CCA-102:

Data

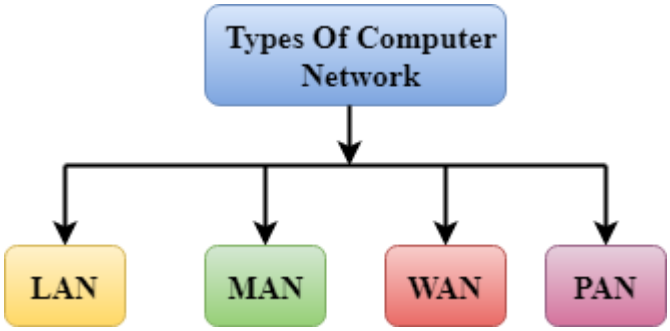
Communications

ASSIGNMENT

1. What are the different types of networks?

Ans. Computer Network Types

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.

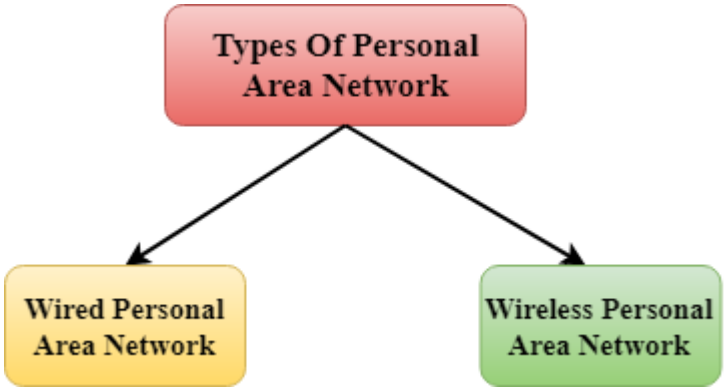
PAN(Personal Area Network)

- 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.

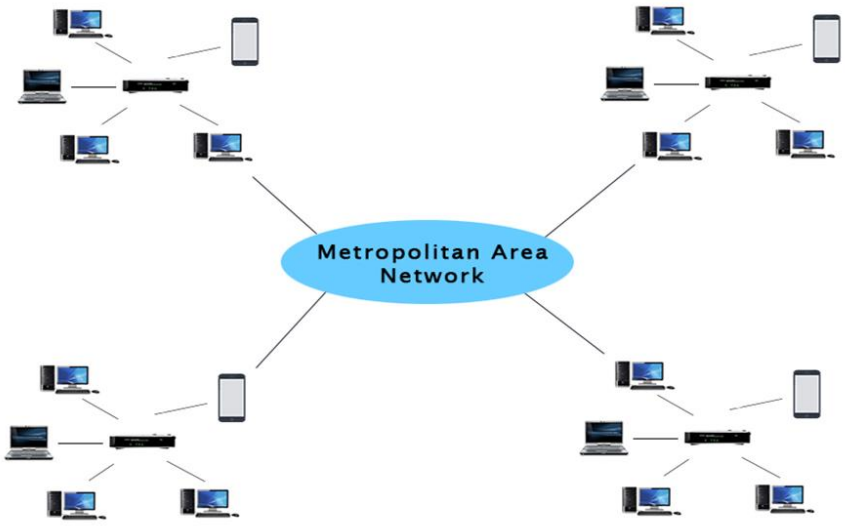
Wired Personal Area Network: Wired Personal Area Network is created by using the USB.

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).

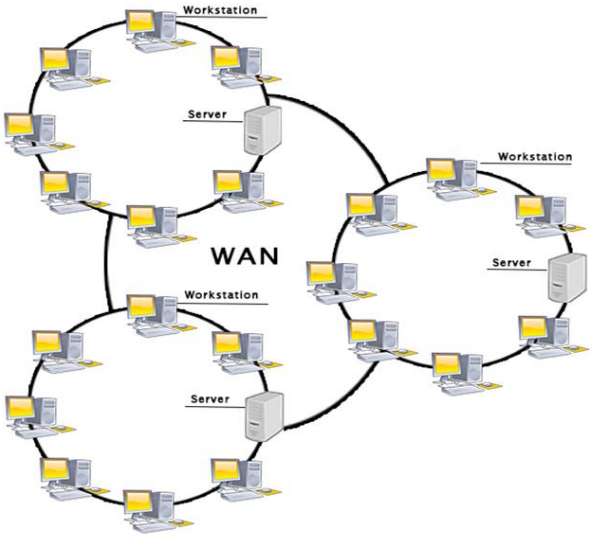


Uses Of Metropolitan Area Network:

- 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.

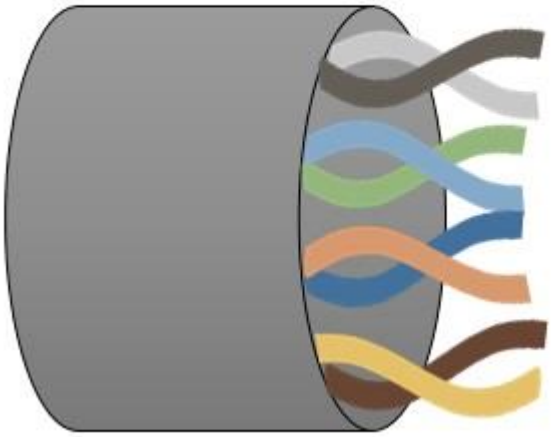
2. Explain the Shielded twisted pair (STP) and Unshielded twisted pair(UTP)

Ans. **Definition of UTP Cable**

Unshielded twisted-pair (UTP) cable is the most prevalent type of telecommunication medium in use today. Its frequency range is suitable for transmitting both data and voice. Therefore, these are most commonly used in telephone systems.

A twisted pair consists of two insulated conductors (usually copper) in a twisted configuration. Color bands are used in plastic insulation for identification. In addition, colors also identify the specific conductors in a cable and to indicate which wires belong in pairs and how they relate to other pairs in a larger bundle.

