market or even sell goods and services entirely online. Business-to-business and financial services on the Internet affect supply chains across entire industries.

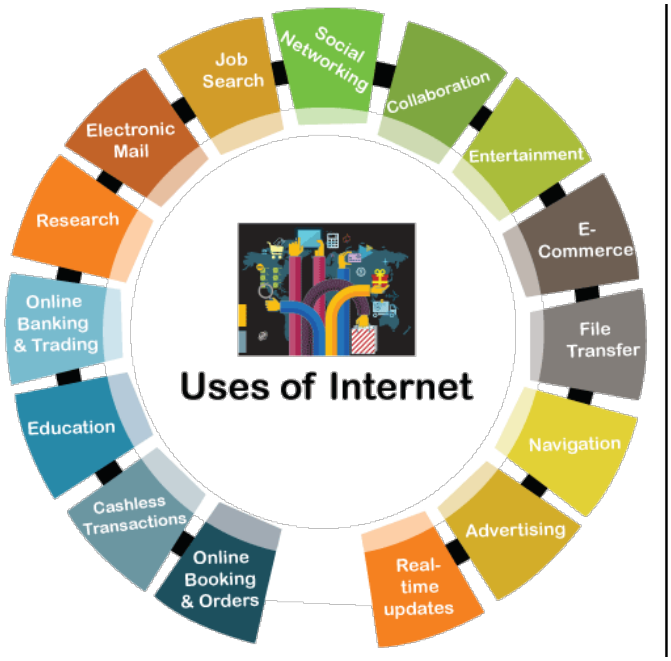
The Internet has no single centralized governance in either technological implementation or policies for access and usage; each constituent network sets its own policies.[1]

The overarching definitions of the two principal name spaces on the Internet, the Internet Protocol address (IP address) space and the Domain Name System (DNS), are directed by a maintainer organization, the Internet Corporation for Assigned Names and Numbers (ICANN). The technical underpinning and standardization of the core protocols is an activity of the Internet Engineering Task Force (IETF), a non-profit organization of loosely affiliated international participants that anyone may associate with by contributing technical expertise.

In November 2006, the Internet was included on *USA Today*'s list of the New Seven Wonders.

- The Internet is a global networking system that can be used on most devices nowadays and has become an essential part of our lives. In today's technological era, most of the companies are getting their operations done over the Internet. There are various uses of the Internet by which companies and individuals are making their daily tasks more productive and more comfortable.

- Here, we have discussed the major uses of the Internet that play a vital role in daily life:



Online Booking & Orders

- The Internet has made it a lot easier for people to book tickets for buses, trains, flights (domestic and international) directly using their devices from anywhere. People can also book a taxi by choosing their current location, and they will be picked up or dropped at a specified location. Now no one needs to wait in long queues for their turn to book tickets at the ticket counter.

- Besides, people can order a wide variety of products at home using the Internet and devices. It can range from grocery products to ready to eat, fashionable clothes to medicines. Most items can be ordered at home and received directly at the door.

Cashless Transactions

- Most countries are promoting cashless transactions and digital payments. This helps people not carry much cash. People can pay their bills through debit or credit cards using POS devices. These devices are connected to the payment gateway on the Internet. Besides, People can also use their smartphone and the

Internet for processing transactions on UPI (Unified Payment Interface). It does not even require them to carry their cards. The UPI payment method is continuously evolving and is expected to cover most transactions in the near future.

- ## Education

- Most of the devices nowadays are connected through the Internet. The Internet has the availability of broad educational content on any topic with different types. People can study the relevant topic just by spending a couple of minutes over the Internet. Internet Search engines help people quickly find the relevant study material in multiple formats (such as images, videos, documents, etc.). This helps eliminate the need to go to the library to read several books to find the desired information.

- Besides, the Internet has also enabled students to participate in their classes through video conferencing, where students can connect with their teachers or professionals anywhere in the world.

- ## Online Banking & Trading

- The way of banking has changed after the introduction of the Internet. The Internet has made banking online where people can manage their bank accounts while sitting at home or traveling abroad. Nowadays, most of the features of banking are right in people's hands. With the help of online banking, people can securely transfer the money from one account to another, change their ATM pins, apply for the physical or virtual credit cards, update credit card limits, enable or disable international transactions, track their transactions, and many more. Also, they can even raise an online complaint or contact to bank's support staff.

- Apart from this, the Internet has made it a lot easier for people to trade in the Stock market from anywhere. People can easily buy, sell, or manage stocks online.

