CCA-102: Data Communications
ASSIGNMENT

Q: 1 - What are the different types of networks?

Ans:-1

Computer Network Types:

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

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

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

LAN(Local Area Network)

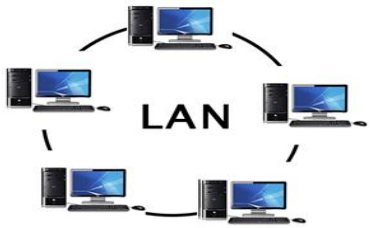
Local Area Network is a group of computers connected to each other in a small area such as building, office.

LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.

It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.

The data is transferred at an extremely faster rate in Local Area Network.

Local Area Network provides higher security.



PAN (Personal Area Network)

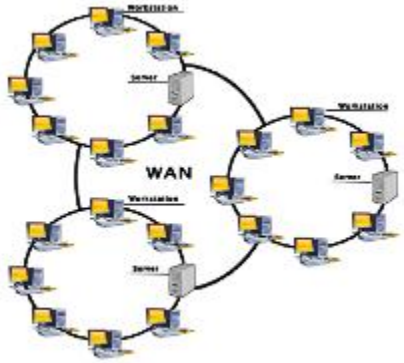
- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of **30 feet**.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

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).

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.



Q 2:-- Explain the Shielded twisted pair (STP) and Unshielded twisted pair (UTP)

Ans:--

Shielded Twisted Pair (STP) Cables

In a shielded twisted pair (STP), the wires are enclosed in a shield that functions as a grounding mechanism. Shielded twisted pair (STP) cable was originally designed by IBM for token ring networks that include two individual wires covered with a foil shielding. The shielding is done to provide greater protection from electromagnetic interference and radio frequency interference leaking into or out of the cable; thereby transporting data faster. However, STP cable is more expensive and difficult to install, compared with UTP.

Shielded twisted pair cable is available in three different configurations:

- Each pair of wire is individually shielded with foil
- There is a foil or braid shield inside the jacket covering all wires (as a group).
- There is a shield around each individual pair, as well as around the entire group of wires (referred to as double shield twisted pair).

STP cable has an impedance of 150 ohms, has a maximum length of 90 meters and is used primarily in networking environments with a high amount of EMI due to motors, air conditioners, power lines or other noisy electrical components. SPT is the default type of cabling for IBM token ring network.

Categories Of STP Cable

- IBM Type 1
- IBM Type 1A
- IBM Type 2A

- IBM Type 6A

BASIS OF COMPARISON	UTP	STP
Electromagnetic Interference	Electromagnetic interference and noise is more in UTP.	STP cable reduce electrical noise within the cable and from outside of the cable (e.g EMI, RFI).
Speed	It offers speed or throughput of about 10 to 1000Mbps.	It offers speed or throughput of about 10 to 100 Mbps.
Distance	It offers maximum cable length of about 100 meters.	It supports maximum segment of length about 100 meters.
Characteristic	Each of the 8 individual copper wires in UTP cable is covered by insulating material. In addition, wires in each pair are twisted around each other.	Each pair of wires in STP cable is wrapped in an overall metallic foil usually 150 Ohm cable.
Attenuation	In UTP, attenuation is high when compared to STP.	In STP, attenuation is low when compared to UTP.
Application	UTP is widely used for data transmission within short distance and is very popular for home network connecting.	STP is mainly used for connection of enterprises over a long distance.
Crosstalk Generation	In UTP the generation of crosstalk is high when compared to STP.	In STP, generation of crosstalk is quite less when compared to UTP.
Cost	The cost of UTP is less when compared to that of STP.	STP is costlier than UTP.
Grounding	In UTP grounding cable is not required.	In STP, grounding cable is required.

Unshielded Twisted Pair (UTP) Cables

In UTP cable, conductors which form a single circuit are twisted around each other in order to cancel out electromagnetic interference (EMI) from external sources. Unshielded means no additional shielding like meshes or aluminum foil which add bulk is used. UTP cables are often groups of twisted pairs grouped with color coded insulators, the number of which depends on the purpose. Alternatives to UTP cable include **coaxial cable and fiber optic cable.**

Inside a UTP cable, there are up to four twisted pairs of copper wires of copper wires, enclosed in a protective plastic cover, with the greater number of pairs corresponding to more

bandwidth. The two individual wires in a single pair are twisted around each other and then the pairs are twisted around each other, as well. This is usually done to reduce crosstalk and electromagnetic interference, each of which can degrade network performance. Each signal on twisted pair requires both wires. UTP is commonly used in telephone wiring and local area networks (LANs).

