1 What are the different types of networks?

Used for everything from accessing the internet or printing a document to downloading an attachment from an email, networks are the backbone of business today. They can refer to a small handful of devices within a single room to millions of devices spread across the entire globe, and can be defined based on purpose and/or size.

1. Personal Area Network (PAN)

The smallest and most basic type of network, a PAN is made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building. These types of networks are typically found in small offices or residences, and are managed by one person or organization from a single device.

2. Local Area Network (LAN)

We're confident that you've heard of these types of networks before – LANs are the most frequently discussed networks, one of the most common, one of the most original and one of the simplest types of networks. LANs connect groups of computers and low-voltage devices together across short distances (within a building or between a group of two or three buildings in close proximity to each other) to share information and resources. Enterprises typically manage and maintain LANs.

Using routers, LANs can connect to wide area networks (WANs, explained below) to rapidly and safely transfer data.

3. Wireless Local Area Network (WLAN)

Functioning like a LAN, WLANs make use of wireless network technology, such as Wi-Fi. Typically seen in the same types of applications as LANs, these types of networks don't require that devices rely on physical cables to connect to the network.

4. Campus Area Network (CAN)

Larger than LANs, but smaller than metropolitan area networks (MANs, explained below), these types of networks are typically seen in universities, large K-12 school districts or small businesses. They can be spread across several buildings that are fairly close to each other so users can share resources.

5. Metropolitan Area Network (MAN)

These types of networks are larger than LANs but smaller than WANs – and incorporate elements from both types of networks. MANs span an entire geographic area (typically a town or city, but sometimes a campus). Ownership and maintenance is handled by either a single person or company (a local council, a large company, etc.).

6. Wide Area Network (WAN)

Slightly more complex than a LAN, a WAN connects computers together across longer physical distances. This allows computers and low-voltage devices to be remotely connected to each other over one large network to communicate even when they're miles apart.

The Internet is the most basic example of a WAN, connecting all computers together around the world. Because of a WAN's vast reach, it is typically owned and maintained by multiple administrators or the public.

7. Storage-Area Network (SAN)

As a dedicated high-speed network that connects shared pools of storage devices to several servers, these types of networks don't rely on a LAN or WAN. Instead, they move storage resources away from the network and place them into their own high-performance network. SANs can be accessed in the same fashion as a drive attached to a server. Types of storage-area networks include converged, virtual and unified SANs.

8. System-Area Network (also known as SAN)

This term is fairly new within the past two decades. It is used to explain a relatively local network that is designed to provide high-speed connection in server-to-server applications (cluster environments), storage area networks (called "SANs" as well) and processor-to-processor applications. The computers connected on a SAN operate as a single system at very high speeds.

9. Passive Optical Local Area Network (POLAN)

As an alternative to traditional switch-based Ethernet LANs, POLAN technology can be integrated into structured cabling to overcome concerns about supporting traditional Ethernet protocols and network applications such as PoE (Power over Ethernet). A point-to-multipoint LAN architecture, POLAN uses optical splitters to split an optical signal from one strand of singlemode optical fiber into multiple signals to serve users and devices.

10. Enterprise Private Network (EPN)

These types of networks are built and owned by businesses that want to securely connect its various locations to share computer resources.

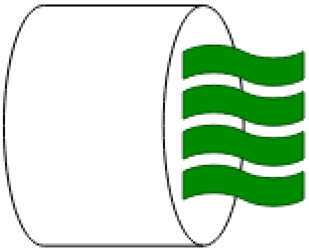
11. Virtual Private Network (VPN)

By extending a private network across the Internet, a VPN lets its users send and receive data as if their devices were connected to the private network – even if they’re not. Through a virtual point-to-point connection, users can access a private network remotely.

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

UTP:

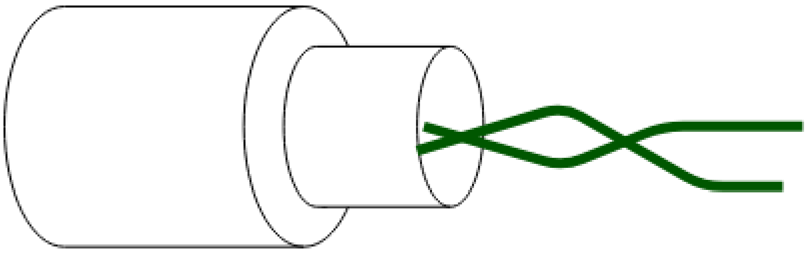
UTP is the type of twisted pair cable. It stands for Unshielded twisted pair. Both Data and voice both are transmitted through UTP because its frequency range is suitable. In UTP grounding cable is not necessary also in UTP much more maintenance are not needed therefore it is cost effective.



Unshielded Twisted Pair

STP:

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



Shielded Twisted Pair

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

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

	to STP.	
8.	In UTP, attenuation is high in comparison to STP.	While in STP attenuation is low.

3 What is the difference between baseband and broadband transmissions?

Ans: **Broadband** system use modulation techniques to reduce the effect of noise in the environment. Broadband transmission employs multiple channel unidirectional transmission using combination of phase and amplitude modulation.

Baseband is a digital signal is transmitted on the medium using one of the signal codes like NRZ, RZ Manchester biphase-M code etc. is called baseband transmission.

These are following differences between Broadband and Baseband transmission.

Baseband transmission –

1. Digital signalling.
2. Frequency division multiplexing is not pssible.
3. Baseband is bi-directional transmission.
4. Short distance signal travelling.
5. Entire bandwidth is for single signal transmission.
6. Example: Ethernet is using Basebands for LAN.

Broadband transmission –

1. Analog signalling.
2. Transmission of data is unidirectional.
3. Signal travelling distance is long.
4. Frequency division multiplexing possible.
5. Simultaneous transmission of multiple signals over different frequencies.
6. Example : Used to transmit cable TV to premises.

