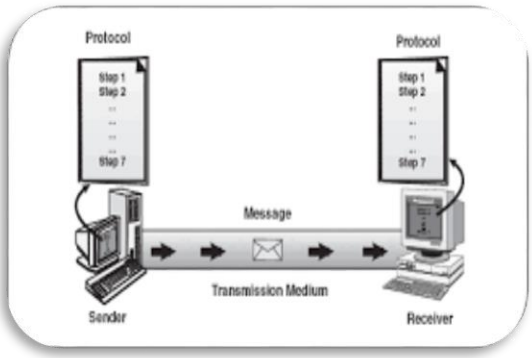
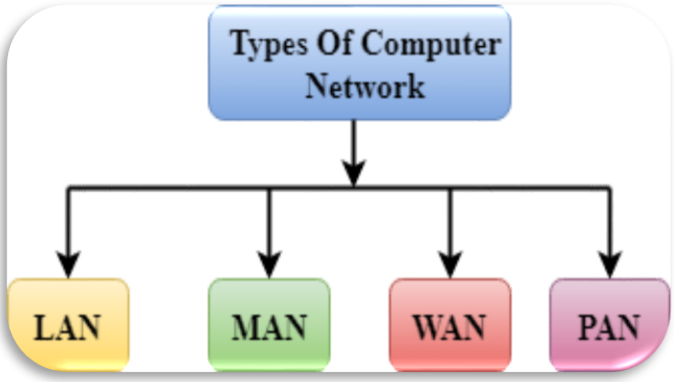
Unit #1

BASIC TERMINOLOGIES

Computer Network





UNIT #1: BASIC TERMINOLOGIES

Q1. DEFINE COMPUTER NETWORK. EXPLAIN ITS ADVANTAGES.

Ans: DEFINITION OF NETWORK:

A computer network is defined as the interconnection of two or more computers. It is done to enable the computers to communicate and share available resources.

APPLICATIONS:

i. Sharing of resources such as printers
ii. Sharing of expensive software's and database
iii. Communication from one computer to another computer
iv. Exchange of data and information among users via network
v. Sharing of information over geographically wide areas.

NETWORK BENEFITS:

The network provided to the users can be divided into two categories:

i. Sharing
ii. Connectivity

SHARING RESOURCES:

Types of resources are:

1. Hardware: A network allows users to share many hardware devices such as printers modems, fax machines, CD ROM, players, etc.

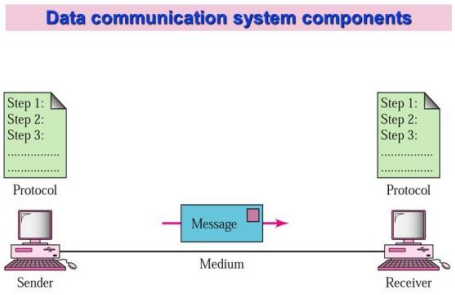
2. Software: Sharing software resources reduces the cost of software installation, saves spac on hard disk.

OTHER BENEFITS OF COMPUTER NETWORK:

- Increased speed
- Reduced cost
- Improved security
- Centralized software managements
- Electronic mail
- Flexible access

Q2. EXPLAIN BASIC DATA COMMUNICATION COMPONETS?

Ans: COMPONENTS OF DATA COMMUNICATION: A data communication system consist of five basic components.



1. Sender
2. Message
3. Medium
4. Protocol
5. Receiver

1. **SENDER:** Sender or transmitter is a device that sends the message. It may be a computer, workstation, telephone handset or video camera. Th transmitter converts the electrical signals into a form that is suitable for transmission through th physical channel or transmission media.

2. **MESSAGE:** Message is the data or information that is to be transmitted. Message can be number, video, text or any combination of these.
3. **MEDIUM:** Medium is the physical path that message uses to travel from source to destination. I can either guided or unguided media i,e it can be fiber optic cable, coaxial cables, twisted pai cable and even can be a wireless media.
4. **PROTOCOL:** A protocol is the set of rules that governs data communication. It represents a agreement between the communication devices. Without a protocol, two devices connected ma not able to communicate with each other.
5. **RECEIVER:** Receiver is the device which receives transmitted message. It can be a computer workstation, telephone handset or television set. There are five receiving steps in the process o communication i,e **Receive**, **Understand**, **Accept**, **Use** and give a **Feedback**. Without these step communication process may not be completed and successful.

Q3. EXPLAIN DIFFERENT TYPES OF COMPUTER NETWORK

Ans: Networks are divided into two main categories

- **i. Geographical Area Wise (Physical)**
  - a. LAN
  - b. MAN
  - c. WAN
- **ii. Virtual (Logical)**
  - a. VLANS
  - b. VPNS

1. LAN: LAN stands for Local Area Network. It is the most common type of a network. It covers small area within one room, office or a building. LAN is often used to share resources such as printers hard disks and programs. Each computer or device in a network is called a node. The nodes are usuall connected through wires. A LAN that uses no physical wires is called wireless LAN. LAN transmission speed is typically 10 MBPS to 1000 Mbps. LAN can transmit data in a limited distance Another name of LAN is Intranet

EXAMPLES:

I. In a computer lab, there are 40 computers connected through LAN. The students can shar software, files and data in the lab.