Categories Of UTP Cables

- **CAT3:** Not commonly used today but it can be deployed in phone lines. It supports 10 Mbps for up to 100 meters.
- **CAT 4:** It supports 16 Mbps for up to 100 meters. Commonly used in token ring networks.
- **CAT5:** It supports 100 Mbps for up to 100 meters. It typically made up of two twisted pairs and commonly used in Ethernet-based LANs.
- **CAT5e:** It supports 1 Gbps for up to 100 meters. It typically made up of two twisted pairs and commonly used in Ethernet-based LANs.
- **CAT6:** It supports 1 Gbps for up to 100 meters and 10 Gbps for up to 50 meters. This cable is typically used in data center networks and in Ethernet-based LANs.

Q 3:- What is difference between baseband and broadband transmission ?

Ans:--

Difference between Broadband and Baseband Transmission

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.**

Q 4:-- What is the difference between a hub, modem, router and a switch?
Ans:--

Hub

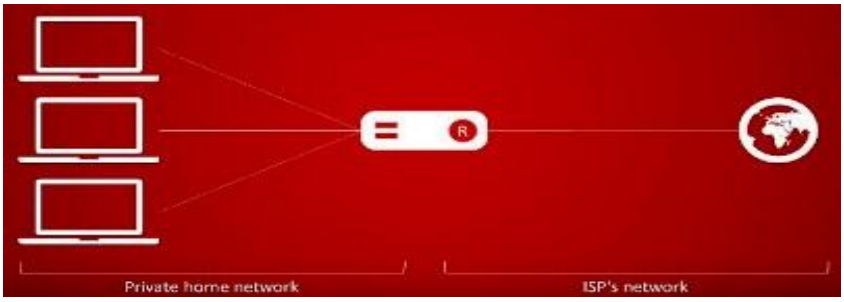
A hub is to sent out a message from one port to other ports. For example, if there are three computers of A, B, C, the message sent by a hub for computer A will also come to the other computers. But only computer A will respond and the response will also go out to every other port on the hub. Therefore,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

Switch

A switch is able to handle the data and knows the specific addresses to send the message. It can decide which computer is the message intended for and send the message directly to the right computer. The efficiency of switch has been greatly improved, thus providing a faster network speed.

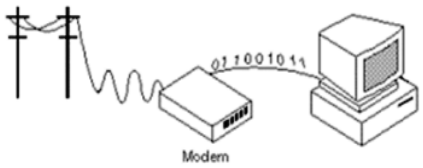
Router

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



Modem:

A modem is short for a **mo**dulator-**dem**odulator. Its function is to facilitate the transmission of data, by converting an **analogue signal to code** and **decoding digital information**. This means that it converts the telephone connection information into digital information for the computer to understand, and converts computer digits into analog waves so that it can be transmitted over telephone lines. It could be seen as the center for information collection from WAN, as it directly connects to the outside world.



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

Ans:--

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

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

Ans:-

A large percentage of a network is made up of hardware. Problems in these areas can range from malfunctioning hard drives, broken NICs, and even hardware startups.

Most common hardware related problems are PaBX, LAN Card, WLAN Card and Wi-Fi AP if it is wireless, Cables, Switches, Routers and Wireless Controllers.

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

Ans:-

An anti-virus program must be installed on all servers and workstations to ensure protection.

That’s because individual users can access any workstation and introduce a computer virus when plugging in their removable hard drives or flash drives.

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

Ans:-

Static IP:

A static IP address is simply an address that doesn't change. Once your device is assigned a static IP address, that number typically stays the same until the device is decommissioned or your network architecture changes. Static IP addresses generally are used by servers or other important equipment.

Static IP addresses are assigned by Internet Service Providers (ISPs). Your ISP may or may not allocate you a static IP address depending on the nature of your service agreement. We describe your options a little later, but for now assume that a static IP address adds to the cost of your ISP contract.

A static IP address may be IPv4 or IPv6; in this case the important quality is static. Some day, every bit of networked gear we have might have a unique static IPv6 address. We're not there yet. For now, we usually use static IPv4 addresses for permanent addresses.

Dynamic IP:-

Dynamic IP addresses are subject to change, sometimes at a moment's notice. Dynamic addresses are assigned, as needed, by Dynamic Host Configuration Protocol (DHCP) servers.