S.No	Baseband Transmission	Broadband Transmission
1.	In baseband transmission, the type of signalling used is digital.	In broadband transmission, the type of signalling used is analog.
2.	Baseband Transmission is bidirectional in nature.	Broadband Transmission is unidirectional in nature.
3.	Signals can only travel over short distances.	Signals can be travelled over long distances without being attenuated.
4.	It works well with bus topology.	It is used with a bus as well as tree

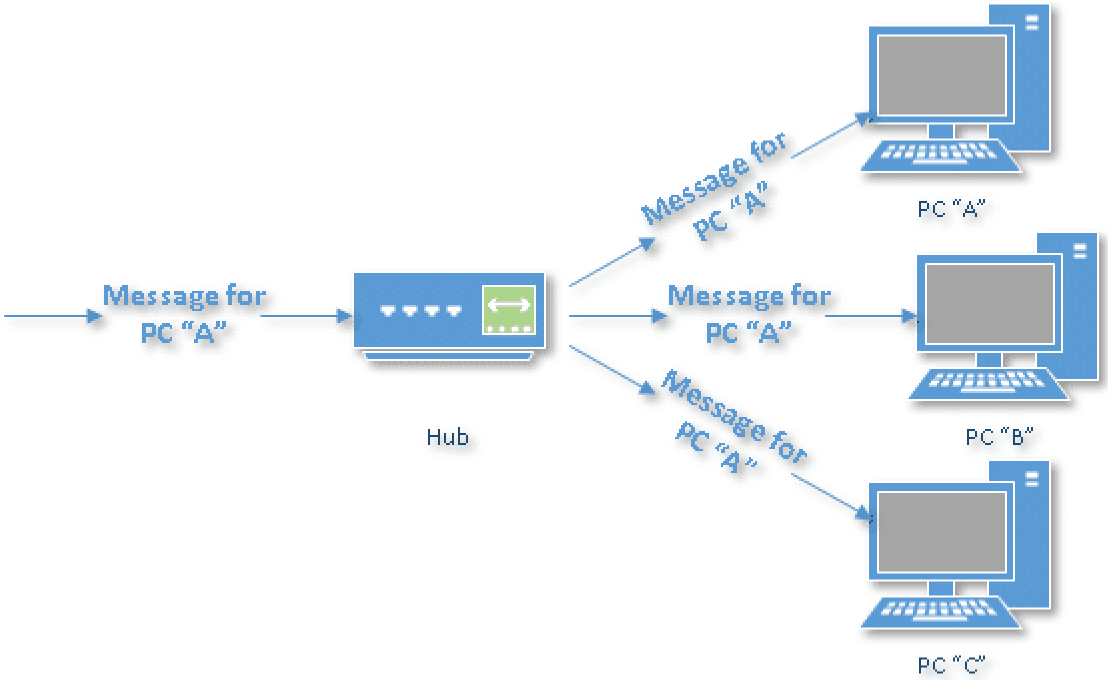
		topology.
5.	In baseband transmission, Manchester and Differential Manchester encoding are used.	Only PSK encoding is used.

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

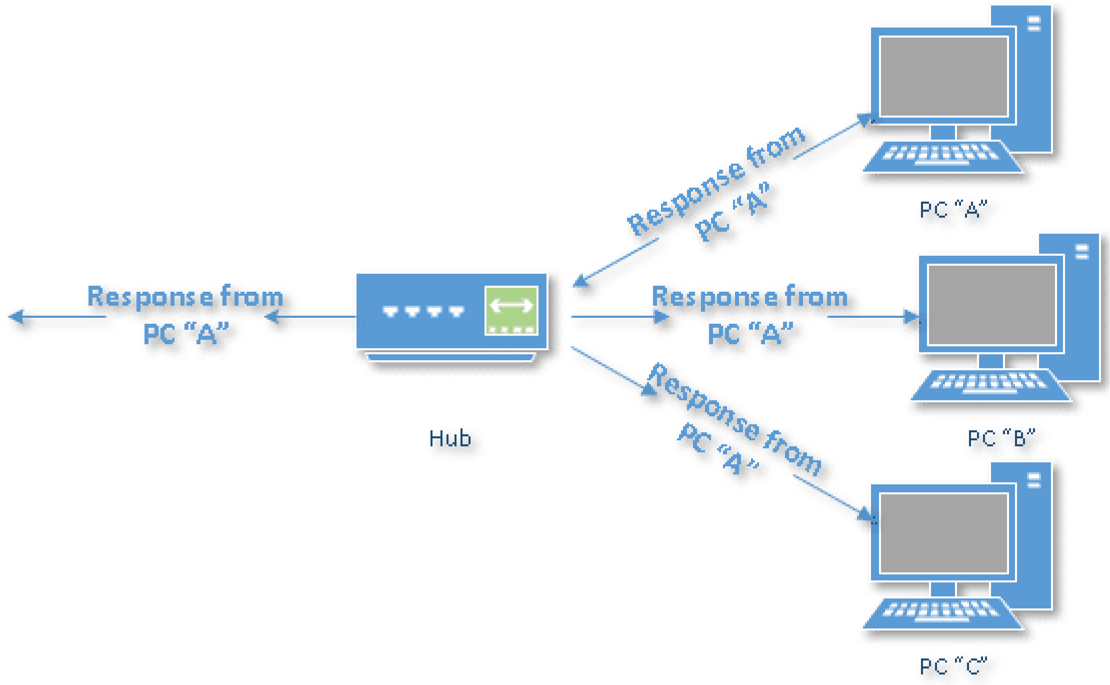
Ans: Hubs, switches, and routers are all devices that let you connect one or more computers to other computers, networked devices, or even other networks. Each has two or more connectors called ports, into which you plug the cables to make the connection.

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.