- ## Research

- The Internet is playing a significant role in the field of research. Before the use of the Internet, it was quite hard to look for information about anything. People had to go through hundreds of books for references to find the desired information. However, the Internet has made it a lot easier, and anyone can find the required information at some clicks only. In research, people can study about the success and failed research and work further for the improvements. Uses of the Internet in research have incredibly beneficial for the researchers.

Electronic Mail

- Email or electronic mail is one of the first significant uses of the Internet. The email has enabled faster communication between people on the Internet. Using email, people can quickly share information, data files, such as images, audio, video, and other types of files. The use of email has significantly reduced paper use, which was the primary source of communication in the olden days. Anyone can have a free email address and can easily communicate with others. This has also reduced the load on the physical mail system, although it is still in use.

Job Search

- Getting a job is a lot easier than before. Any person can view relevant job information using the Internet. Earlier, people had to go through each company individually to know if a position was vacant or not. However, the Internet has enabled people to find employment sitting at home to suit their interests. Many websites provide details about job availability. Once people submit their resumes, these websites keep informing about vacancies through email. Besides, each well-known company has its website, where the company posts about the vacancy opening. So, just sitting at home, people can search, apply for jobs and even give their interviews and see or know their results.

Social Networking

- Social networking sites have connected people around the world. Social networking is an essential part of the Internet. With the help of the Internet, people have got the ability to form social groups where they can share

information, thoughts and ideas about anything. The social networking platform is the largest source of content, covering everything from informative content to entertainment. The best thing is that people don't have to pay anything to use these services. This helps businesses develop their community and promote their products.

- ## Collaboration

- Due to the Internet, communication has become easier and better. You can easily connect with anyone on the Internet, either texting, calling or video calling. It has created new cooperation opportunities for the people. There are several online chat software and websites that help people create group discussions or meetings. It helps businesses to have a hassle-free discussion. Therefore, people do not always need to travel long distances to attend meetings. This helps people avoid unnecessary travel and save time for productive use.

- Besides, there are many cloud-based software and websites that offer people to work on the same project simultaneously at the same time. People from different places can easily connect and support their specialties using the Internet.

- ## Entertainment

- The Internet is the most effective means of entertainment. There are various options available on the Internet, which people can try, such as watching movies, playing online games, listening to songs, etc. The Internet has also made it easy for people to download entertainment items to their local storage. Using the Internet, people can also share their videos, songs, pictures online with others. Also, nowadays, people can watch live TV or sports on the Internet.

- ## E-Commerce

- The Internet is not just limited to ordering things; it can also be used to sell products. Many e-commerce websites allow businesses and individuals to sell their products. Products are purchased by these e-commerce companies, stored in their warehouses, packaged in their brand packaging, and distributed by themselves. E-

commerce companies charge some commission to distribute goods to customers. Also, they offer great discounts and offers to customers. The best thing is that customers do not have to go to physical stores.

- Besides, sellers can also create their website and list their products there. They can refer to all information about the product, answer customer questions and provide online payment options to their customers. All these things are possible on the Internet.

File Transfer

- The Internet has made file transfer between systems or devices easier. With FTP (File Transfer Protocol), data can be securely exchanged over the Internet. FTP is mainly beneficial when large files need to be transferred because email allows sharing files with limited size. FTP is the best way to exchange information between two stakeholders. This method is still quite popular and in use.

Navigation

- The navigation mechanism is one of the most beneficial uses of the Internet. Once a user put the location in the online maps (such as Google maps), it provides all the details about that location. Users can even find the best route to visit that particular location. The map also provides the distance between the locations. The best thing about navigation is that it will provide the shortest possible route with less traffic. One can also search for any specific place like the nearest hotel, restaurants, banks, ATM, etc. Apart from this, a person can share a live location with others using the Internet and the navigation technique.

Advertising

- Because most people use the Internet, it is the best means of promoting something or advertising. There are options for paid promotion as well as free promotion. There are many advertising platforms on the Internet that help promote products or businesses online. These platforms advertise products on other related websites using banners, videos, email etc. They charge for these advertisements according

to distance, keywords and audience etc. However, one can also use social media platforms to create online groups or communities and advertise freely.

- Real-time updates

- The Internet is helping people to keep up with what is happening around the world. Many news and information websites provide real-time updates on various categories, such as politics, history, news, geology, leisure, sports, technology, marketing, and more. One can easily select the category of interest and stay connected with updates. The presence of e-newspapers and magazines is updating people and helping to cut paper usage.

Q13.What is the internet service provider? Give some example of ISP in India.

The internet service provider

The term “internet service provider (ISP)” refers to a company that provides access to the internet to both personal and business customers. ISPs make it possible for their customers to surf the web, shop online, conduct business, and connect with family and friends—all for a fee.