We use dynamic addresses because IPv4 doesn't provide enough static IP addresses to go around. So, for example, a hotel probably has a static IP address, but each individual device within its rooms would have a dynamic IP address.

On the internet, your home or office may be assigned a dynamic IP address by your ISP's DHCP server. Within your home or business network, the dynamic IP address for your devices -- whether they are personal computers, smartphones, streaming media devices, tablet, what have you -- are probably assigned by your network router. Dynamic IP is the standard used by and for consumer equipment.

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

Difference Between IPv4 and IPv6 Addresses

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	IPv6 provides interoperability and mobility capabilities which are embedded in network devices.

Basis for differences	IPv4	IPv6
	capabilities.	
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 auto configuration 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	Internet Protocol Security (IPSec) Concerning network security is mandatory
	optional	
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.

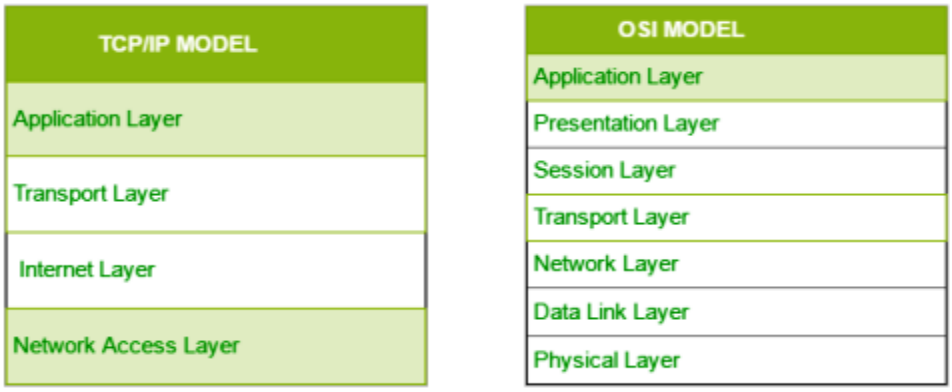
Q 9:- Discuss TCP/IP model in detail.
Ans:-

TCP/IP model:-

- The TCP/IP model was developed prior to the OSI model.

- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

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

1. Network Access Layer –

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.

We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

2. Internet Layer –

This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

1. **IP –** stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions: IPv4 and IPv6. IPv4 is the one that most of the websites are using

currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.

2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
3. **ARP –** stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

3. Host-to-Host/Transport Layer

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

1. **Transmission Control Protocol (TCP) –** It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
2. **User Datagram Protocol (UDP) –** On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

4. Application Layer –

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at **Protocols in Application Layer** for some information about these protocols. Protocols other than those present in the linked article are :

1. **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
2. • **SSH –** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
3. • **NTP –** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.

Q 10:- What is a Web Browser (Browser)? Give some example of browsers.

Ans:-

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.

5 Popular Browsers

1. Google Chrome

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

2. Apple Safari

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

3. Microsoft Internet Explorer and Edge

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

4. Mozilla Firefox

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

5. Opera

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

Q 11:- What is a search engine? Give example.

Ans:-

search engine means that it is **searching** for the information that the user needs. The knowledge is found and listed, on the World Wide Web. The provided Google, Yahoo and Bing are examples of search engines.

A **search engine** is **software** accessed on the Internet that searches a database of information according to the user's query. The engine provides a list of results that best match what the user is trying to find. Today, there are many different search engines available on the Internet, each with its own abilities and features. The first search engine ever developed is considered Archie, which was used to search for FTP files, and the first text-based search engine is considered Veronica.

Currently, the most popular and well-known **search engine** is **Google**.

Other popular **search engines** include **AOL, Ask.com, Baidu, Bing, DuckDuckGo,** and **Yahoo**.

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

Ans :-

Internet

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

Important Uses of Internet in Our Daily Life

The Internet has left a huge impact on our life. Since the internet was founded, it has brought **information and knowledge on our fingertips.** Internet has brought positivity in our life and has made it simple and easy. The Internet has left a huge impact in our daily life. Earlier we used to go to **libraries in search of information** on something but now we get that **information** in just a few clicks.

The internet provides us with useful data, information and knowledge that is useful for social, personal and economic development. It is up to us to utilize our time on the internet in a useful and productive way.

There are many uses of the internet. The most important use is that you can get **information and education** from the internet. It provides us with various sites and various blogs that give us informative content which helps us in studies. It helps people learn various things and people get knowledge which they implement in their daily life.