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



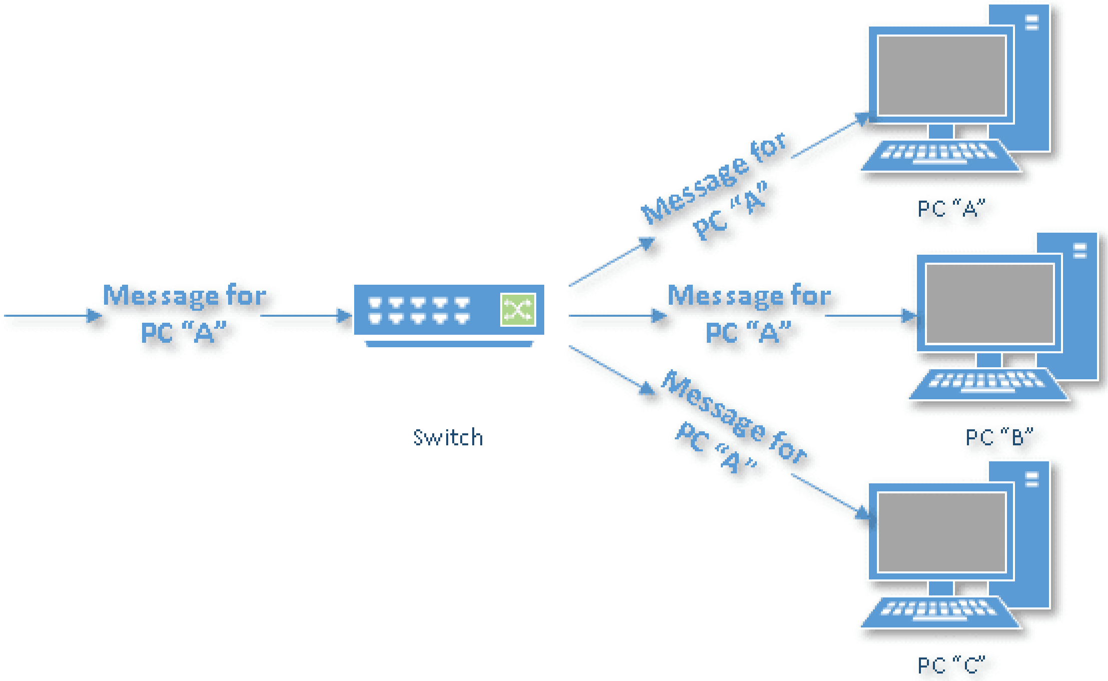
Every computer connected to the hub "sees" everything every other computer on the hub does. It's up to the computers themselves to decide if a message is for them and whether or not it should be paid attention to. The hub itself is blissfully ignorant of the data being transmitted.

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.

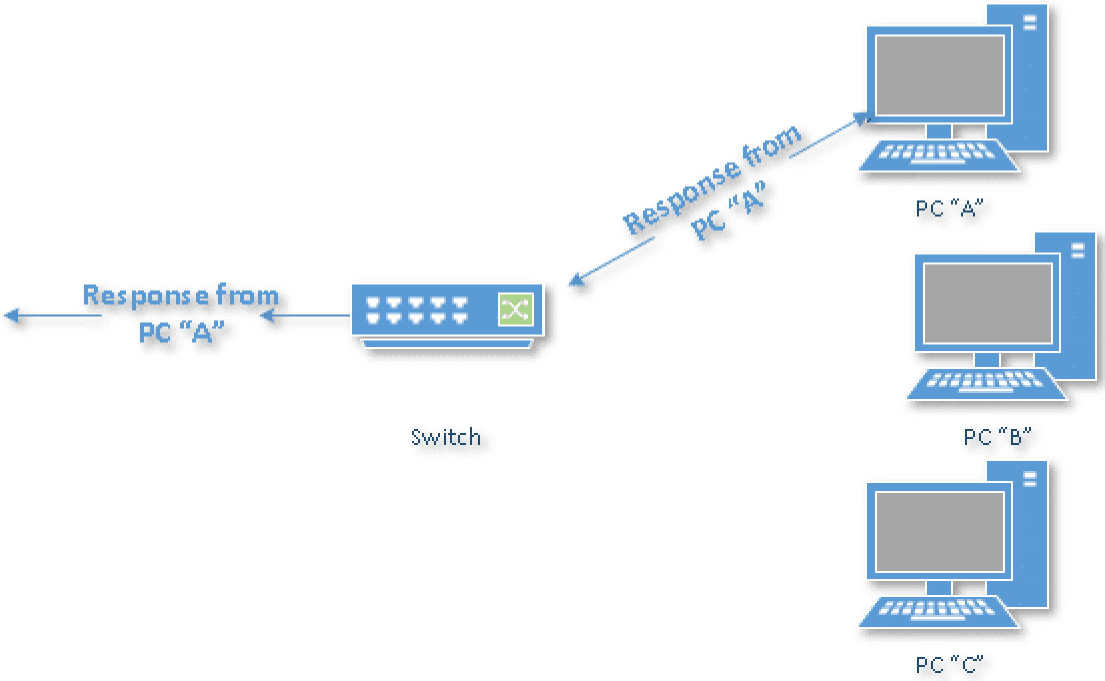
Switches

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.

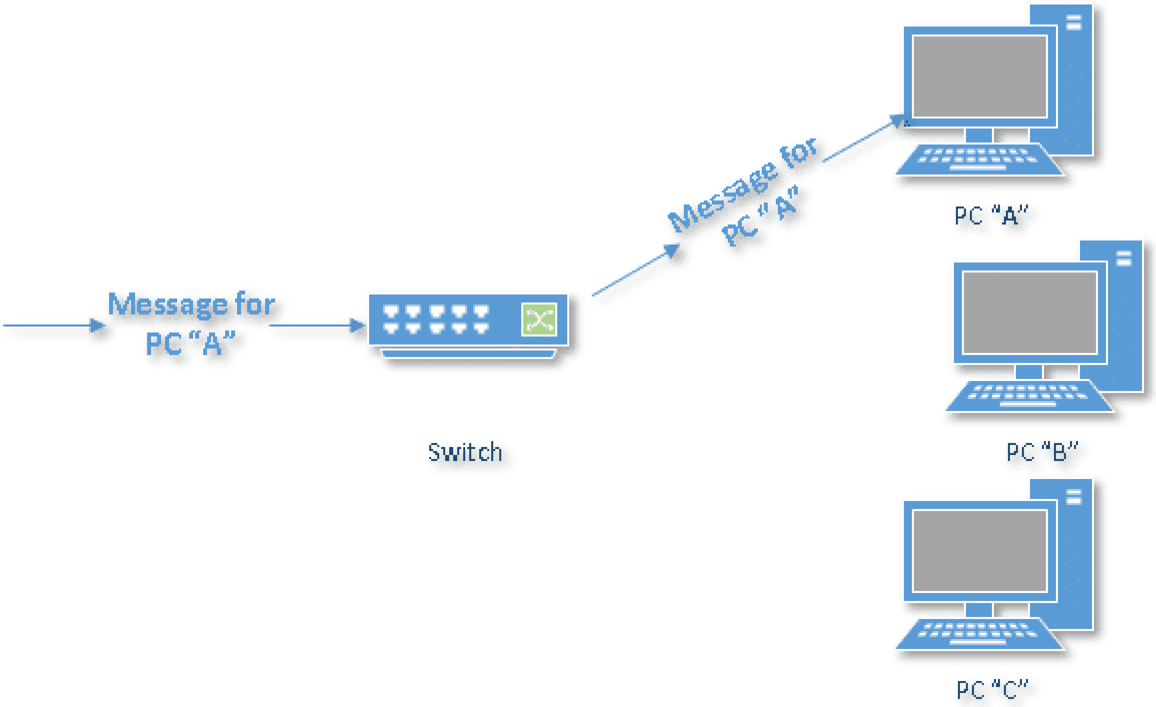
Initially, a switch knows nothing, and simply sends on incoming messages to all ports.