II. In Internet Club, many computers can be connected through LAN. These computers ca share single connection of the Internet.

BENEFITS / ADVANTAGES OF LAN: Following are the advantages of LAN

- Resource Sharing
- Communication
- Application Sharing
- Centralized Data
- Internet Access Sharing
- Data Security & Management

LIMITATIONS / DISADVANTAGES OF LAN

- Privacy Threat
- Expensive to Install
- Data Security Concerns

2. MAN: MAN stands for Metropolitan Area Network. This type of network covers an area of a city MAN is larger than LAN but smaller than WAN. It is usually connect two or more LAN's in a city o town. Another name of MAN is Extranet

EXAMPLES:

i. The network connecting different branches of a company in same city.
ii. The network connecting different campuses of a college in a city.
iii. Cable TV network in a city.

BENEFITS / ADVANTAGES OF MAN:

- MAN covers a larger than LAN
- It provides higher data speed than LAN

LIMITATIONS / DISADVANTAGES OF MAN

- It is more expensive than LAN
- It is difficult to maintain as compared to LAN

3. WAN: WAN stands for Wide Area Network. This type of network covers a large area. It connect computers and other devices in different cities and countries. WAN usually consists of several LAN' and MAN's connected together. Computers in a WAN are often connected through telephone lines They can be also connected through leased lines or satellites. The transmission rate of WAN i typically 56 Kbps to 50 Mbps.

EXAMPLES:

i. The network connecting the ATM's of a bank located in different cities.
ii. The network connecting NADRA offices in different cities of Pakistan.
iii. Internet connects millions of users all over world to share information

BENEFITS / ADVANTAGES OF WAN:

- Communication Facility
- Remote Data Entry
- Centralized Data
- Entertainment

LIMITATIONS / DISADVANTAGES OF WAN

- Hardware, Software and Setup Costs
- Hardware, Software and Management Costs
- Data Security Concerns
- Failure of Server

II. VIRTUAL (LOGICAL)

a. **VLANS**
b. **VPNS**

VLANS: A VLAN (Virtual Local Area Network) is a technology that allows you to create separate isolated networks within a single physical network. VLANs enable logical grouping of devices i different segments, even if they are on the same physical network, helping improve networ performance, security, and manageability. Here's how it works:

Key Features of VLANs:

Segmentation: VLANs divide a physical network into multiple logical sub-networks. Devices withi the same VLAN can communicate with each other as if they are on the same network, regardless o their physical location.

1. **Security:** VLANs can isolate traffic to prevent devices in one VLAN from accessing device in another VLAN, which improves security by limiting unauthorized access.

2. **Improved Network** Management: With VLANs, you can easily manage and configure group of devices as needed without physical changes to the network infrastructure. This i particularly useful in large organizations or data centers.
3. **Traffic Reduction**: VLANs reduce broadcast traffic. Devices in one VLAN won't receiv broadcast messages from another VLAN, improving overall network efficiency.

VLAN Example:

In an office network, you could set up:

- VLAN 10 for management.
- VLAN 20 for the accounting department.
- VLAN 30 for guests.

Each of these VLANs operates as a separate network, even though all devices may be connected t the same physical switch or router.

Communication Between VLANs:

Devices in different VLANs can communicate, but this requires a device (such as a router or a witch to route traffic between VLANs, a process known as Inter-VLAN Routing.

VLANs are widely used in enterprise networks, data centers, and virtualized environments to improv flexibility and control.

b. VPNS: A VPN (Virtual Private Network) is a technology that creates a secure, encrypte connection between your device and a remote server over the internet. It allows you to browse the wel privately and securely by masking your IP address and routing your internet traffic through a VPN server.

Key Features of VPNs:

1. Privacy: VPNs hide your real IP address and replace it with the IP address of the VPN server This makes it harder for websites, advertisers, or hackers to track your online activity.
2. Security: VPNs encrypt your internet traffic, which protects your data from being intercepte by hackers, especially on public Wi-Fi networks.
3. Bypassing Geo-Restrictions: VPNs allow you to access content that may be restricted base on your geographical location by connecting to servers in different countries.
4. Anonymity: Your online activities, like the websites you visit or files you download, ar shielded from prying eyes, offering an additional layer of anonymity.

How a VPN Works:

1. You connect to a VPN server.
2. The VPN server assigns you a new IP address and encrypts your data.
3. Your internet traffic is routed through the VPN server, making it appear as if you're browsing from a different location.

Example Use Cases:

- Secure Browsing: Protect your data while using public Wi-Fi networks.
- Bypass Censorship: Access websites or services that may be blocked in your country.
- Remote Access: Connect securely to your organization's internal network from anywhere i the world.

VPNs are widely used for both personal and business purposes to ensure secure and private onlin activities.