Unshielded Twisted Pair Cable

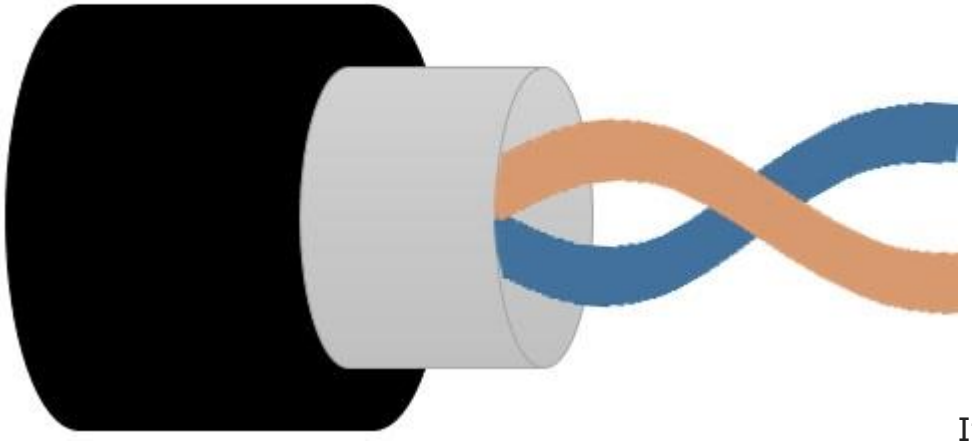


The two wires are twisted in the twisted pair cable which significantly reduces the noise generated by the external source. The **noise** here we are talking about is generated when two wires are parallel which causes an increase in voltage level in the wire closest to the source and also uneven load and damaged signal.

Definition of STP Cable

Shielded twisted-pair (STP) cable has an additional braided mesh coating or metal foil that wraps each set of insulated conductors. The metal casing intercepts the penetration of **electromagnetic noise**. It also can eradicate a phenomenon called crosstalk, which is the unwanted effect of one circuit (or channel) on another circuit (or channel).

Shielded Twisted Pair Cable



It occurs when one line (acting as a kind of receiving antenna) picks up some of the signals travelling down another line (acting as a kind of sending antenna). This effect can be experienced during telephone conversations when one

can hear other conversations in the background. Shielding each pair of a twisted-pair cable can eliminate most crosstalk.

STP has the similar quality factor and uses the same connectors as UTP, but the shield must be connected to the **ground**.

Key Differences Between UTP and STP Cables

1. UTP and STP are the types of twisted pair cable where UTP is the unshielded type whereas STP is shielded, for doing so metal foil or braided mesh is used.
2. UTP reduces the crosstalk and noise as compared to the parallel arrangement of the wires but not at great extent. On the contrary, STP decreases the crosstalk, noise, and electromagnetic interference significantly.
3. UTP cables are easily installed while installation of STP cables is difficult are the cables are bigger, heavier and stiffer.
4. Grounding is not required in UTP cables. As against, STP cables requires grounding.
5. UTP cables are inexpensive whereas STP cables are costly comparatively due to additional material and manufacturing.
6. STP cables incorporate a conducting shield built of metallic foil enclosing the twisted wire pairs, which obstructs out electromagnetic interference, permitting it to carry data at an enhanced rate of speed. In contrast, UTP provides less speed of data transfer.

Conclusion

UTP and STP cables differ in the design and structure where STP cable has an additional metal foil wrapped in insulated conductors.

However, both STP and UTP cables have their respective merits and demerits, when it comes to proper installation and maintenance in a suitable situation for their use, both work finely.

3. What is difference between baseband and broadband transmission?

Ans. Differentiating Between Baseband and Broadband Signaling

Two types of signaling methods are used to transmit information over network media: baseband and broadband. Before we get any further into 802.3 standards we should clarify the difference between the two.

Exam Alert: Baseband and broadband

Be prepared to identify the characteristics of baseband and broadband for the Network+ exam.

Baseband

Baseband transmissions typically use digital signaling over a single wire; the transmissions themselves take the form of either electrical pulses or light. The digital signal used in baseband transmission occupies the entire bandwidth of the network media to transmit a single data signal. Baseband communication is bidirectional, allowing computers to both send and receive data using a single cable. However, the sending and receiving cannot occur on the same wire at the same time.

Note: Ethernet and baseband

Ethernet networks use baseband transmissions; notice the word "base"—for example, 10BaseT or 10BaseFL.

Using baseband transmissions, it is possible to transmit multiple signals on a single cable by using a process known as *multiplexing*. Baseband uses Time-Division Multiplexing (TDM), which divides a single channel into time slots. The key thing about TDM is that it doesn't change how baseband transmission works, only the way data is placed on the cable.

Broadband

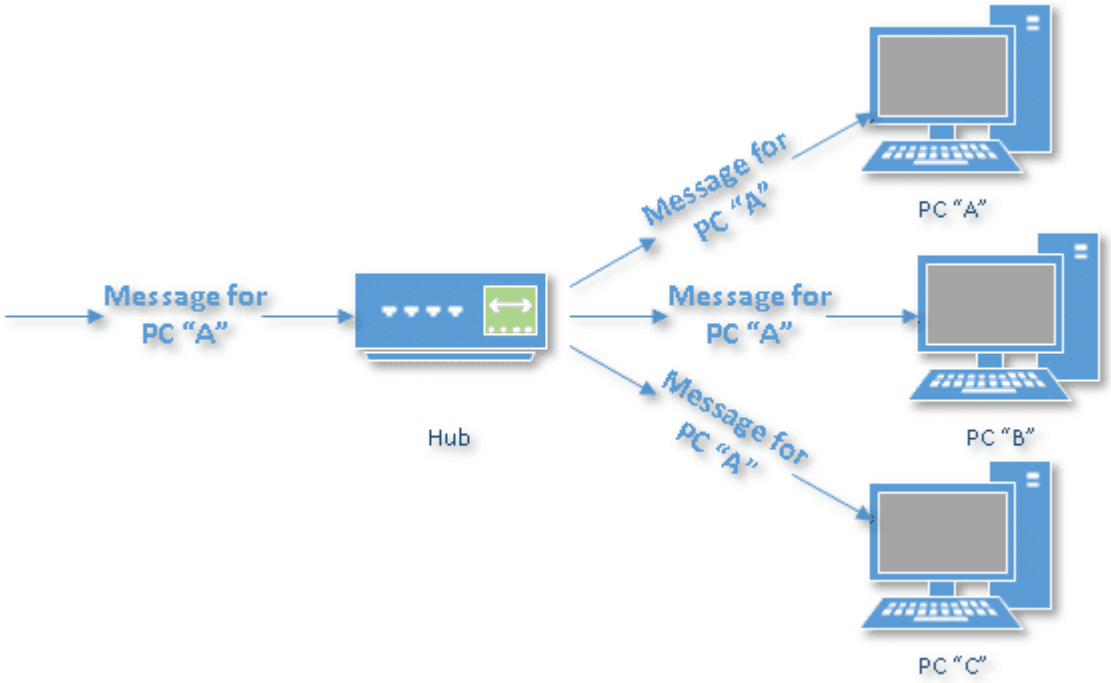
Whereas baseband uses digital signaling, broadband uses analog signals in the form of optical or electromagnetic waves over multiple transmission frequencies. For signals to be both sent and received, the transmission media must be split into two channels. Alternatively, two cables can be used: one to send and one to receive transmissions.