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.



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.

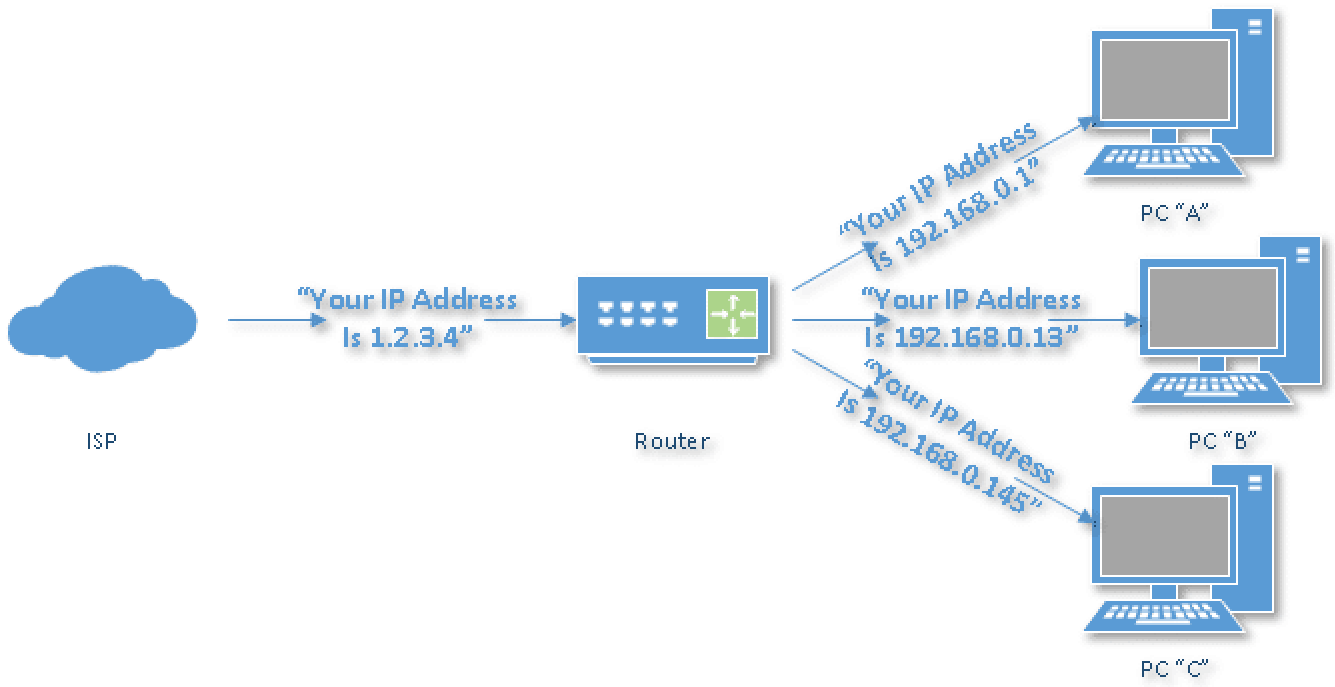


Switches learn the location of the devices they are connected to almost instantaneously. The result is, most network traffic only goes where it needs to, rather than to every port. On busy networks, this can make the network *significantly* faster.

Routers

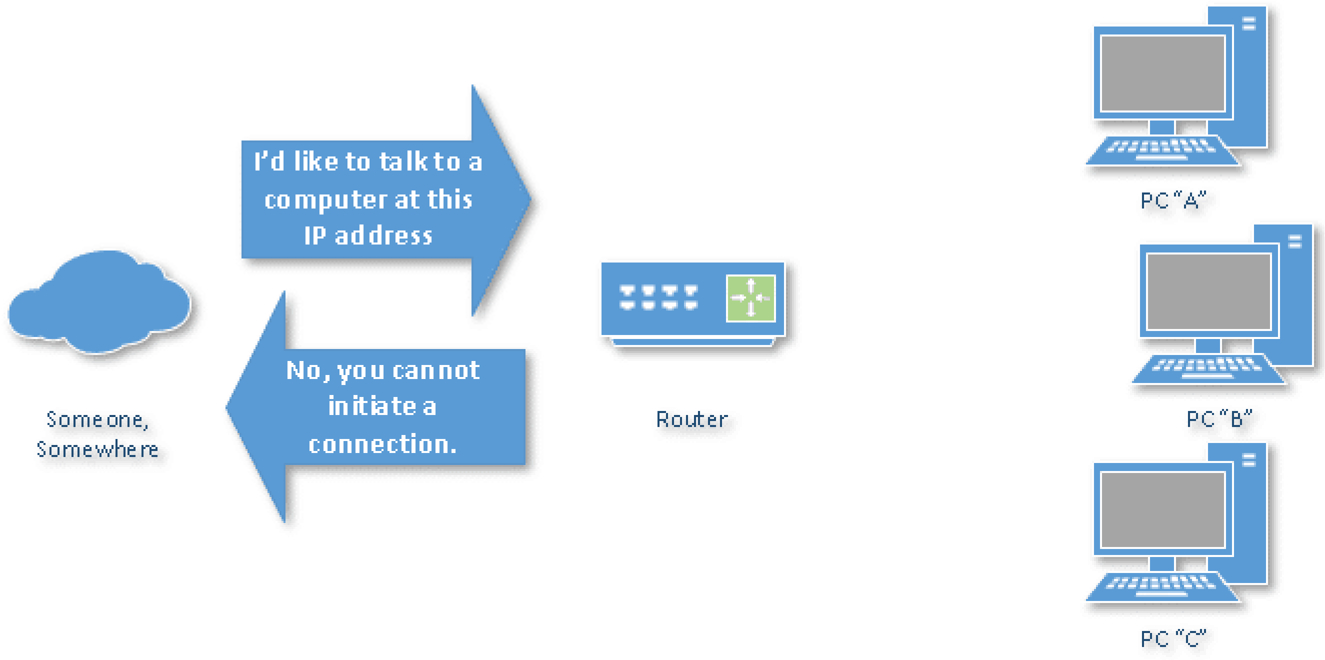
A router is the smartest and most complicated of the three. Routers come in all shapes and sizes, from small, four-port broadband routers to large industrial-strength devices that drive the internet itself.
One way to think of a router is as a computer[2] that can be programmed to understand, manipulate, 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.