ISPs may also provide other services, including email services, domain registration, web hosting, and browser packages. An ISP may also be referred to as an information service provider, a storage service provider, an internet network service provider (INSP), or any combination of these three based on the services offered by the company.

KEY TAKEAWAYS

- An internet service provider (ISP) is a company that provides web access to businesses and consumers.
- ISPs may also provide other services such as email services, domain registration, web hosting, and browser services.
- An ISP is considered to be an information service provider, storage service provider, internet network service provider (INSP), or a mix of all of them.

- Internet use has evolved from only those with university or government accounts having access to nearly everyone having access, whether it's paid or free.
- Access has gone from dial-up connections to high-speed broadband technology.

Example of ISP in India

- Many of the largest ISPs are also large telecommunications companies that provide a wide array of services. For example, in addition to data and broadband internet services, AT&T (T) provides local and long-distance telephone service, managed networking, telecom equipment, and feature film, television, and gaming production and distribution.

- Verizon Communications (VZ) is another ISP that has a diversified range of services. The conglomerate offers local and long-distance voice, as well as broadband video, data center and cloud services, and security and managed network services.

- To help low-income families and seniors handle the cost, some ISPs offer special programs. The federal government also opened an Emergency Broadband Benefit (EBB) program on May 12, 2021, to provide help to families to get these services.4

Q14. Discuss the difference between MAC address, IP address and Port address.

. Mac Address

Media Access Control (MAC) address is a physical address that works at the data link layer of the OSI model.

- A MAC address is a 48 or 64-bit address associated with a network adapter.
- MAC addresses are linked to the hardware of the network adapters, hence they are also known as the "hardware address" or "physical address."
- MAC addresses uniquely identify the adapter on the LAN.
- MAC addresses are expressed in hexadecimal notation. For example, "01-23-45-67-89-AB" in a 48-bit address or "01-23-45-67-89-AB-CD-EF" in a 64-bit address. Sometimes, colons (:) are used instead of dashes (-).
- MAC addresses are often considered permanent, but in some conditions, they can be changed.

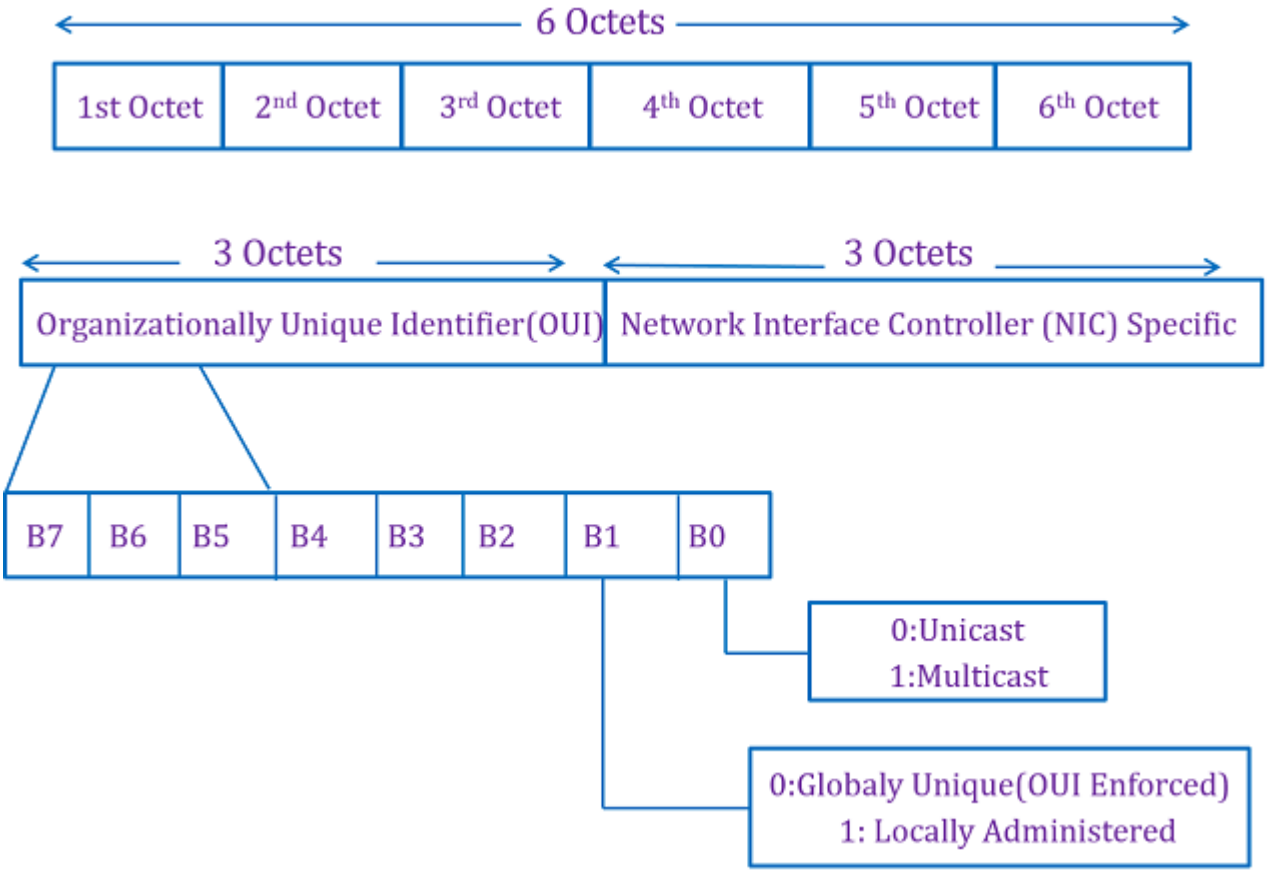
There are three types of MAC addresses −