Q4. DIFFERENTIATE BETWEEN LAN, MAN & WAN

Ans: **DIFFERENCES BETWEEN LAN,MAN& WAN**

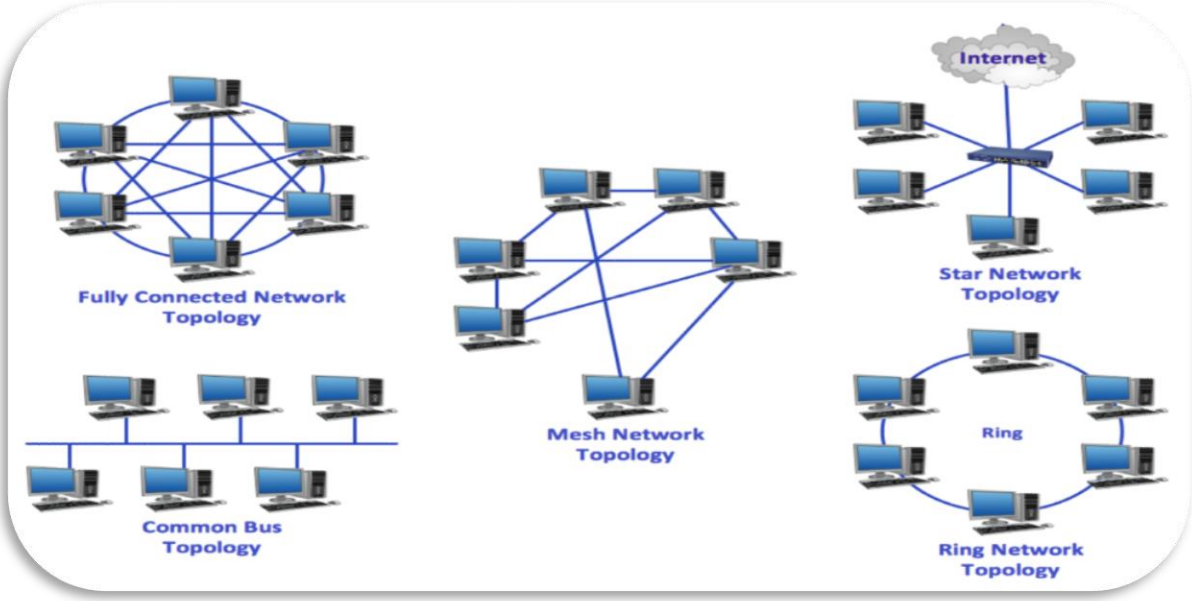
LAN	MAN	WAN
It is limited within a house, office or a school.	It is limited within a city.	It has a wide range such as a country or a continent.
Set up cost is low since less hardware is required.	Set up cost is higher than LAN.	It is the most expensive network to set up.
Bandwidth is low.	Bandwidth is higher than LAN.	It has the highest bandwidth among all the types of networks.
The range of LAN is very low (1 KM)	The range of MAN is higher than LAN but lower than WAN (100 KM)	WAN has the highest range (beyond 100 KM)
The Ethernet cable is used as the main communication medium.	Coaxial cables and microwave communication technologies are used	High-speed communication technologies like satellite, telephone lines are used.

UNIT #2: TOPOLOGIES

Unit #2

TOPOLOGIES

Computer Network

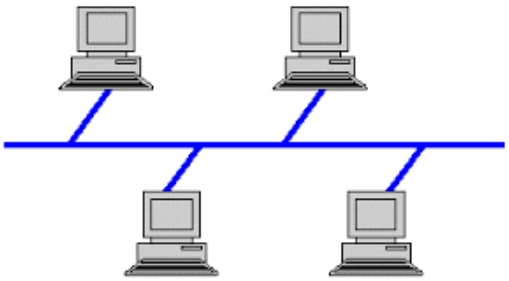


Q5. DEFINE NETWORK TOPOLOGIES & ITS TYPES.

Ans: NETWORK TOPOLOGY: Network topology refers to the physical layout and Connectivity of computers in a network. Network topologies are categorized into the following four basic types.

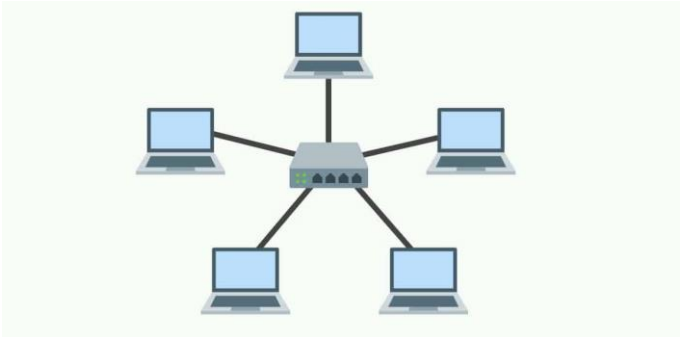
1. Bus topology
2. Star topology
3. Ring topology
4. Mesh topology

1. **BUS TOPOLOGY:** In the bus topology, each node (computer, server or peripheral device) i attached to a single common cable. This topology type is considered as a passive technolog because the computers on a bus just sit and listen. When they "hear" data on the wire that belongs to them, they accept that data. When they are ready to transmit, they make sure no one else on the bus is transmitting and then they send their packets of information on the network. Bus network typically uses coaxial networking cable hooked in to each computer using a T-Connector. Each end of the network is terminated using a terminator.