NAT — Network Address Translation- – is the way the router *translates* the IP addresses of packets that cross the internet/local network boundary. When computer "A" sends a packet, the IP address that it's "from" is that of computer "A" — 192.168.0.1, in the example above. When the router passes that on to the internet, it replaces the local IP address with the internet IP address assigned by the ISP — 1.2.3.4, in the example. It also keeps track, so if there's a response the router knows to do the translation in reverse, replacing the internet IP address with the local IP address for machine "A", and then sending that response packet on to machine "A".

A side effect of NAT is that machines on the internet cannot *initiate* communications to local machines; they can only respond to communications initiated by them. This means that the router also acts as an effective firewall.


I'd like to talk to a computer at this IP address
No, you cannot initiate a connection.
Someone, Somewhere
Router
PC "A"
PC "B"
PC "C"

Malware that spreads by trying to independently connect to your computer over the network cannot do so.
All routers include some kind of user interface for configuring how the router treats traffic. Really large routers include the equivalent of a full-blown programming language to describe how they should operate, as well as the ability to communicate with other routers to describe or determine the best way to get network traffic from point A to point B.

What about wireless?

Of the devices we've discussed, only routers can be wireless. The wireless component is simply another way of making a connection to the device. For example, a wireless router might have four physical network connections to which cables can be connected, but the wireless component allows many more devices to connect over the air.

Modem:

A modem modulates outgoing digital signals from a computer or other digital device to analog signals for a conventional copper twisted pair telephone line and demodulates the incoming analog signal and converts it to a digital signal for the digital device.

In recent years, the 2400 bits per second modem that could carry e-mail has become obsolete. 14.4 Kbps and 28.8 Kbps modems were temporary landing places on the way to the much higher bandwidth devices and carriers of tomorrow. From early 1998, most new personal computers came with 56 Kbps modems. By comparison, using a digital Integrated Services Digital Network adapter instead of a conventional modem, the same telephone wire can now carry up to 128 Kbps. With Digital Subscriber Line (DSL) systems, now being deployed in a number of communities, bandwidth on twisted-pair can be in the megabit range.

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

Ans: The Media Access Control address (MAC address) for any network adapter is hard coded into the card itself. Each manufacturer of network adapters has a group of characters assigned that refer specifically to that company. I believe that is the first 1/2 of the MAC address which is 12 hexadecimal characters long. But the MAC address is part and parcel of the network adapter, just as your internal organs are part of you. When you move to a new house, you take your liver with you. In the same way, when you move a NIC to a different computer, it takes its MAC address with it.

Yes, certainly. The MAC address is set by the manufacturer of the end-station (the system that the Ethernet is plugged in to).

If the network interface is integrated within a computer, for instance, then the MAC is set there. If, let’s say, you installed a NIC within that computer and plugged the Ethernet cable into that NIC, then the MAC address would be the one on the NIC, not the one that’s associated with the integrated network interface which, in this case, isn’t used.
MAC addresses are burned into the NIC card and transfer with the network adapter.

Having said that, I can’t think of an even semi-modern OS that won’t let you change it to whatever you want in the configuration of the device. I’ve changed MAC addresses of computers many times over the years. Usually to fix stupid crap like assigning a software license to a particular MAC address. Worthless because you can easily change it. If I want to move it to a new server I’m just gonna change it rather than deal with trying to contact a company that may or may not even be in business anymore.

NIC is a Network Interface *Card*. Some computers have the network interface on the board so, technically, they don’t have a NIC but still have a MAC address. There are wireless connections that also have MAC addresses. There are probably a few other exceptions.

Almost any modern computer will have some sort of MAC address. So much so, that we are destined to run out of them at some point (4,294,967,296 in all), where some large blocks have been reserved. Hence the need for the IPv6 protocol.

As others have said MAC spoofing is the common terminology for using any mechanism that allows you to specify a different MAC address than the one programmed into your adapter.

You typically cannot change the MAC of your NIC permanently, although in some cases the MAC address is stored in non-volatile memory on the device and with sufficient access to its contents you could do so.

The main legitimate use of MAC spoofing is for some ISPs (rare) which identify the customer by the MAC of a combined modem/router that the customer then wants to replace with different equipment, which necessitates providing the original MAC address to the firmware of the new device via its configuration UI. Virtually all retail routers support this capability.

There should be few concerns about public identification of your MAC, as it is only part of the “physical layer” Ethernet or wifi traffic. This address is only used in Ethernet frames on whatever network segment the adapter is connected to, and as soon as your IP traffic passes through a router, your MAC address is no longer included in the data. IP packets do not use or transmit the MAC address of the source, only its IP address. *That* will be visible globally to every device that sees your traffic as it travels from source to destination.

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

Ans: A hardware problem or issue is one of the most dreaded incidences for a computer user. This is due to the fact that such a malfunction can result into complete computer failure. With respect to this, it is considered very important for an individual to be conversant with all the available troubleshooting tools. In addition, one should ensure that he or she is familiar with the indicators or symptoms of a hardware failure so as to curb it in advance. Below is a brief description of some of the most common hardware problems and their resolutions.