- Unicast MAC Address
- Multicast MAC address
- Broadcast MAC address

MAC Address Format

A 48-bit MAC address is represented as a string of six octets, "MM:MM:MM:SS:SS:SS".

- The first half (24 bits) of the MAC address contains the ID number of the adapter manufacturer. These IDs are regulated by an Internet standards organization.
- The second half (24 more bits) of the MAC address represents the serial number assigned to the adapter by the manufacturer.



As shown in the above diagram, MAC addresses are 12-digit hexadecimal numbers (48 bits in length or 6-byte binary number). For example, let's take a network adapter with the MAC address "00-A0-C9-14-C8-29." The OUI (Organizational Unique Identifier) for the manufacture of this router is the first three octets ("00-A0-C9") is Intel corporation and the rightmost six digits represent the Network Interface Controller.

OUIs of some well-known manufacturers −

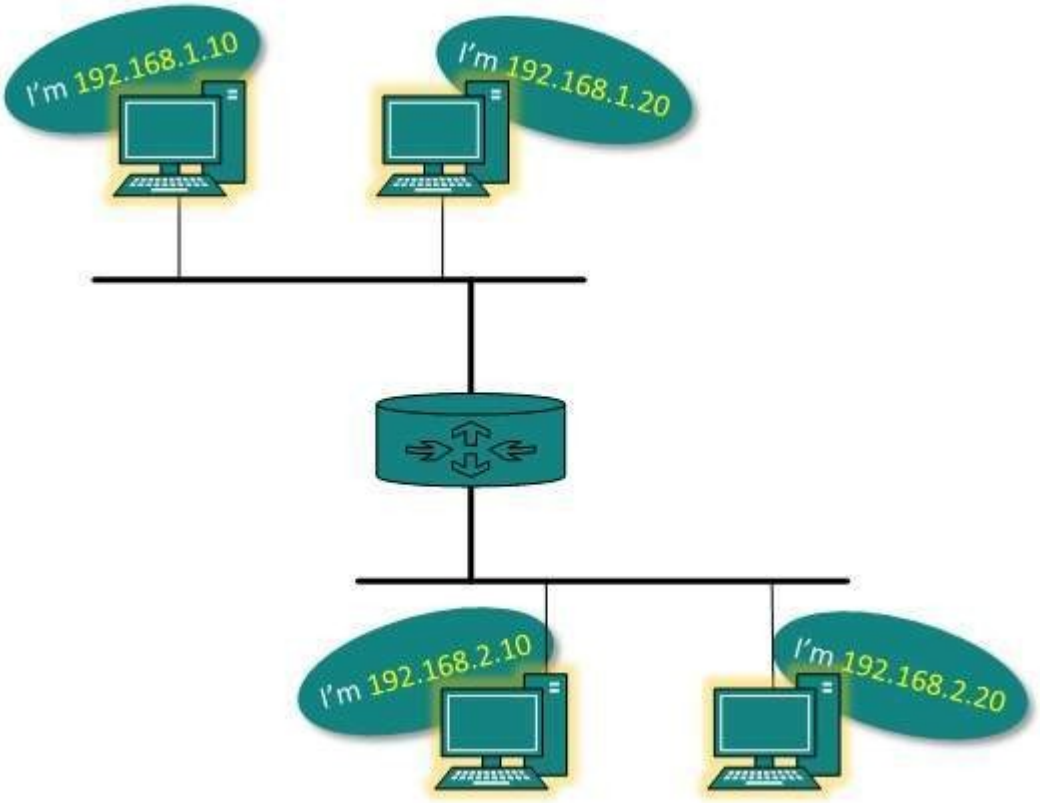
- "00-14-22" – Dell
- "00-04-DC" – Nortel
- "3C:5A: B4" – Google, Inc.