ADVANTAGES OF A BUS TOPOLOGY

- Bus topology costs very less
- Easy to connect a computer or peripheral to a linear bus
- Require less cable length than another topologies
- Easy to set-up and extend bus network
- Mostly used in small networks

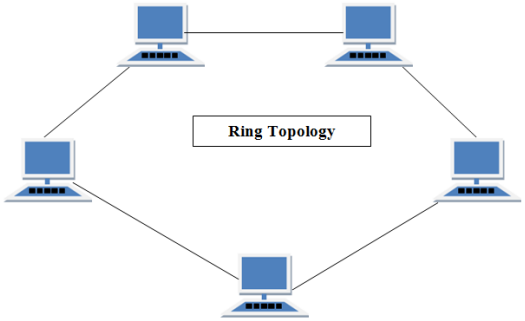


DISADVANTGES OF A BUS TOPOLOGY

- Entire network shuts down if there is break in the main cable
- There is a limit on central cable length and number of nodes that can be connected.
- Use of terminator is must
- Difficult to detect and troubleshoot fault at individual station
- Not suitable for networks with heavy traffic.

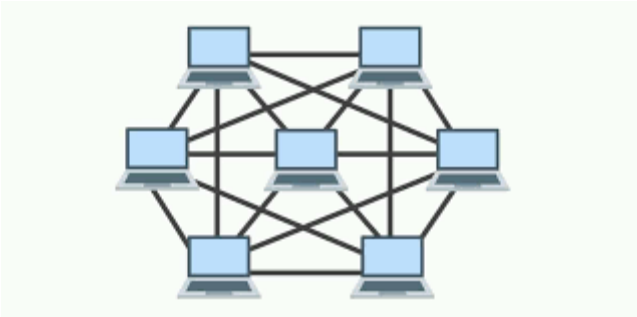
2. **STAR TOPOLOGY:** In a star topology all the nodes (server, workstations, peripheral devices o the network are connected directly to a centralized connectivity device called hub, switch or route Each computer is connected with its own cable to a port on he hub. Data on a star network passe through the hub, switch or router before continuing to its destination. The hub, switch, or route

manages and controls all functions of the network. It also acts as a repeater for the data flow. It use coaxial cable or fiber optic cable.



ADVANTAGES OF A STAR TOPOLOGY

- Centralized management. It helps in monitoring the network
- Easy to install and configure
- No disruptions to the network when connecting or removing devices
- Easy to detect faults and to remove parts
- Failure of one node or link doesn't affect the rest of network



DISADVANTAGES OF A STAR TOPOLOGY

- Requires more cable than a bus topology
- If he hub, switch, or concentrator fails, nodes attached become disable
- More expensive than linear bus topology because of the cost of the hubs.

3. **RING TOPOLOGY:** In a ring topology, every node is logically connected to two other precedin and succeeding nodes, forming a ring. Traffic flows through the entire ring until reaches th destination. Data packets travel in a single direction around the ring from one network device t the next. Each network device acts as a repeater, meaning it regenerates the signal the packets the receive and then send them on to the next computer in the ring.

ADVANTAGES OF RING TOPOLOGY

- Even when the load on the network increases, its performance is better than that of Bu topology.
- There is no need for network server to control the connectivity between workstations.
- Additional components do not affect the performance of network .
- Each computer has equal access to resources.

DISADVANTAGES OF RING TOPOLOGY

- Each packet of data must pass through all the computers between source and destination. Thi makes it slower than star topology.
- If one workstation or port goes down, the entire network gets affected.
- Network is highly dependent on the wire which connects different components.
- Ring topology can be difficult to troubleshoot
- Adding or removing components from this type of topology can disrupt the operation of the network.

4. **MESH TOPOLOGY:** In a mesh network topology, each of the network node, computer and othe devices, are interconnected with one another. Messages sent on a mesh network can take any o several possible paths source to destination. This type of topology is very inexpensive as there ar many redundant connections. It is commonly used in wireless network.

ADVANTAGES OF MESH TOPOLOGY

- Data can be transmitted from different devices simultaneously. This topology can withstand high traffic.
- Even if one of the components fails there is always an alternative link present. So data transfer doesn't get affected.
- Expansion and modification in topology can be done without disrupting other nodes.