Multiple channels are created in a broadband system by using a multiplexing technique known as *Frequency-Division Multiplexing (FDM)*. FDM allows broadband media to accommodate traffic going in different directions on a single media at the same time.

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

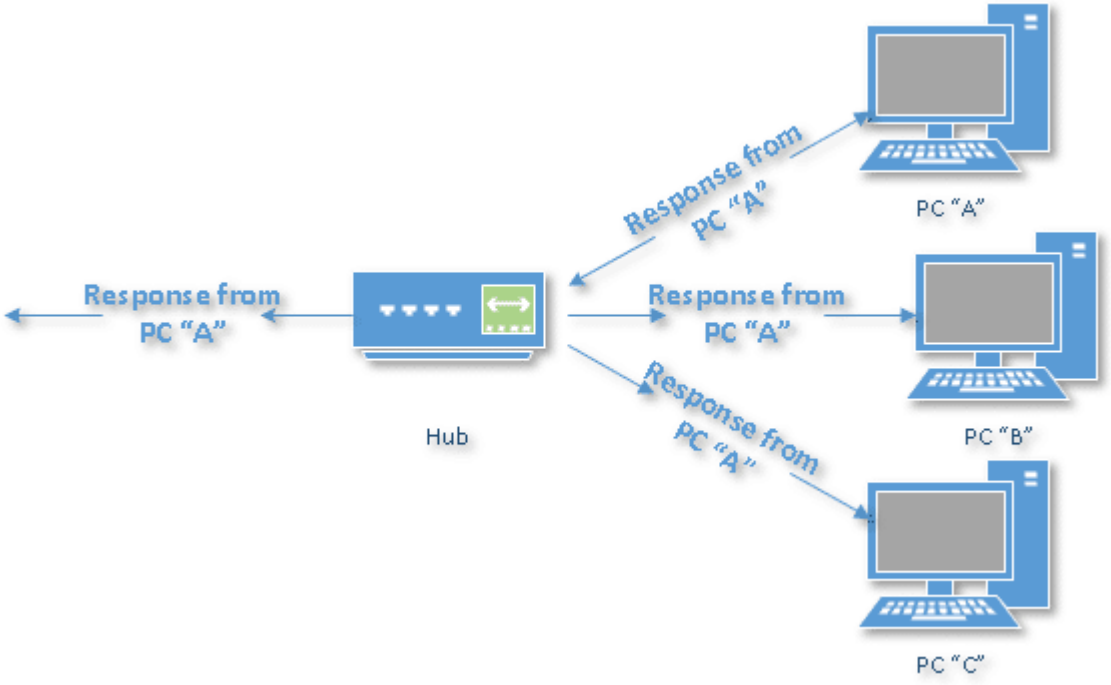
Ans. Hubs

A hub is the least expensive, least intelligent, and least complicated of the three. Its job is very simple: anything that comes in one port is sent out to the others. That's it.
If a message[1] comes in destined for computer "A", that message is sent out to all the other ports, regardless of which computer "A" is.



Incoming data passing through a hub.

When computer "A" responds, its response also goes out to every other port on the hub.



Returned response passing through a hub.

Every computer connected to the hub "sees" everything every other computer on the hub does. It's up to the computers themselves to decide if a message is for them and whether or not it should be

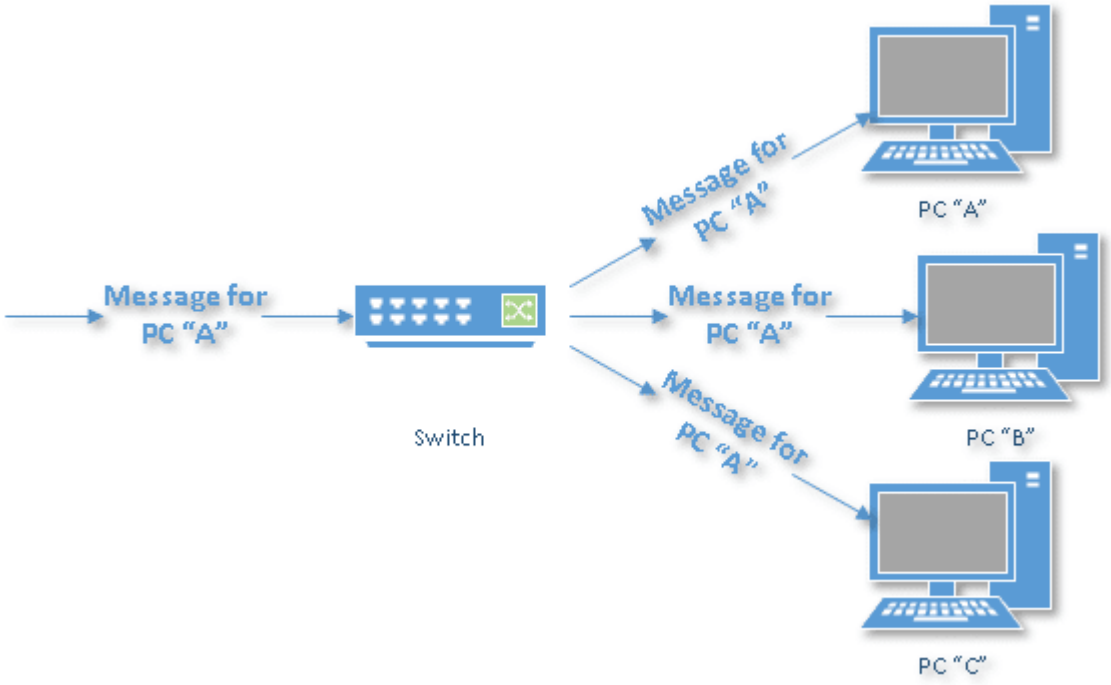
paid attention to. The hub itself is blissfully ignorant of the data being transmitted.

