Assignment 2.

Q1. The different types of computer are:-

1. LAN:
    - Local Area Network is a group of computers connected to each other in small area such as building.
    - LAN is use 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.
2. PAN:
    - Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
    - PAN is used for connecting the computer devices of personal use is known as Personal Area Network.
    - Thomas Zimmerman was the first researcher scientist to bring the idea of PAN.
    - Personal computer device are used to develop the personal area network are the Laptop, mobile phones, Media player and PlayStation.
3. MAN:
    - A metropolitan area network is a network that covers a large geographical area by interconnecting a different LAN to form a larger network.
    - IN MAN various LANs are connected to each other through a telephone exchange line.
    - The most widely use protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
    - It has a higher range than Local Area Network.
4. WAN:
    - A Wide Area Network is a network that covers a larger Geographic area such as states or Countries.
    - A Wide Area Network is quite bigger network then 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.
    - The WAN is widely used in the field of Business, Government and education.

Q2.

- Shielded Twisted Pair (STP):
  Shielded Twisted Pair is a special kind of copper telephone and local area network (LAN) wiring used in some business installations .It adds an outer covering or shield that functions as a ground to ordinary twisted pair wiring.

  Twisted pair is the ordinary copper wire that connects many computer networks to the telephone company. To reduce cross-talk or electromagnetic induction between pairs of

wires, two insulate copper wires are twisted around each other. Each signal on twisted pair requires both wires. Unlike unshielded twisted pair (UTP) shielded twisted pair also encloses this wires in a shield and grounds them to further reduce electromagnetic and radio frequency interface. STP cables are more expensive and harder to install the UTP wiring.

Shielded twisted pairs come in a variety of cables categories. The most popular in use today are Cat5e, Cat6, Cat6a and Cat7. In electrically noisy business environment, shielded twisted pair uses RS-449, RJ-45, RS-232 and RJ-11 connectors to maximize the reduction of interference.

- Unshielded Twisted Pair (UTP):
  Unshielded Twisted pair (UTP) cable is a 100 ohm copper cable that consists of 2 to 1800 UTP surrounded by an outer jacket. They have no metallic shield. This make the cable small in diameter but unprotected against electrical interface. The twist helps to improve its immunity to electrical noise and EMI.

  Unshielded Twisted Pair (UTP) cables are found in many Ethernet networks and telephone systems. For indoor telephone applications, UTP is often grouped into sets of 25 pairs according to standard 25-pair colour code originally developed by AT&T corporation .A typical subset of these colours shows up in most UTP cables. The cables are typically made with copper wire measured at22 or 24 American Wire Gauge (AWG). With the coloured insulation typically made from an insulator such as polyethylene or FEP and the total package covered in a polyethylene jacket.

  UTP is also the most common cable used in computer networking. Modern Ethernet, the most common data networking standard ,can used UTP cable, CAT3, CAT4, CAT5, CAT5e, CAT6, etc. are some examples of Unshielded Twisted Pair cables.

Q3. Different between Baseband and Broadband are:-

Baseband	Broadband
• It refers to a communication channel in which information is carried in digital form. • Communication is bi-directional which means the same channel is used to transmit and receive signals. • Every device on a baseband system shares the same channel. • Baseband LANs are inexpensive and easier to install and maintain. • Baseband LANs have a limited distance reach is more than a couple miles.	• The signals are modulated as radio frequency analog waves that use different frequency ranges. • Communication is unidirectional meaning two different channels are needed in order to send and receive signals. • Multiple independent channels can carry analog or digital information through FDM. • Broadband system is generally more expensive because of additional hardware involved. • Broadband LANs span much longer distance and baseband.

Q4.

- Hub:
  A Hub is a device that allows several network devices to connect together to exchange data on a single network however, they have no management component Network hubs are also known as repeaters. They are less 'intelligent 'than switches, which forward data to the intended devices, hubs merely send the data packets to all its ports. So, as the name repeaters suggests. It only repeats the data from an incoming port to all the other devices; this leads to frequent collisions between packets.
- Modem:
  A Modem is short for a modulator-demodulator. Its function is to facilitate the transmission of data, by converting an analogue signal to code and decoding digital information.
- Router:
  A network router directs the data packets along networks. A router has a minimum of two networks, usually LANs or WANs or a LAN and its ISP. However, unlike a modem, it cannot work single standing, however is able to connect to multiple nodes.
- Switch:
  A switch is a network that connect network segments on a single network. It connects many devices together on the same network, sending data to device that's need to request it. A switch is able to improve the performance of a network by increasing network capacity.

Q5.

Yes, The MAC address also gets transferred. Because, every NIC card is associated with unique MAC address.

Q6.

When troubleshooting computer network problems, the most common hardware related problem can be: -

- Hard Drive malfunctioning
- PaBX
- LAN Card
- WLAN Card
- Cables
- Routers
- RAM needs to be upgraded
- VGA Cable is not properly connected
- Broken NICs

Q7.