It helps people connect with each other socially. It helps us to talk to people that are from far off places like in different state or foreign country. There are various apps that help us to share messages, photos and videos with different people that are living near or far off places. The apps like **Whatsapp, Facebook, Twitter, Instagram, etc helps people share photos, videos and messages.** There is another feature of internet called video calling. This is a very useful feature of internet. Everyone should know that use of internet technology in our daily life. You can see and **talk to people that are living in far off places for free**. It helps people **download or stream movies and TV shows.**

World Wide Web, which is also known as a Web, is a collection of websites or web pages stored in web servers and connected to local computers through the internet. These websites contain text pages, digital images, audios, videos, etc. Users can access the content of these sites from any part of the world over the internet using their devices such as computers, laptops, cell phones, etc. The WWW, along with internet, enables the retrieval and display of text and media to your device.

The building blocks of the Web are web pages which are formatted in HTML and connected by links called "hypertext" or hyperlinks and accessed by HTTP. These links are electronic connections that link related pieces of information so that users can access the desired information quickly. Hypertext offers the advantage to select a word or phrase from text and thus to access other pages that provide additional information related to that word or phrase.
A web page is given an online address called a Uniform Resource Locator (URL). A particular collection of web pages that belong to a specific URL is called a website, e.g., www.facebook.com, www.google.com, etc. So, the World Wide Web is like a huge electronic book whose pages are stored on multiple servers across the world.

Small websites store all of their WebPages on a single server, but big websites or organizations place their WebPages on different servers in different countries so

that when users of a country search their site they could get the information quickly from the nearest server.
So, the web provides a communication platform for users to retrieve and exchange information over the internet. Unlike a book, where we move from one page to another in a sequence, on World Wide Web we follow a web of hypertext links to visit a web page and from that web page to move to other web pages. You need a browser, which is installed on your computer, to access the Web.

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

Ans:-

An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet. Internet service providers can be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned.

The **examples** of some internet service providers are **Hathway, BSNL, Tata teleservices, Verizon, Reliance Jio,** ACT Fibernet and many more working in India as well as worldwide. Internet service providers or ISPs are responsible for providing services for using the Internet.

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

Ans:-

Definition of Mac Address

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

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

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

Definition of IP Address

The address provided to a connection in a network is called IP (Internet Protocol) address. IP address does not uniquely identify a device on a network but, it specifies a particular connection in a network. IP address is provided by the administrator of the network or by Internet Service Provider (ISP).

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

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

Port?

To the uninitiated or the otherwise-gifted computer user, technical geek-speak can be rather frustrating and aggravating. When instructions are filled with such things as "port," "TCP," "UDP," and other acronyms or technical terminology, the user feels more isolated and rarely finds a solution or comprehension. Fortunately, comprehension is just moments away.

Picture a bay where there are lots of private boats are docked. The overall location is called a seaport, literally a port at or on the sea. Everyone wanting to dock there—requesting landing services—uses the same port. Seaports work with berth numbers assigned to individual boats. The port name and the berth number combine into the "who, what, and where" of boat identification.

In geek-speak, berth numbers on the Internet are Internet Protocol or IP addresses, a user's numerical identifier on the Internet. Depending on connection type and service provider, a user's IP address may or may not remain the same with each connection to or "docking" on the Internet.

A computer port is a type of electronic, software- or programming-related docking point through which information flows from a program on you

computer or to your computer from the Internet or another computer in a network. (A network, by the way, is a series of computers that are physically or electronically linked.)

In computer terms, a computer or a program connects to somewhere or something else on the Internet via a port. Port numbers and the user's IP address combine into the "who does what" information kept by every Internet Service Provider.

Ports are numbered for consistency and programming. The most commonly used and best known ports are those numbered 0 to 1023 dedicated for Internet use, but they can extend far higher for specialized purposes. Each port set or range is assigned specialized jobs or functions, and that's generally all they do. Usually, all identical system services or functions use the same port numbers on the receiving servers.

For example, all computers accessing or requesting Quote of the Day will always use port 17, because that port is officially reserved for that purpose, and only requests for that service use port 17. Outgoing information is channeled through a different or private port, keeping the "incoming line" open for others. Email received on a local computer generally uses a TCP port 25. File Transport Protocol or FTP uses port 21, to name only a few port assignments.

Q 15:- How do we view my Internet browser's history?

Ans :-

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