For many years, hubs were quick and easy ways to connect computers in small networks. In recent years, hubs aren't as common, and switches have come into greater use.

Switches

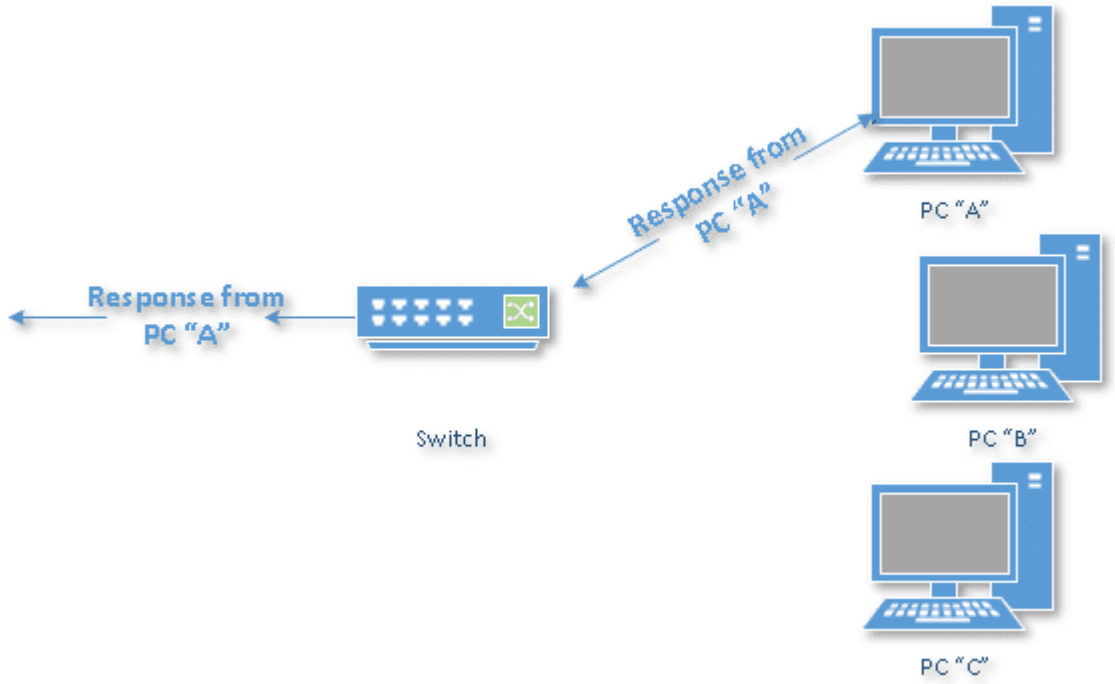
A switch does what a hub does, but more efficiently. By paying attention to the traffic that comes across it, it learns which computers are connected to which port.

Initially, a switch knows nothing, and simply sends on incoming messages to all ports.



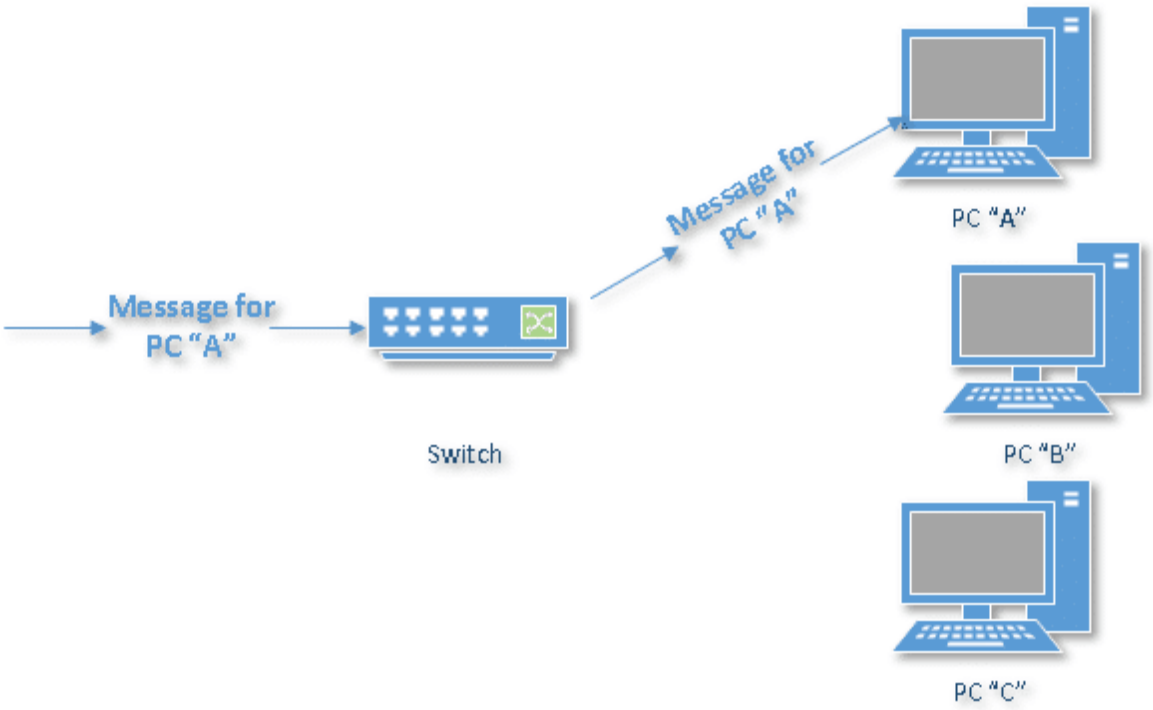
Incoming data passing through a switch.

Just by accepting that first message, however, the switch has learned something: it knows on which connection the *sender* of the message is located. Thus, when machine "A" responds to the message, the switch only needs to send that message out to the one connection.



Returned response passing through a switch.