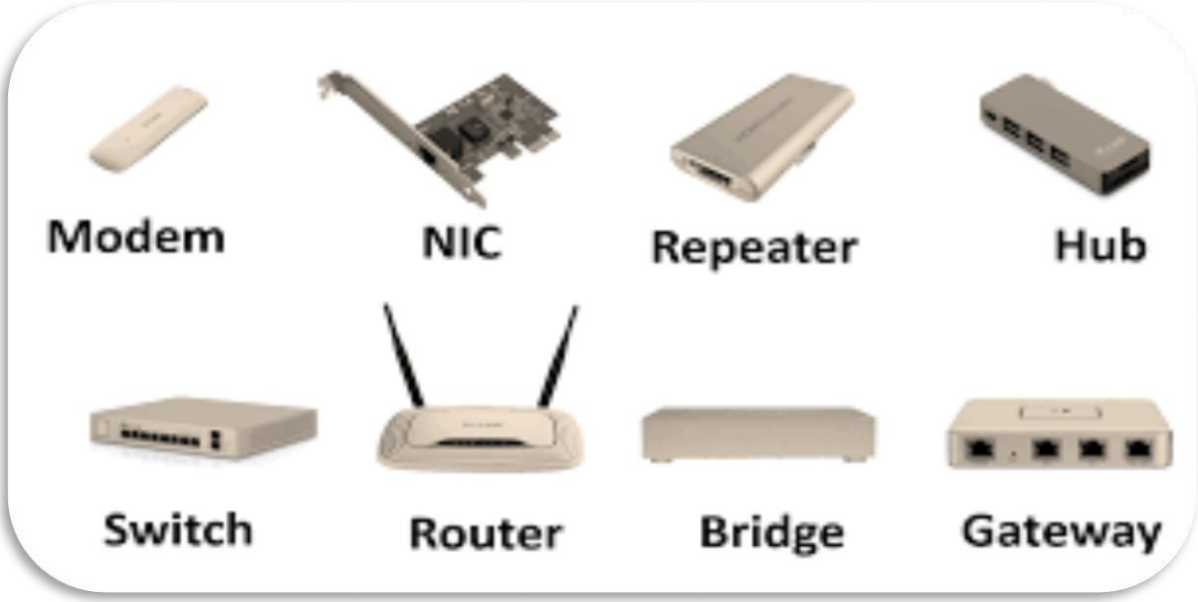
DISADVANTAGES OF MESH TOPOLOGY

- There are high chances of redundancy in many of the network connections.
- Overall cost of the network is too high as compared to other network topologies
- Set-up and maintenance of this topology is very difficult. Even administration of the network is challenging.

Unit #3

NETWORK DEVICES

Computer Network



Q6. WHAT IS NODE IN A COMPUTER NETWORK?

Ans: A node in networking is any device, such as a computer, router, switch, or printer, that is connected to a network and can send, receive, or process data. Nodes serve as communication points within network.

Q7. WHAT IS NIC (NETWORK INTERFACE CARD)?

Ans: NETWORK INTERFACE CARD (NIC): A network interface card (NIC) is a hardware component, typically a circuit board or chip, which is installed on a computer so that it can connect to a network. The NIC use the OSI model to send signals at the physical layer, transmit data packets at the network layer an operate as an interface at the TCP/IP layer. The network card operates as a middleman between computer and a data network.

Q8. HOW NIC WORKS?

Ans: When a user requests a web page, the computer will pass the request to the network card whic converts it into electrical impulses. Those impulses are received by a web server on the interne and responds by sending the web page back to the network card as electrical signals. The card get these signals and translates them into the data that the computer displays.

Q9. WHAT ARE THE TYPES OF NIC?

Ans: Following are the types of network interface card;

- **Wireless** - These are NICs that use an antenna to provide wireless reception through radi frequency waves. Wireless NICs are designed for Wi-Fi connection.
- **Wired** - These are NICs that have input jacks made for cables. The most popular wired LA technology is Ethernet.
- **USB** - These are NICs that provide network connections through a device plugged into th USB port.
- **Fiber optics** - These are expensive and more complex NICs that are used as a high-spee support system for network traffic handling on server computers. This could also b accomplished by combining multiple NICs.

Q10. WRITE DOWN THE COMPONENTS OF NETWORK INTERFACE CARDS?

Ans: Network interface card components include the following:

1. **Speed** - All NICs have a speed rating in terms of Mbps. The average Ethernet NICs are offere in 10 Mbps, 100 Mbps, 1000 Mbps and 1 Gbps varieties.
2. **Driver** - This is the required software that passes data between the computer's operatin system (OS) and the NIC. When a NIC is installed on a computer, th corresponding driver software is also downloaded. Drivers must stay updated and uncorrupte to ensure optimal performance from the NIC.
3. **MAC address** - Unique, unchangeable MAC addresses, also known as a physical networ address, are assigned to NICs that is used to deliver Ethernet packets to the computer.

Q11. What is MODEM?

Ans: MODEM: A **modem** stands for modulator-demodulator is a hardware device that convert data so that it can be transmitted from computer to computer over telephone wires. The goal is t produce a signal that can be transmitted easily and decoded to reproduce the original digital data.

A common type of modem is one that turns the digital data of a computer into modulated electrica signal for transmission over telephone lines and demodulated by another modem at the receiver sid to recover the digital data.
Modems are generally classified by the maximum amount of data they can send in a given unit o time, usually expressed in bits per second (symbol **bit(s)**, sometimes abbreviated "bps"), or bytes pe second (symbol **B(s)**).
Types of modem: There are two different types of modem:

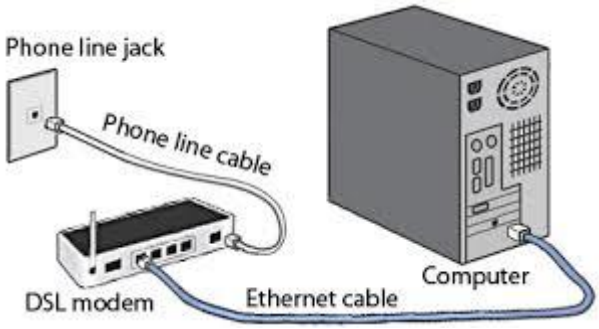
i. Ethernet modems that plug into the network card in the computer, and
ii. Wireless modems that connect to a computer using a wireless LAN (WLAN).

Q12. WHAT IS DSL?

Ans: DSL (Digital Subscriber Line) is the term for services that provide internet connections usin digital data connections between a modem and a phone line. What's great about DSL, is that eve when the phone line is in use, there is no interruption, and you can still experience a high speed interne connection even when you are making calls.