In a network that Contains two servers and twenty workstations, the best place to install Anti-virus program is to install in all computes, systems or workstations. If we want to install only in one system, install in the main server.

Q8.

Static IP Address:
It is an IP address that computer or web server has and is identified by the rest of the internet or system and does not change at all, instead it remains the same.

Dynamic IP Address:
It is an IP Address that a computer or web server has and is identified by the rest of the internet or systems and this IP address does not remain the same, instead it changes over time.

Different between IPv4 and IPv6:

IPv4	IPv6
• ipv4 has 32-bit address length • It supports manual and DHCP configuration • In IPv4 end to end connection integrity is unachievable • it can generate $4{,}29\times10^{9}$ address space • The security feature is dependent on application • Address representation of IPv4 is in decimal • Fragmentation performed by sender and forwarding routers • In IPV4 packet flow identification is not available • In IPv4 checksum field is available. It has broadcast message Transmission Scheme. • IPv4 has a header of 20-60 bytes	• IPv6 has a 128-bit address length • It supports auto renumbering address configuration • In IPv6 end to end connection integrity is achievable • Address space of IPv6 is quite large it can produce 3.4×10^{38} address space • IPSEC is an inbuilt security feature in the IPv6 protocol • Address representation od IPv6 is in hexadecimal • In IPv6 fragmentation perform only by the sender • In IPv6 packet flow identification are available and uses the flow label field in the header • In IPv6 checksum field is not available. It has multicast and any cast message transmission scheme is available • In IPv6 has header of 40 bytes fixed

Q9.

TCP/IP Model is a four Layered suit of communication protocols. It was developed by the DoD (Department of Defence) In the 1960s. It is name 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.
It has 4 layers:

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:

   a) 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.
   b) ICMP-stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
   c) 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 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:

   a) 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.
   b) 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 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 needs 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.

Q10.

A web Browser is an Application Software for excessing the World Wide Web or a local website.
Examples of Web Browser:

- Google chrome
- Mozilla Firefox
- Opera
- Internet Explorer
- Uc Browser

Q11.

A search engine is a software system that is designed to carry out web searches.
Examples of Search Engine:

- Google
- Bing
- YouTube
- Yahoo
- Yippy

Q12.

Internet	WWW
• The Internet is a globally connected network system facilitating worldwide communication and access to data resources through a huge collection of personal, public, business, academic and government networks. It's Govern by agencies just like Internet Assigned Numbers Authority that establish universal protocols. • Internet is Infrastructure. • Internet is primarily hardware-based.	• World Wide Web by name Web, is leading information retrieval service of web. Online gives users access to a huge array of documents that are connected to every other by means of hypertext or hypermedia links i.e., hyperlinks, electronic connections that link related pieces of data so as to permit a user to quick access to them. Hypertext allows the user to pick a word or phrase from text and thereby access other documents that contain additional information concerning that word or phrase. • World Wide Web which is a collection of information which is accessed via the internet.

	• WWW is service on top of infrastructure.

Uses of internet in our daily life:

- We use internet for Shopping.
- We use internet for Education.
- We use internet for Playing Games.
- We use internet for Communication.
- We use internet for Digital Transaction.
- We use internet for Research and Development.
- We use internet for Entertainment.

Q13.

Internet Service Provider

- An internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet.

- Internet Services typically provided by ISPs include Internet Access, Internet transit, Domain name registration, web hosting, and Usenet Service.

Some examples of ISP in India are:

1. Airtel
2. Jio
3. BSNL
4. Vodafone
5. Vodafone Idea Ltd

Q14. The difference between MAC address, IP address and Port address are: -

Mac Address	IP Address	Port Address
1. MAC Address stands for Media Access Control Address. 2. MAC Address is a six-byte hexadecimal address 3. A device attached with MAC Address can retrieve by ARP protocol. 4. NIC Card's Manufacture provides the MAC Address.	1. IP Address stands for Internet Protocol Address. 2. IP Address is either a four-byte (IPv4) or a sixteen-byte (IPv6) address. 3. A device attached with IP Address can retrieve by RARP protocol. 4. Internet service provider provides IP address.	1. Port Number is use to identify process/service on the system. 2. The Port number is 16 bits numbers. 3. Port number is the address of the layer - 4 protocols. 4. Port number for application is provided by kernel of Operating System.

5. MAC Address is used to ensure the physical address of a computer	5. IP Address is the logical address of the computer.	5. Port numbers are logical interfaces used by communication protocols.

Q15. Steps to view my internet browser's history are:

1. Open chrome and click on the three dots on the right top Corner.
2. Click History on the dialog box, and then we view our Internet browser's history.

OR

1. Open chrome and click CTRL+H on the keyboard.
2. My recent Internet browser's history will appear.