By processing the response, the switch has learned something else: it now knows on which connection machine "A" is located. That means subsequent messages destined for machine "A" need only be sent to that one port.



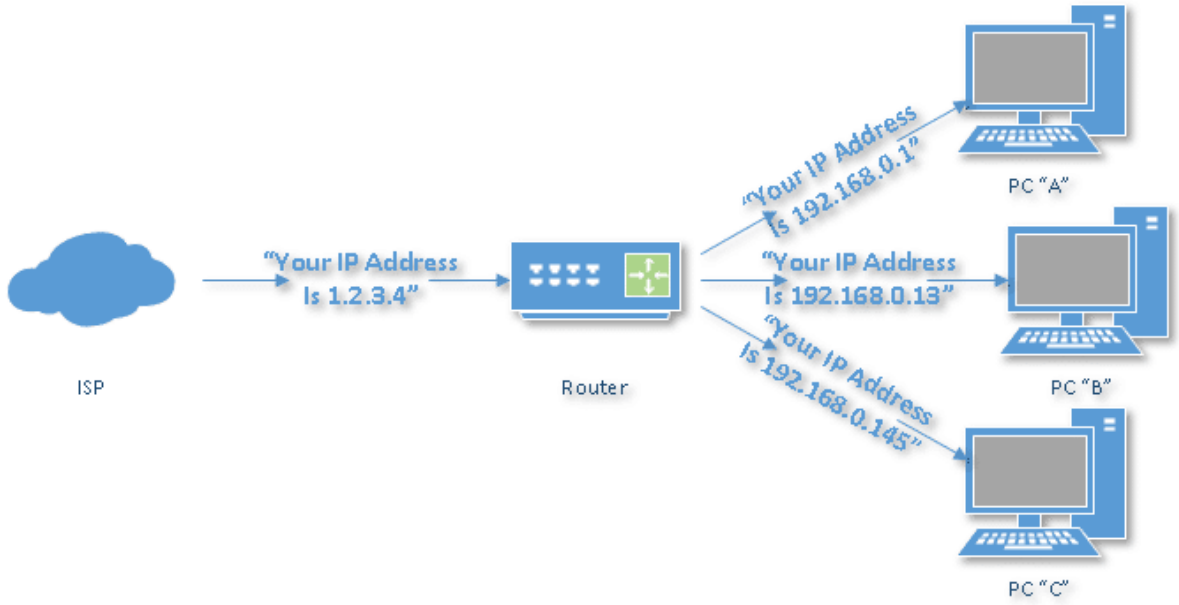
Second incoming message passing through a switch.

Switches learn the location of the devices they are connected to almost instantaneously. The result is, most network traffic only goes where it needs to, rather than to every port. On busy networks, this can make the network *significantly* faster.

Routers

A router is the smartest and most complicated of the three. Routers come in all shapes and sizes, from small, four-port broadband routers to large industrial-strength devices that drive the internet itself.
One way to think of a router is as a computer[2] that can be programmed to understand, manipulate, and act on the data it handles.
A router operates as a switch for basic routing: it learns the location of the computers sending traffic, and routes information only to the necessary connections.

Consumer-grade routers perform (at minimum) two additional and important tasks: DHCP and NAT.
DHCP — Dynamic Host Configuration Protocol — is how dynamic IP addresses are assigned. When it first connects to the network, a device asks for an IP address to be assigned to it, and a DHCP server responds with an IP address assignment. A router connected to your ISP-provided internet connection will ask your ISP's server for an IP address; this will be your IP address on the internet. Your local computers, on the other hand, will ask the router for an IP address, and these addresses are local to your network.



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.

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

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

Ans. **Common PC Hardware Problems**

In general, PCs are built with all security measures because all of their sensitive components and hardware will be housed inside a casing to protect the components from dust and other harsh elements. However, some common PC hardware problems occur despite the protection. Even though the most complex computer issues at the workplace can often be solved by the business IT support team, there are many other small, but common, problems that occur quite often on a personal computer. It's very important to identify and recognize such problems. The following are some of the commonly found hardware related problems on your PC.

Blank monitors

A blank monitor is the most common computer problem. Most people who work with computers might have dealt with such a non-working blank monitor at least once. In such cases, first and foremost is to check the supply cord and power systems. Sometimes, the video cable might be loosened. Just push the video cable and place it again, it should help you now.

Mouse Problems

The mouse is used for a variety of purposes, such as playing games or opening files, and moreover, it facilitates easy navigation, thus easy access to your data. The most common problems related to the mouse include failure to move, connection problems, freezing on the screen, or damage to the mouse.

Jumpy Mouse

Jumpy Mouse! Sounds strange right? Actually, a jumpy mouse is just a muted mouse i.e. cannot be scrolled. If you have a track and ball mouse, then simply turn it over and open the ball container, and remove the excess

debris and clean the dirt that lines the rollers. For an optical mouse, eliminate the dust that has collected around the optical sensor.

PC won't recognize my USB camera

In this case, even when you connect your USB camera, your PC might not be able to recognize it and hence throw errors like "Device not recognized" error. This might be due to the USB connector problems or the software malfunctioning. Before plugging in the camera, turn it on. This action can usually solve your problem.

My smartphone will not synch with my PC

In order to ensure backup of your smartphone, it is important that you regularly sync your phone content with your computer. At times, your PC might fail to sync with your smartphone. It can be due to many reasons. Sometimes it is required that all programs are closed, during syncing or backup.

Keyboard Problems

As we all know the keyboard is a vital part of any computer. It not only allows typing, but it also gives commands as well. However, you might encounter some common potential problems with the keyboard that includes keyboards that will not connect to the computer, stuck keys, broken keyboards, or keyboards where the letters end up jumbled.

Power Cord Problems

Whether it is a laptop or a desktop, power cords are a vital part of any computer. The desktop needs the power cord to work. A laptop can run on

batteries for a limited amount of time but then needs the power cord for recharging. The most common problem with the power cord is an improper connection.

Motherboard Problems

The motherboard contains several parts of the computer including the RAM, BIOS system, mass storage, and CPU. The computer motherboard contains several devices, which can create numerous potential problems. Problems with the motherboard range from too little RAM to BIOS problems. Fixing the problems will depend on the specific problem and, in the worst-case scenario, purchasing a new motherboard will fix the problems.