Q13. WHAT IS ADSL?

Ans: ADSL: stands for Asymmetric Digital Subscriber Line. This type of service means that the spee of data sent is known as upstream, and the data received is known as downstream, and the speeds ar not always guaranteed to be the same. They have different speeds that change from time to time. The word 'asymmetric' in ADSL actually means that the downstream is faster than the upstream. ADSL supports a downstream rate of 1.5 to 9 Mbps, and an upstream rate of 16 to 640 Kbps.



Q14. WHAT IS HUB?

Ans: HUB: When referring to a network, a hub is the most basic networking device that connects multiple computers or other network devices together. Unlike a network switch or router, a networ hub has no routing tables or intelligence on where to send information and broadcasts all network dat across each connection.

Most hubs can detect basic network errors such as collisions, but having all information broadcast t multiple ports can be a security risk and cause bottlenecks. In the past, network hubs were popula because they were cheaper than a switch or router. Today, switches do not cost much more than a hu and are a much better solution for any network. The hub contains multiple ports. When a packet arrive at one port, it is copied to the other ports so that all segments of the LAN can see all packets.

Q15. WHAT HUBS DO?

Ans: Hubs serve as a central connection for all of your network equipment and handles a data type known as frames. Frames carry your data. When a frame is received, it is amplified and then transmitted on to the port of the destination PC. In a hub, a frame is passed along o "broadcast" to every one of its ports. It doesn't matter that the frame is only destined for one port. Th

hub has no way of distinguishing which port a frame should be sent to. Passing it along to every por ensures that it will reach its intended destination. This places a lot of traffic on the network and ca lead to poor network response times.

Q16. WRITE DIFFERENT TYPES OF HUBS?

Ans: There are three types of hubs;

1. Passive,
2. Intelligent and
3. Switching Hubs

1. **PASSIVE HUBS:** A passive hub serves simply as a conduit for the data, enabling it to go fron one device (or segment) to another.
2. **INTELLIGENT HUBS** include additional features that enables an administrator to monitor th traffic passing through the hub and to configure each port in the hub. Intelligent hubs are als called *manageable hubs.*
3. **SWITCHING HUBS:** A third type of hub, called a *switching hub*, actually reads the destinatio address of each packet and then forwards the packet to the correct port.

Q17. WHAT IS A SWITCH?

Ans: A network switch (also called switching hub, bridging hub, officially MAC bridge is a compute networking device that connects devices together on a computer network by using packet switching t receive, process, and forward data to the destination device.

A network switch is a multiport network bridge that uses hardware addresses to process and forwar data at the data link layer (layer 2) of the OSI model. Switches for Ethernet are the most common forn of network switch.

Unlike less advanced hubs, which broadcast the same data out of each of its ports and let the device decide what data they need, a network switch forwards data only to the devices that need to receive i

HOW IT WORKS?

A switch is a device in a computer network that connects together other devices.

Multiple data cables are plugged into a switch to enable communication between different networke devices.

Switches manage the flow of data across a network by transmitting a received network packet only t the one or more devices for which the packet is intended.

Each networked device connected to a switch can be identified by its network address, allowing th switch to direct the flow of traffic maximizing the security and efficiency of the network.

A switch is more intelligent than an Ethernet hub, which simply retransmits packets out of every port of the hub except the port on which the packet was received, unable to distinguish different recipients, and achieving an overall lower network efficiency.

An Ethernet switch operates at the data link layer (layer 2) of the OSI model

The network switch plays an integral role in most modern Ethernet local area networks (LANs).

Mid-to-large sized LANs contain a number of linked managed switches.

Q18. WRITE DIFFRENCES BETWEEN HUB & SWITCH

BASIS	HUB	SWITCH
Definition	An electronic device that connects many network device together so that devices can exchange data	A network switch is a computer networking device that is used to connect many devices together on a computer network. A switch is considered more advanced than a hub because a switch will on send message to device that needs or request it
Layer	Physical layer. Hubs are classified as Layer 1 devices per the OSI model.	Data Link Layer. Network switches operate at Layer 2 of the OSI model.
Ports	4/12 ports	Switch is multi port Bridge. 24/48 ports
Used in (LAN, MAN, WAN)	LAN	LAN
Table	A network hub cannot learn or store MAC address.	Switches use content accessible memory CAM table
Transmission Mode	Half duplex	Half/Full duplex
Speed	10Mbps	10/100 Mbps, 1 Gbps
Address used for data transmission	Uses MAC address	Uses MAC address
Necessary for Internet Connection?	No.	No
Device Category	non intelligent device	Intelligent Device

WIRELESS DEVICES

Q19. WHAT IS ACCESS POINT (AP)?

Ans: In computer networking, a wireless access point, or more generally just access point, is a networking hardware device that allows a Wi-Fi device to connect to a wired network.
An access point (AP) is a device that creates a wireless local network, or WLAN in an office or large building. An access point connects to a wired router, switch, or hub via an Ethernet cable.
It allows a Wi-Fi device to connect to a wired network.

Q20. What is Wireless Modem?