Here are some common symptoms through which one can know if the hardware has got some problems or not;

Unexpected shutdowns

Unexpected shutdowns occur when a computer just turns off without making any notification or giving a message. This is a problem that can be very frustrating since it can lead to loss of unsaved work or even interruption of a session one are logged onto. In most cases, such a problem occurs due to possible system changes such as addition of a new hardware driver. In such an occurrence, the operating system is not completely stopped and one can press the NUM Lock key or Ctrl+Alt+Del to try and get back to the OS for recovery.

In case that fails, one can run some hardware diagnostic tests so as to have a thorough check of anything that could be interrupting one's system. One can perform the Power on Self-Test (POST).

System lockups

System lockups can be very frustrating especially if they occur without the display of an alert message. The screen appears as if it is frozen. Looking at the Event viewer can be good but in such problems with one's hardware, it may not be of much help because the Event Viewer has nothing written on it.

POST code beeps

The Power on self-test occurs when one's computer is immediately powered on to check for one's computer's minimum hardware configurations. POST code beeps are normally delivered via the system speaker and serve as a communication media when the video is not working. Each beep has a correspondence to a specific error message.

Blank screen on boot up

A blank screen on boot up is another dreaded problem that does not necessarily indicate a problem with video but one associated with configurations of the BIOS. In such a case, one may choose to make BIOS modifications so that instead of using a separately installed video card, one can configure the BIOS to utilize the in-built one and identify some of the problems occurring.

BIOS time and settings resets

Unplugging one's computer or powering it off does not lead to lose of computer configurations. At times, the BIOS configurations may keep resetting and getting erased due to the CMOS battery on the motherboard getting spoilt or it no longer being charged. In addition, one may also receive some prompts indicating an invalid configuration or incorrect date and time setting. In case of such a problem, replacing the CMOS battery can be the best way to come up with a resolution for the problem. One can also decide to carry out a complete clearance of the BIOS configuration which should be done in accordance to documentations by the manufacturer.

Attempts to boot to incorrect device

At times, one may see attempts by one's computer to boot from the wrong device for instance when one are using an external USB and the computer system attempts to boot from the USB instead of the internal drive in the computer. The boot order of one's computer can be set at the BIOS where one decide the particular drive to start up or one may alter the order in which the boot process occurs. With such a problem at hand, one should take a look at one's BIOS configurations and possibly modify them in a way that is ideal for one's system.

Continuous reboots

This is a problem that mostly occurs in instances where one's computer keeps looping over the start up process where it appears to be starting and then restarts. In such a case, the first step should be to try and establish the occurrence point of the problem either in the course of the BIOS check where the Power on Self-test is undergoing among some other possible reasons. Once that is established, then one can easily decide if the problem is hardware related or related to the Windows configuration.

No power

At times, one may turn on one's computer and nothing of much significance happens. This should therefore reflect to the possibility of some power related issues in one's computer. Use one's Multimeter check so as to see if there is some power coming from the wall socket. Also ensure that the motherboard is powered which can then help in identification of the problem in one's computer.

Overheating

One's computer tends to emit a lot of heat due to the numerous numbers of components running in it and generating the heat. In case of an overheating problem, then urgent cooling is required. One can induce cooling by using some fans to bring in cool air into one's computer. In this case, the fans can be passed over the warm equipment making the heat to rise up and allow the cool air to pass in much faster.

The HW Monitor is an example of software that one can use to access and determine the level of heat in one's computer

One can also do some troubleshooting or maybe clean one's system. Make an effort to ensure that there is proper spinning of the fans, clear dust and restart one's system to check if such a heat problem occurs. With that, one will be able to accurately determine the occurrence point of one's problem.

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

Ans: The best solution is to install anti-virus on all the computers in the network. This will protect each device from the other in case some malicious user tries to insert a virus into the servers or legitimate users.

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

Ans:

Static IP:

A static IP address is an IP address that was manually configured for a device instead of one that was assigned by a DHCP server. It's called static because it doesn't change vs. a dynamic IP address, which does change.

Routers, phones, tablets, desktops, laptops, and any other device that can use an IP address can be configured to have a static IP address. This might be done through the device giving out IP addresses (like the router) or by manually typing the IP address into the device from the device itself.

Dynamic IP:

A dynamic IP address is an IP address that changes from time to time unlike a static IP address. Most home networks are likely to have a dynamic IP address and the reason for this is because it is cost effective for Internet Service Providers (ISP's) to allocate dynamic IP addresses to their customers.

Instead of one IP address always being allocated to your home network (Static IP), your IP address is pulled from a pool of addresses and then assigned to your home network by your ISP. After a few days, weeks or sometimes months that IP address is put back into the pool and you are assigned a new IP address.

Difference between IPV4 And IPV6:

Basis for differences	**IPv4**	**IPv6**
Size of IP address	IPv4 is a 32-Bit IP Address.	IPv6 is 128 Bit IP Address.
Addressing method	IPv4 is a numeric address, and its binary bits are separated by a dot (.)	IPv6 is an alphanumeric address whose binary bits are s

Basis for differences	**IPv4**	**IPv6**
		eparated 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.	IPv6 allows storing an unlimited number of IP Address.
Configuration	You have to configure a newly installed system before it can communicate with other systems.	In IPv6, the configuration is optional, depending upon on functions needed.
VLSM support	IPv4 support VLSM (Virtual Length Subnet Mask).	IPv6 does not offer support for VLSM.
Fragmentation	Fragmentation is done by 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.

Basis for differences	**IPv4**	**IPv6**
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.

