**Assignment - 5**

**Module – 1**

**Network**

1. A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications.
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 communicate from anywhere with an Internet connection.
2. A network topology is the physical and logical arrangement of nodes and connections in a network. Nodes usually include devices such as switches, routers and software with switch and router features.
3. Twisted pair cable :- Twisted pair cables are made up of pairs of copper wires twisted around each other to reduce interference and crosstalk.

* UTP :- UTP cables are not shielded, making them more susceptible to electromagnetic interference.
* They are commonly used for Ethernet connections and other networking applications.
* STP :- STP cables have a shield around the pairs of wires or around the entire cable to reduce interference.
* STP cables are more expensive than UTP cables and are used in environments with high interference.
* Fiber optic cable :- Fiber optic cables use light signals to transmit data through strands of glass or plastic fibers.
* Single-Mode Fiber : - Single-mode fiber uses a single, narrow core to transmit light, allowing data to travel long distances without signal loss.
* It supports higher data rates and is commonly used in long-distance and high-bandwidth applications.
* Multi-Mode Fiber :- Multi-mode fiber has a larger core, allowing multiple light signals to travel through the fiber simultaneously.
* It is used for shorter distances and is generally more cost-effective than single-mode fiber.

1. 568 A :-

Pin 1: White/Green

Pin 2: Green

Pin 3: White/Orange

Pin 4: Blue

Pin 5: White/Blue

Pin 6: Orange

Pin 7: White/Brown

Pin 8: Brown

568 B : -

Pin 1: White/Orange

Pin 2: Orange

Pin 3: White/Green

Pin 4: Blue

Pin 5: White/Blue

Pin 6: Green

Pin 7: White/Brown

Pin 8: Brown

1. Fiber optics module :- A fiber optics module, also known as an optical transceiver, is a device that converts electrical signals into optical signals (for transmission) and optical signals into electrical signals (for reception)

* Fiber connector :- A fiber connector is a device that connects optical fibers together or to optical networking equipment.

1. A switch is a hardware component in network infrastructure that performs the switching process. The switch connects network devices, such as computers and servers, to one another. A switch enables multiple devices to share a network while preventing each device's traffic from interfering with other devices' traffic.
2. A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.
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. The full form of Modem or modem stands for modulator–demodulator.
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

* Protocol :- A protocol is a set of rules and conventions that define how data is transmitted, received, and processed in a network.

1. Unicast :- In unicast communication, data is sent from one source to one specific destination.

* It is a one-to-one communication method.
* Multicast :- In multicast communication, data is sent from one source to multiple destinations simultaneously.
* It is a one-to-many communication method.
* Multicast is more efficient than unicast when delivering data to multiple destinations because the data is sent once and distributed to all recipients interested in receiving it.
* Broadcast :- In broadcast communication, data is sent from one source to all possible destinations in a network segment.
* It is a one-to-all communication method.
* Broadcast is used when the same data needs to be sent to all devices on a network.

1. The open systems interconnection (OSI) model is a conceptual model created by the International Organization for Standardization which enables diverse communication systems to communicate using standard protocols.
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. The main difference between TCP (transmission control protocol) and UDP (user datagram protocol) is that TCP is a connection-based protocol and UDP is connectionless. While TCP is more reliable, it transfers data more slowly. UDP is less reliable but works more quickly.
4. 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.
5. Difference Between TCP/IP and OSI Model. TCP/IP is a practical model that addresses specific communication challenges and relies on standardized protocols. In contrast, OSI serves as a comprehensive, protocol-independent framework designed to encompass various network communication methods.
6. 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.
7. A MAC address (short for medium access control address) is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment.
8. IP address is a unique identifier assigned to devices on a network to enable them to communicate with each other.

* 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

1. The primary use of 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. This includes setting a unique name and password for your wireless network. Using your web browser, enter the router's default IP address into the address bar, then press Enter.

* Wireless access point : - A wireless access point (WAP) is a device that allows wireless-capable devices to connect to a wired network using Wi-Fi.
* Wireless extenders :- A wireless extender (also known as a range extender or repeater) is a device that amplifies and retransmits the existing Wi-Fi signal to extend its range.