Ans: A **wireless modem** is a device that allows computers, smartphones, or other devices to connect to the internet without the need for physical cables. It connects to the internet service provided by an Internet Service Provider (ISP) and transmits the signal wirelessly, typically via Wi-Fi, so that multiple devices can connect to the internet.

Q21. What is a wireless USB antenna?

Ans: A wireless USB antenna is a device that enhances the wireless connectivity of a computer or laptop by improving its ability to detect and connect to Wi-Fi networks. It plugs into the USB port of a device and typically consists of a small external antenna that can capture Wi-Fi signals more effectively than the device's built-in wireless receiver.

Q22.. WHAT IS A ROUTER?

Ans: **ROUTER:** A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet.

Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork until it reaches its destination node.

A router is connected to two or more data lines from different networks. When a data packet comes in on one of the lines, the router reads the network address information in the packet to determine the ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey.

The most familiar type of routers are home and small office routers that simply forward IP packets between the home computers and the Internet.

An example of a router would be the owner's cable or DSL router, which connects to the Internet through an Internet service provider (ISP).

Unit #4

TRANSMISSION MEDIA

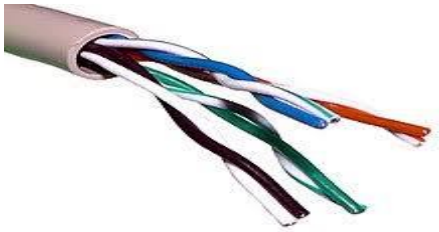
Computer Network

Q23. DEFINE COMMUNICATION MEDIA?

Ans: COMMUNICATION MEDIA / MEDIA: Communication media are the links that provid paths for communicating devices. It is an important part of a communication model. Transmissio medium should provide communication media with good quality. Communication media can b classified into two types;

a. Guided or Bounded Communication Media
b. Unguided or Unbounded Communication Media

a. GUIDED COMMUNICATION MEDIA



Guided media are the physical links in which signals are confined along a narrow path. These are also called bounded media. Three common types of bounded media are:

i. Twisted Pair Cable
ii. Coaxial Cable
iii. Fiber Optic Cable

i. TWISTED PAIR CABLE

Twisted Pair Cable is formed of two insulated copper wires twisted together. The wires ar twisted with each other to minimize interference from other twisted pairs cable. Twisted wire pair have bandwidths than coaxial cable or optical fiber cable. There are two types of twisted pair cables shielded (STP) and unshielded. (UTP)

UNSHIELDED TWISTED PAIR (UTP) CABLE:

UTP is the most commonly used networking wire. It is inexpensive, flexible and light., thu making it very easy to work with. The quality of UTP may vary from telephone-grade wire t extremely high-speed cable. The cable has four pairs of wires inside the jacket. UTP cable is furthe divided into 7 different categories;

CAT 1: (Category 1)

CAT 1 is typically used for telephone wire.
This type of wire is not capable of supporting computer network traffic and is not twisted.

CAT 2: (Category 2)

CAT2 are network wire specifications.
This type of wire can support computer network and telephone traffic.
CAT2 is used mostly for token ring networks, supporting speeds up to 4 Mbps.

CAT 3: (Category 3)

CAT3 cable is 4 pairs of twisted copper wires
CAT3 used for Token Ring networks
CAT 3 can provide support of a maximum 10Mbps.
Limit is 100 meters.

CAT 4 :(Category 4)

CAT4 cable is 4 pairs of twisted copper wires.
CAT4 used for Token Ring networks.
CAT4 pushed the limit up to 16Mbps.

Limit of 100 meters.
CAT5/CAT5e: Category 5/Category 5 enhanced)

The more popular CAT5 wire was later on replaced by the CAT5e
specification which provides improved crosstalk specification, allowing it to support speeds of up t
1Gbps. CAT5e is the most widely used cabling specification world-wide.

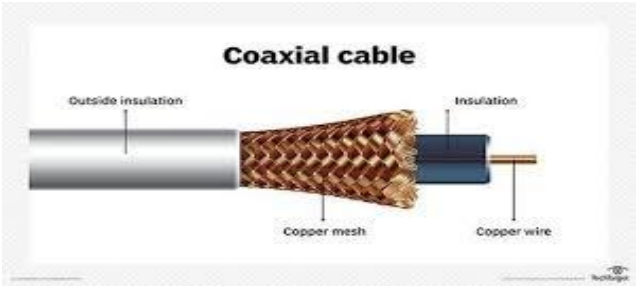
(CAT6: Category 6)

CAT6 wire was originally designed to support gigabit Ethernet.
It is similar to CAT5e wire, but contains a physical separator between the four pairs to further reduc
electromagnetic interference.
CAT6 is able to support speeds of 1Gbps for lengths of up to 100 meters, and 10Gbps is also supporte
for lengths of up to 55 meters.

SHIELDED TWISTED PAIR (STP) CABLE

The difference between UTP and STP is that the STP uses metallic shield wrapped to protect the wire from interference. Shielded cables can help to extend the maximum distance of the cables. Data rate of STP is from 16 to 155 Mbps. It cost more than UTP.

ii. COAXIAL CABLE



A Coaxial cable is a cable used in the transmission of video, communications, and audio. This cable has high bandwidths and greater transmission capacity. Most users relate to a coaxial or coax cable as a cable used to connect their TVs to a cable TV service. However, these cables are also used in networks and what allow a broadband cable Internet connection using a cable modem. The picture is an example of a coaxial cable.