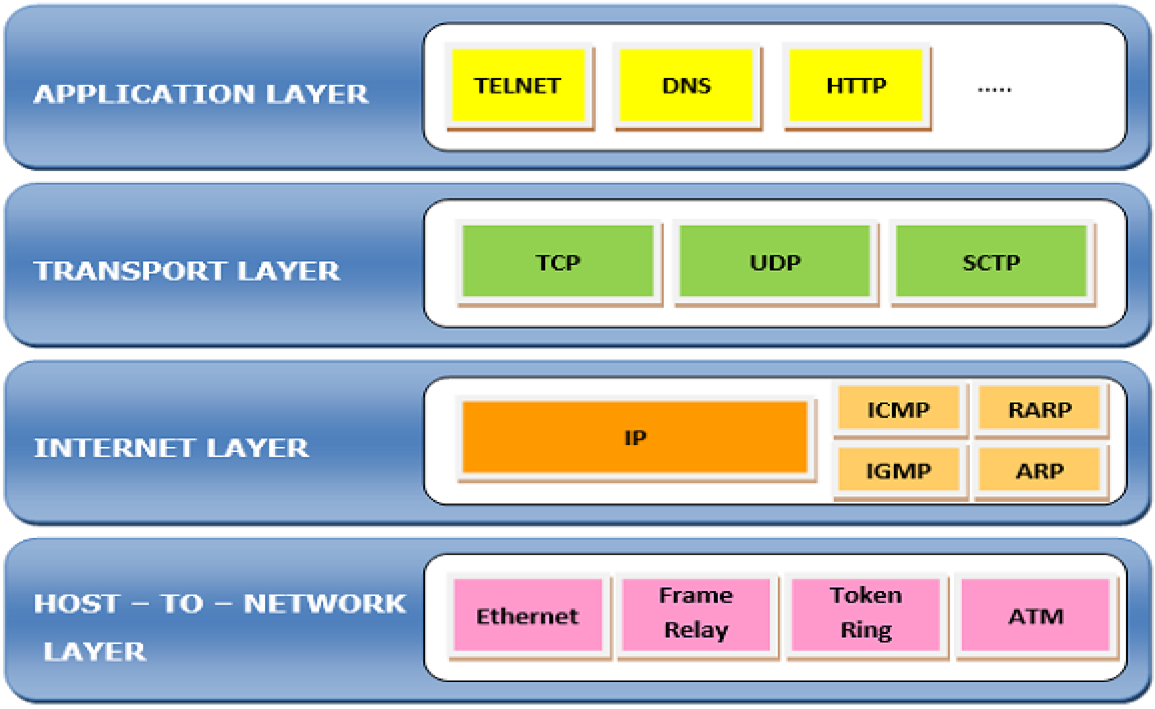
IPv4 and IPv6 cannot communicate with other but can exist together on the same network. This is known as **Dual Stack.**

9 Discuss TCP/IP model in detail.

Ans: TCP/IP Reference Model is a four-layered suite of communication protocols. It was developed by the DoD (Department of Defence) in the 1960s. It is named after the two main protocols that are used in the model, namely, TCP and IP. TCP stands for Transmission Control Protocol and IP stands for Internet Protocol.

The four layers in the TCP/IP protocol suite are −

- **Host-to- Network Layer −**It is the lowest layer that is concerned with the physical transmission of data. TCP/IP does not specifically define any protocol here but supports all the standard protocols.
- **Internet Layer −**It defines the protocols for logical transmission of data over the network. The main protocol in this layer is Internet Protocol (IP) and it is supported by the protocols ICMP, IGMP, RARP, and ARP.
- **Transport Layer −** It is responsible for error-free end-to-end delivery of data. The protocols defined here are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- **Application Layer −** This is the topmost layer and defines the interface of host programs with the transport layer services. This layer includes all high-level protocols like Telnet, DNS, HTTP, FTP, SMTP, etc.



10. What is the Web browser (browser)? Give some examples of browsers.

Ans: **Web Browser**:

A web browser, or browser for short, is a computer software application that enables a person to locate, retrieve, and display content such as webpages, images, video, as well as other files on the World Wide Web.

Browsers work because every web page, image, and video on the web has its own unique Uniform Resource Locator (URL), allowing the browser to identify the resource and retrieve it from the web server

Examples:

1. Google Chrome

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

2. Apple Safari

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

3. Microsoft Internet Explorer and Edge

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

4. Mozilla Firefox

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

5. Opera

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

11. What is a search engine? Give examples.

Ans: A search engine is a web based tool that is used by people to locate information on the internet. Some of the most popular examples of search engines are Google, Bing, Yahoo!, & MSN Search.

Google is the most used search engine worldwide with a 92 percent market share in mid-2019. Google may be one of the most popular search engines but there are many more alternative search engines available for users.

Top Search Engines alternative to Google

1. Bing
2. DuckDuckGo
3. Wiki.com
4. Ecosia
5. Yahoo!
6. Swisscows
7. CC Search
8. Gibiru

9. Qwant
10. Yandex
11. Disconnect
12. Ask

1. **Bing**

   Bing after Google is the best search engine example. Bing is operated and owned by Microsoft. Bing provides the user a variety of search services, like web, video, image and map search products. It performs perfectly across browsers. It works fairly well with mobile apps on Android as well as iOS. Bing enjoys a 33 percent market share in US. Its image search is amazing as it offers sharp and high-resolution images .

2. **DuckDuckGo**

   DuckDuckGo is a search engine perfect for those who like to keep their browsing information personal. Thus, in case of privacy DuckDuckGo is the next best example of a search engine. It is user friendly. DuckDuckGo does not profile its users and does not track searches.

3. **Wiki.com**

   Another search engine example is Wiki.com. Users can use it as a quick reference guide for various topics. Wiki.com is the best choice for people who like Wikipedia type of content. It can be used as a quick reference guide.

4. **Ecosia**

   Ecosia is an environment-friendly search engine. Ecosia has a tie-up with Bing. It is safe as they do not collect any userâ€™s data or even use it to show customized ads. For every 45 searches you make, you will be supporting them in planting a tree.

5. **Yahoo!**

   Yahoo another search engine example has been around before Google. Yahoo offers loads of other services other than search. Even on privacy front Yahoo performs better than Google. Its web portal offers services like sports, travel and entertainment.

6. **Swisscows**

   Swisscows also overpower Google in the case of privacy as this search engine does not track data. Users will get an interactive search experience. Swisscows is based on semantic data recognition that gives faster answers to queries.

7. **CC Search**

CC Search provides a copyright free content. This search engine works the best if you are looking for an image for your content or some original music for your video. It offers over 300 million images indexed from multiple collections.

8. **Gibiru**

   This search is the best in terms of privacy and censorship. User search queries are not saved on its servers making the information searched confidential. Gibiru shows results of the search, including those that have been censored for regular users.

9. **Qwant**

   Qwant is an EU search engine. It does not do any user tracking and does not personalize search results. The interface is user friendly with myriad features like news, entertainment on the homepage.

