**ASSIGNMENT- 3**

1. A network consists of two or more computer that are linked order to share resources (such as printer and CDs), exchange file, or allow electronic communication.
2. LAN – (local area network) is generally used to connect devices of a limited area such as a building, home, office, etc.

MAN – (metropolitan area network) is used to connect the devices among the city, a town, or any other small area.

WAN – (wide area network) is a type of network that covers a large geographical area.

1. The internet is a vast network that connects computers all over the world. Through the internet, people can share information and communication from anywhere with an internet connection.
2. A network topology is the physical and logical arrangement of nodes and connections in a network.
3. Twisted pair- twisted pair is one of the most commonly used types of network cable.

* Two types of twisted pair cable.

1. Unshielded twisted pair cable
2. Shielded twisted pair cable

Fiber optic cable – fiber optic cable are commonly used in a high-speed network connection, telecommunication system, and data centers.

* Three types of fiber optic cable.

1. Single-mode fiber
2. Multi-mode fiber
3. Plastic optical fiber
4. T-568A , the green wire connects to pin two and the orange wire connect to pin six.

T-568B, the orange wire connects to pin two and the green wire connect to pin six.

1. A fiber optical module is a component used in a fiber optical communication system to transmit or receiver optical signal.

* An fiber optical connector is a device used to link optical fiber, facilitating the efficient transmission of light signal.

1. A switch is a networking device that operates at the data link layer (Layer 2) or sometimes at the network layer (Layer 3) of the OSI (Open Systems Interconnection) model. It's used to connect multiple devices within a local area network (LAN) and selectively forward data packets between them.
2. A router is a device that connects two or more packet – switched networks or subnetworks.
3. A modem is a hardware which connects to a computer, broadband network or wireless router. Modem converts information between analogue and digital formats in real time making seamless two-way network communication.
4. Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. A protocol is a standardized set of rules for formatting and processing data. Protocols enable computers to communicate with one another.
5. Unicast - unicast is used for one-to-one communication. Ex- One to one.

Multicast - from one source to multiple destinations stating an interest in receiving the traffic. Ex – one to many.

Broadcast - from one source to all possible destinations. Ex one to all.

1. The OSI Model can be seen as a universal language for computer networking. It is based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last.
2. A port number is a way to identify a specific process to which an internet or other network message is to be forwarded when it arrives at a server.
3. TCP – (transmission control protocol)

* TCP is a connection based protocol.
* TCP is more reliable, it transfer data more slowly.

UDP – (user datagram protocol)

* UDP is connectionless.
* UDP is less reliable but works more quickly.

1. flow control is the process of managing the rate of data transmission between two nodes to prevent a fast sender from overwhelming a slow receiver.
2. TCP/IP model - The TCP/IP model comprises four layers: Network Interface, Internet, Transport, and Application.

* The TCP/IP model combines multiple functionalities into fewer layers, resulting in a more streamlined structure.
* The TCP/IP model is more rigid and less modular compared to the OSI model. However, it is well-suited for the internet's decentralized architecture and has been highly successful in practical implementations.

OSI model - The OSI model consists of seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

* Each layer in the OSI model performs specific functions related to data communication, and each layer communicates only with its adjacent layers.
* The OSI model provides a more flexible and modular approach to networking, with distinct layers allowing for easier integration of new protocols and technologies.

1. ARP broadcasts a request packet to all the machines on the LAN and asks if any of the machines are using that particular IP address.
2. A MAC address (media access control address) is a 12-digit hexadecimal number assigned to each device connected to the network.
3. An IP (Internet Protocol) address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.

* Different between ipv4 and ipv6 address
* IPV4 Address - IPv4 has a 32-bit address length.
* It Supports Manual and DHCP address configuration.
* In IPv4 end to end, connection integrity is Unachievable.
* IPV6 Address - IPv6 has a 128-bit address length
* It supports Auto and renumbering address configuration.
* In IPv6 end-to-end, connection integrity is Achievable.

Assigning multiple IPv4 addresses to a single network adapter on a PC is a common practice, especially in scenarios where a single network interface needs to serve multiple services or virtual hosts.

1. A firewall in networking is to secure the network from cyberattacks. For example, a firewall prevents malicious and unwanted content from entering your environment. As well, a firewall protects vulnerable systems and private data in the network from unauthorized access–such as hackers or insiders.
2. A wireless access point (WAP) is a networking device that allows wireless devices to connect to a wired network using Wi-Fi. WAPs are commonly used in home and business networks to extend wireless coverage and provide access to the network from multiple locations.

* A wireless extender, also known as a Wi-Fi range extender or repeater, is a device that extends the coverage of an existing wireless network. It receives the wireless signal from the main router or access point and retransmits it, effectively expanding the coverage area of the network.
* Physical Setup: Connect the wireless router to the modem provided by your internet service provider (ISP) using an Ethernet cable. Power on the router and modem.
* Access Router Settings: Open a web browser on a device connected to the router (either wired or wirelessly) and enter the router's IP address in the address bar. This IP address is typically printed on a label on the router or provided in the router's manual.
* Login to Router: Enter the router's username and password when prompted. The default login credentials are often found on the router itself or in the user manual. If you've changed the login credentials before, use those instead.
* Internet Setup: Follow the setup wizard or navigate to the internet setup section in the router's settings. Choose the appropriate connection type (DHCP, PPPoE, Static IP, etc.) based on your ISP's requirements and enter any necessary information provided by your ISP.
* Wireless Settings: Navigate to the wireless settings section in the router's settings. Set up the wireless network name (SSID) and password (Wi-Fi passphrase) for your wireless network. Choose a strong passphrase and encryption method (such as WPA2-PSK) to secure your wireless network.
* Wireless Security: Enable wireless security features such as WPA2 encryption and MAC address filtering to enhance the security of your wireless network. MAC address filtering allows you to specify which devices are allowed to connect to your network based on their MAC addresses.