Insufficient Memory

Processor-intensive programs also demand a lot of memory. Random access memory (RAM) aides the central processing unit (CPU) by storing instructions linked to common operations. Without enough RAM, software crashes and slowdowns can occur.

Above mentioned are some of the commonly found PC hardware problems. However, these are minor issues and you can easily find a solution for it. As you can observe most of these issues are related to PC peripherals, for example, Mouse, keyboard, USB camera, etc. Hence, one of the root causes of these issues lies with your devices. Actually some devices need third-party software to be connected to the PC and even for its proper functioning. The software is referred to as Device drivers. Drivers help the operating system to communicate with the hardware and help in the proper functioning of these peripherals. Even your video cards, keyboards, mouse, or any USB device plugged into the computer requires device drivers.

At times, these device drivers become outdated, and hence, PC encounters any of the problems explained above. Most of the time updating your device drivers has resolved all your hardware issues caused by bad device drivers. So, you will have to find out an outdated driver and get the newer version of it and update the driver. In case all the drivers are outdated, then you need to download and update all the drivers in order to fix these PC hardware problems.

This is really a tedious process right. But, this is the only solution to get rid of these issues. One simple solution for this is Remo Driver Discover tool that could scan your PC thoroughly and locate all the outdated drivers. In addition, it even provides a single interface to download and update the device driver in just a few clicks. It is a time-savvy tool; you can make use of it or can do it manually that consumes lots of time. However, the best solution is to always keep updating your drivers to its newer versions and clean the peripherals regularly to avoid dirt that causes jumpy mouse and other problems.

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

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

Ans. **Static IP** addresses

If your computer is hosting a web server, its **IP** address is what identifies it to the rest of the Internet. A computer on the Internet can have a **static IP** address, which means it stays the same over time, or a dynamic **IP** address, which means the address can change over time.

Dynamic IP

A **dynamic IP address** is one that changes from time to time and isn't always the same. If you have a residential cable or DSL service, you most likely have a **dynamic IP address**. Internet Service Providers (ISPs) provide customers with a **dynamic IP addresses** because they are more cost effective.

Both are used to identify machines connected to a network. In principle, they are the same, but they are different in how they work.

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 filed	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.	lPv6 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 sending and forwarding routes.	Fragmentation is done by the sender.
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 flow for QoS handling which includes checksum options.	Packet head contains Flow Label field that 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 GMP)	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 DHCS (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
Combability 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, colon-separated notation. IPv6 is better suited to mobile

		networks.

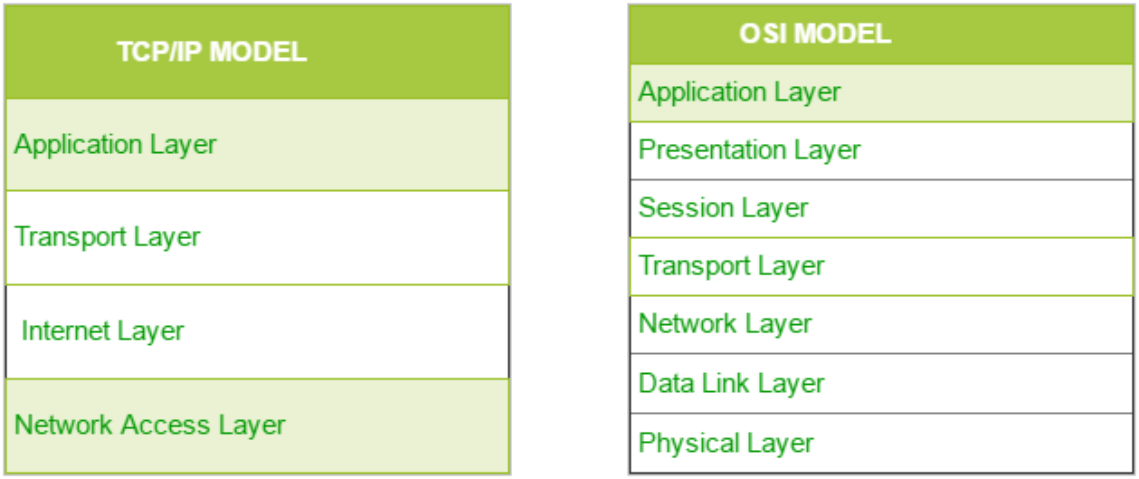
9. Discuss TCP/IP model in detail.

Ans. TCP/IP Model

The **OSI Model** we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

The diagrammatic comparison of the TCP/IP and OSI model is as follows :



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.

11. What is a search engine? Give example.

Ans. What is a search engine?

A search engine is a web-based tool that enables users to locate information on the World Wide Web. Popular examples of search engines are Google, Yahoo!, and MSN Search. Search engines utilize automated software applications (referred to as robots, bots, or spiders) that travel along the Web, following links from page to page, site to site. The information gathered by the spiders is used to create a searchable index of the Web.

How do search engines work?

Every search engine uses different complex mathematical formulas to generate search results. The results for a specific query are then displayed on the SERP. Search engine algorithms take the key elements of a web page, including the page title, content and keyword density, and come up with a ranking for where to place the results on the pages. Each search engine's algorithm is unique, so a top ranking on Yahoo! does not guarantee a prominent ranking on Google, and vice versa. To make things more complicated, the algorithms used by search engines are not only closely guarded secrets, they are also constantly undergoing modification and revision. This means that the criteria to best optimize a site with must be surmised through observation, as well as trial and error — and not just once, but continuously.

Gimmicks less reputable SEO firms tout as the answer to better site rankings may work at best for only a short period before the search engine's developers become wise to the tactics and change their algorithm. More likely, sites using these tricks will be labeled as spam by the search engines and their rankings will plummet.

Search engines only "see" the text on web pages, and use the underlying HTML structure to determine relevance. Large photos, or dynamic Flash animation mean nothing to search engines, but the actual text on your pages does. It is difficult to build a Flash site that is as friendly to search engines; as a result, Flash sites will tend not to rank as high as sites developed with well coded HTML and CSS (Cascading Style Sheets — a complex mechanism for adding styles to website pages above and beyond regular HTML). If the terms you want to be found by do not appear in the text of your website, it will be very difficult for your website to yield high placement in the SERPs.