10. **Yandex**

    Yandex Search engine is a Russian search engine with easy to use features and provides a wide range of specialized search features. Like Google it can be accessed from personal computers, mobiles, tablets.

11. **Disconnect**

    Disconnect Search is a specialized VPN (Virtual private network) that lets you search privately using any search engine. It takes care of privacy as it does not log searches, IP addresses. It is an open source browser.

12. **Ask**

    Ask previously called Ask Jeeves is another popular search engine. It loved for its simple question and answer format. This search engine features faqs on the side. It is also a video search engine, which locates YouTube videos for the user.

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

Ans: Internet:

The internet is the wider network that allows computer networks around the world run by companies, governments, universities and other organisations to talk to one another. The result is a mass of cables, computers, data centres, routers, servers, repeaters, satellites and wifi towers that allows digital information to travel around the world

WWW:

Many people think that the internet and the world wide web are the same thing. While they are closely linked, they are very different systems.

The internet is a huge network of computers all connected together. The world wide web ('www' or 'web' for short) is a collection of webpages found on this network of computers. Your web browser uses the internet to access the web.

Uses of Internet in our Daily life:

- → The Internet is an information and communication network technology consisting of computer devices, united by communication channels to receive and transmit information by connected users.
- → A proper name of the Internet is spelled with a capital letter "**Internet**"✔.
- → In technical words, the Internet is a software and hardware complex for processing, storing, and transferring information, the components of which exchange data over a variety of communication channels.
- → A person perceives the Internet to exchange information (like *audio, video, text, graphics*), exchange of opinions, and self-expression. For society, the Internet is a single information space in which an environment for communication between individuals and groups of people arrangements.
- → The Internet is the most effective mass media communication, allowing communication between a lot of people **without restrictions.**
- → Now almost every city on our planet has access to the Internet. We start every day by checking messages, likes, tweets, trends, news, and memes, all kinds of information. We cannot imagine *life without the Internet* " **A Beloved Internet**."
- → The processing, and use of information and knowledge, due to the increasing technical possibilities of Internet communication are becoming increasingly important for society.
- → The Internet is excellent for **the informatization of the world** since the beginning of the modern world. It is a fair and accessible source of various information and a means of circulation of knowledge.
- → During the 21st century, a stage of mankind's development, all significant communities of interest groups have formed on the Internet, which continues to act as the search engine for the growth of both the process of communication and the Internet itself too.
- → At the same time, information has long become a natural resource that consistently allowing you and me to **change and upgrade our life**.
- → With the Internet's arrival, a person can communicate with another person (often with strangers). Simultaneously, there is no dependence on the location of both, and communication can be maintained continuously. It allows people to create content, solve the problem, and communicate with each other, like virtual reality.
- → This way can be used both for **leisure or for business purposes**. At the same time, communication by using the Internet has removed many technical

and psychological restrictions. It has become easier to contact a person, and communication has become more extended.

→ The reasons for the increasing role of the Internet in modern society are the endless desire of a person to understand others and to be understood by others and the progressive development of methods for receiving, processing, collecting, and businesses.

→ Today’s Internet covers all forms of interpersonal communication, allowing for verbal and non-verbal interaction between people—instant communication on the Internet, which fundamentally distinguishes it from other significant means of communication.

→ Almost every day, we start, spend and finish in front of the computers or smartphones: by watching news feeds, making purchases, paying for services, online gaming, entertainment, work, and study.

→ Thanks to the emergence and development of the Internet, a universal information environment has emerged, distinguished by a high degree of interactivity, availability of information, the efficiency of information exchange, and ease of information transfer.

13 What is and Internet Service Provider? Give some examples of ISP in Indai?

Ans: Internet Service Provider:

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

Examples of ISP:

1	Reliance Jio
2	Airtel
3	Vodafone Idea
4	BSNL
5	ACT Fibernet
6	APSFL

7	MTNL
8	Excitel
9	Hathway
10	You Broadband
11	GTPL Broadband

14 Discuss the difference between Mac Address, IP Address and Port Address.

Ans: Mac Address:

- MAC address is the physical address, which uniquely identifies each device on a given network. To make communication between two networked devices, we need two addresses: **IP address and MAC address.** It is assigned to the NIC (Network Interface card) of each device that can be connected to the internet.
- It stands for **Media Access Control**, and also known as **Physical address, hardware address, or BIA (Burned In Address).**
- It is globally unique; it means two devices cannot have the same MAC address. It is represented in a hexadecimal format on each device, such as **00:0a:95:9d:67:16.**
- It is 12-digit, and 48 bits long, out of which the first *24 bits are used for **OUI**(Organization Unique Identifier),* and *24 bits are for NIC/vendor-specific.*
- It works on the data link layer of the OSI model.
- It is provided by the device's vendor at the time of manufacturing and embedded in its NIC, which is ideally cannot be changed.
- The **ARP protocol** is used to associate a logical address with a physical or MAC address.

IP Address:

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

In essence, IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works.

Port Address:

Ports are standardized across all network-connected devices, with each port assigned a number. Most ports are reserved for certain protocols — for example, all Hypertext Transfer Protocol (HTTP) messages go to port 80. While IP addresses enable messages to go to and from specific devices, port numbers allow targeting of specific services or applications within those devices.

Ports are standardized across all network-connected devices, with each port assigned a number. Most ports are reserved for certain protocols — for example, all Hypertext Transfer Protocol (HTTP) messages go to port 80. While IP addresses enable messages to go to and from specific devices, port numbers allow targeting of specific services or applications within those devices

15 How do we view my Internet browser’s history?

Ans:

BrowsingHistoryView is a utility that reads the history data of different Web browsers (Mozilla Firefox, Google Chrome, Internet Explorer, Microsoft Edge, Opera) and displays the browsing history of all these Web browsers in one table. The browsing history table includes the following information: Visited URL, Title, Visit Time, Visit Count, Web browser and User Profile. BrowsingHistoryView allows you to watch the browsing history of all user profiles in a running system, as well as to get the browsing history from external hard drive.
You can also export the browsing history into csv/tab-delimited/html/xml file from the user interface, or from command-line, without displaying any user interface.

.