IP Address

A network address always points to host / node / server or it can represent a whole network. Network address is always configured on network interface card and is generally mapped by system with the MAC address (hardware address or layer-2 address) of the machine for Layer-2 communication.

There are different kinds of network addresses in existence:

- IP
- IPX
- AppleTalk



IP addressing provides mechanism to differentiate between hosts and network. Because IP addresses are assigned in hierarchical manner, a host always resides under a specific network.The host which needs to communicate outside its subnet, needs to know destination network address, where the packet/data is to be sent.

Hosts in different subnet need a mechanism to locate each other. This task can be done by DNS. DNS is a server which provides Layer-3 address of remote host mapped with its domain name or FQDN. When a host acquires the Layer-3 Address (IP Address) of the remote host, it forwards all its packet to its gateway. A gateway

is a router equipped with all the information which leads to route packets to the destination host.

Routers take help of routing tables, which has the following information:

- Method to reach the network

Routers upon receiving a forwarding request, forwards packet to its next hop (adjacent router) towards the destination.

The next router on the path follows the same thing and eventually the data packet reaches its destination.

Network address can be of one of the following:

- Unicast (destined to one host)
- Multicast (destined to group)
- Broadcast (destined to all)
- Anycast (destined to nearest one)

A router never forwards broadcast traffic by default. Multicast traffic uses special treatment as it is most a video stream or audio with highest priority. Anycast is just similar to unicast, except that the packets are delivered to the nearest destination when multiple destinations are available.

Port addressing

Port addressing refers to using the port numbers assigned to every process to exchange data between them. Now, for processes that send and receive data over the internet, the following information must be assigned to every process:

- **The IP address**: We use this to uniquely identify the machines that run the processes over the internet.
- **The port address (port number)**: We use this to identify the processes uniquely on a machine. This number can range from 0–65535.

Collectively, the IP address and port number form a **socket address (socket number)**. This enables every single process to be uniquely identified over the internet.

Forming the socket address

Socket addressing

The sender must provide the receiver's socket address for a packet to reach its intended destination. The first part of the socket address (the IP address) enables the packet to reach the receiver's machine. It will then route the packet to the designated process through the second part of the socket address (the port number).

The animation below illustrates how two processes on different machines can communicate using port addressing.

Q15.How do we view my Internet browser's history?

Today, all major browsers, including Firefox, Safari, Edge, and Chrome, have functionality that lets you quickly and easily view your search and

destination history. However, as different devices contain browser history, there are multiple ways to view it as well. To proceed, choose your desired device from the section below and follow the instructions.

Desktop or laptop computer

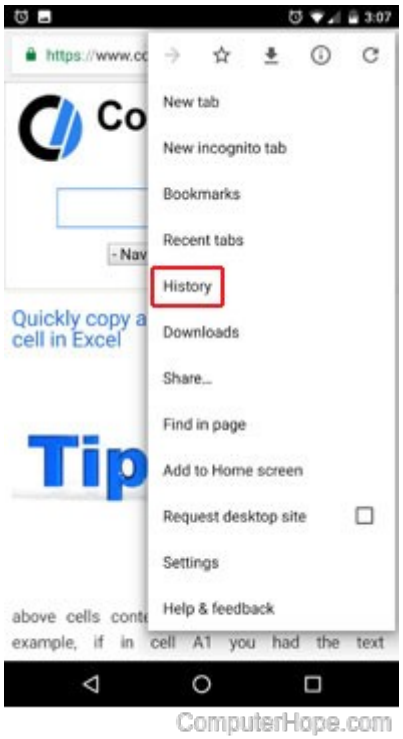
If you are using Windows, Linux, or macOS, a quick keyboard shortcut lets you view your history.

Windows and Linux users: Ctrl+H

Apple users: Command+Shift+H

When one of these keyboard shortcuts 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 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 page that opens contains your device's history.

iPhone or iPad running Safari

Users 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, tap and hold the back arrow.
3. The page that opens contains your browser's history.

Internet Browser

1. From a home screen, tap

   Apps

   .

2. Tap either Chrome or Internet Browser.

   Depending on device, default browser may vary.

3. Tap

   Bookmarks

   .

4. Tap

   History

   .