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

Ans. Internet

The Internet *is a global network of networks while* the Web*, also referred formally as World Wide Web (www) is collection of*

information which is accessed via the Internet*. Another way to look at this difference is;* the Internet *is infrastructure while* the Web *is service on top of that infrastructure. Alternatively,* the Internet *can be viewed as a big book-store while* the Web *can be viewed as collection of books on that store. At a high level, we can even think of* the Internet *as hardware and* the Web *as software!*

World Wide Web

The World Wide Web, commonly known as the Web, is an information system where documents and other web resources are identified by Uniform Resource Locators, which may be interlinked by hypertext, and are accessible over the Internet

What are the uses of internet in our daily life?

Ans. Based on a recent survey of Internet traffic, the 10 most popular uses of the Internet in descending order of use are:

1. **Electronic mail.** At least 85% of the inhabitants of cyberspace send and receive e-mail. Some 20 million e-mail messages cross the Internet every week.
2. **Research.**
3. **Downloading files.**
4. **Discussion groups.** These include public groups, such as those on Usenet, and the private mailing lists that ListServ manages.
5. **Interactive games.** Who hasn't tried to hunt down at least one game?
6. **Education and self-improvement.** On-line courses and workshops have found yet another outlet.
7. **Friendship and dating.** You may be surprised at the number of electronic "personals" that you can find on the World Wide Web.
8. **Electronic newspapers and magazines.** This category includes late-breaking news, weather, and sports. We're likely to see this category leap to the top five in the next several years.
9. **Job-hunting.** Classified ads are in abundance, but most are for technical positions.
10. **Shopping.** It's difficult to believe that this category even ranks. It appears that "cybermalls" are more for curious than serious shoppers.

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

Ans.

List of internet service providers in India

This is a list of **internet service providers in India**. There were 358 internet service providers (ISPs) offering broadband and narrow band internet services in India as of 31 December 2019.

By subscribers[edit]

The following table shows the top 10 ISPs in India by total subscriber base as of 31 December 2019. Broadband is defined as "an always-on Internet connection with download speed of 512 kbit/s or above." The number of internet users are 718.74 million, out of which 56.80 million are narrow band subscribers and 661.93 million are broadband subscribers.[2]

Rank	ISP	Narrowband	Broadband	Total
1	Airtel	0	549,872,755	370,872,755
2	Reliance Jio	26,632,137	244,395,168	167,027,305
3	Vodafone Idea	23,614,475	118,453,704	142,068,179
4	BSNL	6,299,248	23,963,441	30,262,689
5	ACT Fibernet	0	1,518,853	1,518,853
7	Hathway	0	898,834	898,834
6	MTNL	201,088	891,113	1,092,201

Rank	ISP	Narrowband	Broadband	Total
8	APSFL	0	850,000	850,000
9	You broadband	14,675	770,609	785,284
10	GTPL Broadband Pvt. Ltd.	0	325,927	325,927
11	Excitel Broadband Pvt. Ltd.	0	319,323	319,323

Other notable ISPs[edit]

ISP	Coverage area
RailTel Corporation of India	State-owned ISP with pan-India optic fiber network along Railway track
Tikona Infinet Limited	
Fusionnet [1]	One of the best and most reliable ISP provider in Delhi NCR, Lucknow, haryana

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

Ans.

S.NO	MAC ADDRESS	IP ADDRESS
1.	MAC Address stands for Media Access Control Address.	IP Address stands for Internet Protocol Address.

2.	MAC Address is a six byte hexadecimal address.	IP Address is either four byte (IPv4) or six byte (IPv6) address.
3.	A device attached with MAC Address can retrieve by ARP protocol.	A device attached with IP Address can retrieve by RARP protocol.
4.	NIC Card's Manufacturer provides the MAC Address.	Internet Service Provider provides IP Address.
5.	MAC Address is used to ensure the physical address of computer.	IP Address is the logical address of the computer.
6.	MAC Address operates in the data link layer.	IP Address operates in the network layer.
7.	MAC Address helps in simply identifying the device.	IP Address identifies the connection of the device on the network.
8.	MAC Address of computer cannot be changed with time and environment.	IP Address modifies with the time and environment.
9.	MAC Address can't be found easily by third party.	IP Address can be found by third party.

Port address

Ans. A **port** is a number **used** to uniquely identify a transaction over a network by specifying both the host, and the service. They are necessary to differentiate between many different IP services, such as web service (HTTP), mail service (SMTP), and file transfer (FTP).

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

Ans.

As you browse the web, most web page data is cached locally on your computer to help pages load faster and reduces the amount of data you need to transfer over your internet connection.

To help keep your browsing history private, and to free up disk space on your computer, you can clear your local browsing history.

Microsoft Edge

Microsoft Edge is the default browser in Windows 10, replacing Internet Explorer on new computers.

To view your Edge browsing history

In a Microsoft Edge browser window, open the history menu using the keyboard shortcut Ctrl+H. You can also access this menu with the following steps:

1. Click the Hub button in the upper right-hand corner of the window.
2. Click the History icon to open the history menu.

This menu allows you to view the pages you've visited in chronological order.

To clear your Edge browsing history

1. Open the history menu as described above.
2. Click Clear all history.
3. Check the box next to each type of data you'd like to clear. Browsing history is the first item listed, so make sure this is checked.
4. Click Show more for additional options. Select any that you would like to clear.
5. Click Clear to erase the selected data.

6. If you want the selected items to be cleared automatically when you close your browser, set Always clear this when I close the browser to On.
7. When you're done, click the Hub button.

Google Chrome

To view your browsing history in Chrome

1. In any Chrome window, use the keyboard shortcut Ctrl+H, or navigate to the URL chrome://history .
2. Or, click the Menu button, which is located near the top-right side of the browser window, and choose History, then History again.

To clear your browsing history in Chrome

1. Click the Menu button , choose More tools and then Clear browsing data... Or, use the keyboard shortcut Ctrl+Shift+Del.
2. Select what data you'd like to clear from your history using the drop-down menu and check the appropriate boxes.

When you're ready to clear your history, click Clear browsing data.

Google Chrome on Android phone or tablet

Viewing and Deleting History

1. Open the Chrome browser on your Android phone or tablet.
2. Tap the Menu icon in the top right corner of the screen next to the address bar.
3. In the drop-down menu, tap History.
4. Tap CLEAR BROWSING DATA... at the bottom of the screen.
5. Select the appropriate boxes.
6. Tap the Clear button.

Google Chrome on iPhone

1. Open Google Chrome on your iPhone or iPad.
2. Click in the Google search or URL bar at the top of the screen.
3. A the bottom click View search history
4. Click the CLEAR ALL at the top right of the screen.
5. If you're sure, click CLEAR ON-DEVICE HISTORY.

Mozilla Firefox

There are several ways to view and edit your history in Firefox.

To view your browsing history in Firefox

1. If you do not have a custom homepage set, you can click the History button in any new browsing window.
2. Or you can always view your browsing history in the History sidebar. Open it by pressing Alt to show the menu bar, then choosing View → Sidebar → History. Or, you can use the keyboard shortcut, Ctrl+H.
3. You can also view your history if you click the hamburger menu button in the top right-hand corner of your window, then click History. This gives you a quick look at your history. From this menu you can also View History Sidebar.
4. Lastly, you can open your browsing history in the Firefox Library. To open this view, press Alt to show the menu bar, then choose History → Show All History. The keyboard shortcut for this view is Ctrl+Shift+H. When viewing your history here, you can highlight individual pages in your history and press Del to delete them. Right-click any item for more options.

To clear your browsing history in Firefox

1. Click the hamburger menu button and select History.
2. Choose Clear Recent History...

3. The *Clear Recent History* window will open. In the drop-down menu, choose how far back you want to clear the history, then click Clear Now.

   You can also access this menu using the keyboard shortcut Ctrl+Shift+Del.

Opera

The Opera browser has a very straightforward interface for viewing and editing your history.

To view your browsing history in Opera

In an Opera browser window, click the Opera menu button in the upper left-hand corner of the window and choose History to open the History tab. Or, use the keyboard shortcut Ctrl+H.

To clear your browsing history in Opera

1. Open the History tab as described above and click Clear browsing data...
2. In the drop-down menu Obliterate the following items from:, choose how far back in time you want to clear your history. To clear everything, choose the beginning of time.
3. Check the boxes next to the specific types of history you want to clear.
4. Click Clear browsing data.

Safari

Safari is the default web browser on Apple's OSX and iOS operating systems. Although it was previously available for Microsoft Windows, as of 2012 Apple no longer supports Safari on Windows.

To view your browsing history in Safari

1. Open the Safari browser.
2. Click the History menu at the top of the screen. The menu lists recent pages from your browsing history, which you can navigate to by clicking on them. To edit your history or view it in detail, click Show All History...

To clear your browsing history in Safari

1. Open the Show All History view. To delete individual history items, right-click them and choose Delete, or press the Delete key to clear selected history items
2. To clear everything, click Clear History.
3. Use the drop-down menu to choose how far back to delete your history.
4. Click Clear History.

Safari on iPhone and iPad

To view or delete your browsing history on iOS

1. Open the Safari browser on your mobile device.
2. Scroll up until you see the address bar at the top of the screen and a toolbar on the bottom.
3. On the toolbar at the bottom, click the fourth icon from the left that looks like a book.
4. Click History.
5. Click Clear in the lower right-hand side of the screen.

Microsoft Internet Explorer

Internet Explorer was Microsoft's internet browser until 2015, when it was replaced by Microsoft Edge. If you are still using Internet

Explorer on your computer, you can use the following steps to view or clear your browsing history.

WARNING: Security updates are no longer regularly provided for Internet Explorer and are not guaranteed to continue.

To ensure that your browser is secure when browsing the internet, you should use a different browser. If you are going to continue using Internet Explorer, check for any security updates that are still available and install them on your computer.

For example, the September 2016 Cumulative Security Update for Internet Explorer is currently still available from Microsoft's website.

To view your browsing history in Internet Explorer

Press Ctrl+H in any Internet Explorer browser window to view your history.

To clear your browsing history in Internet Explorer

1. Open an Internet Explorer browser window.
2. Press Ctrl+Shift+Del to open the Delete Browsing History window.
3. Check the boxes of the data you'd like to clear.
4. Click Delete.

To view your browsing history (Internet Explorer 7 and above)

1. In a Microsoft Internet Explorer browser window, click Tools in the upper right-hand corner.
2. Select Internet Options from the drop-down menu.
3. In the General tab, under Browsing history, click the Settings button.
4. In the Temporary Internet Files tab, click the View Files button.

To clear your browsing history (Internet Explorer 7 and above)

1. Open a Microsoft Internet Explorer browser window.
2. Click Tools in the upper right-hand corner.
3. Select Internet Options from the drop-down menu.
4. On the General tab, in the Browsing history section, click the Delete button.
5. Check the boxes of the data you'd like to clear.
6. Click Delete.

To view your browsing history (Internet Explorer 6)

1. Open a Microsoft Internet Explorer browser window.
2. In the toolbar at the top of the screen, click Tools.
3. In the Tools drop-down menu, select Internet Options.
4. Click the Settings button.
5. Click the View Files button.

To clear your browsing history (Internet Explorer 6)

1. Open a Microsoft Internet Explorer browser window.
2. In the toolbar at the top of the screen, click the Tools menu.
3. In the Tools drop-down menu, select Internet Options.
4. Click the Clear Browser History button.
5. Click the Delete Files button.
6. Click OK.

To clear your browsing history (Internet Explorer 4)

1. Open a Microsoft Internet Explorer browser window.
2. Click the History icon.
3. Click Clear Internet History.
4. Click OK.

To clear your browsing history (Internet Explorer 3 and below)

1. Open a Microsoft Internet Explorer browser window.
2. In the toolbar, click the View menu.
3. Click Options.
4. Open the Advanced tab.
5. Click the Settings tab.
6. Click the Empty Folder button.

Netscape

To view your browsing history in Netscape Navigator

1. Open a Netscape Navigator browser window.
2. From the toolbar, click Edit, Preferences, History.
3. Locate the folder in which Netscape is storing your files.
4. Double click this folder within Explorer to view your browser history.

To clear your browsing history in Netscape Navigator

1. Open a Netscape Navigator browser window.
2. From the toolbar, click Edit, Preferences, History.
3. Click the Clear History button.