TYPES OF COAXIAL CABLE:

- 10BASE2
- 10BASE 5
- 10BASE T,
- 100BASE FX)

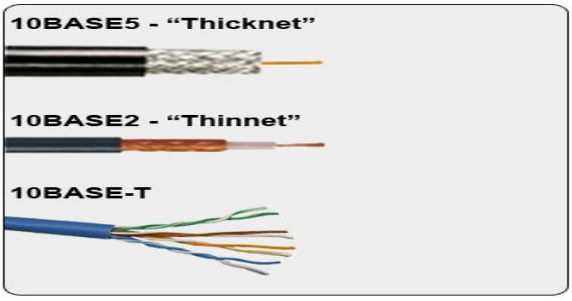
The number 10: At the front of each identifier, 10 denotes the standard data transfer speed over thes
media - ten megabits per second (10Mbps).
The word Base: Short for Baseband or Broadband
The segment type or segment length: This part of the identifier can be a digit or a letter:
Digit - shorthand for how long (in meters) a cable segment may be before attenuation sets in. Fo
example, a 10Base5 segment can be no more than 500 meters long.
Letter - identifies a specific physical type of cable. For example, the T at the end of 10BaseT stand
for twisted-pair.

10BASE2 One of several physical media specified by IEEE (Institute of Electrical and Electronic Engineers) use in an Ethernet local area network (LAN), consists of Thin wire coaxial cable with a maximum segment length of 185 meters.
Like other specified media, 10BASE-2 supports Ethernet's 10 Mbps data rate.
It is now obsolete

10BASE5

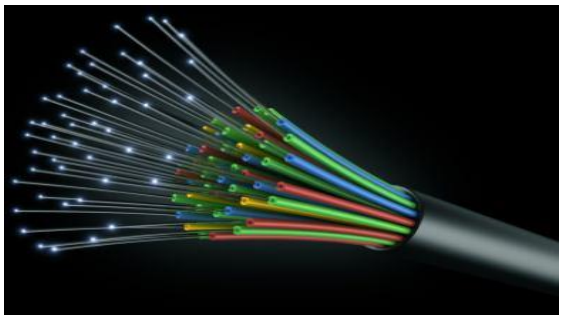
10BASE5 (also known as thick Ethernet or thicknet) was the first commercially available variant of Ethernet. 10BASE5 uses a thick and stiff coaxial cable up to 500 metres (1,600 ft) in length. Up to 100 stations can be connected to the cable 10 Mbit/s of bandwidth shared among them. The system is difficult to install and maintain. It is also now obsolete

10BASE-T, One of several physical media specified in the IEEE 802.3 standard for Ethernet local area networks (LANs)
It is ordinary telephone twisted pair wire.
10BASE-T supports Ethernet's 10 Mbps transmission speed.



iii. Fiber Optic Cable:

A fiber optic cable is a network cable that contains strands of glass fibers inside an insulated casing.
They're designed for long distance, very high-performance data networking and telecommunications.
Compared to wired cables, fiber optic cables provide higher bandwidth and can transmit data over longer distances. Fiber optic cables support much of the world's internet, cable television, and telephone systems.



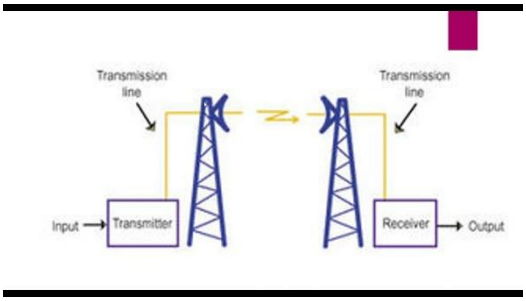
UNGUIDED OR UNBOUNDED MEDIA

It transports signals without using any physical conductor between the two devices communicating. Signals are normally broadcast through the air and thus are available to anyone who has the devic capable of receiving them.

The commonly used wireless transmission media are:

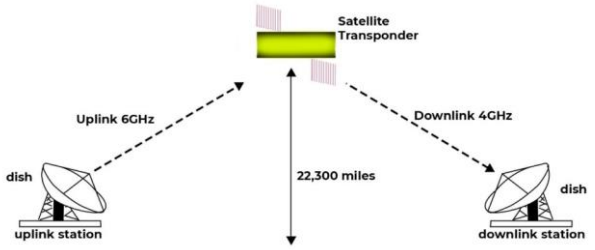
a. **Radio waves**
b. **Micro waves**
c. **Infrared waves**

RADIO WAVES: Radio waves distribute radio signals through the air over long distance such as between cities, regions, and countries and short distance such as within an office or home.
Radio waves are normally multi-directional. When an antenna transmits radio waves they are propagated in all directions. The multi-directional characteristics of radio waves mak them useful for multicasting, (One sender but many receivers). It has frequency between 10 KHz to GHz AM and FM radio stations, cordless phones and television are example of multicasting.



MICRO WAVES: Micro wave is a wireless transmission technology that travels at high frequency than radio waves. Micro wave transmission requires the sender to be in line of sight of the receiver. Electronic waves with frequencies between 1 GHz to 300 GHz are called microwaves. Microwaves are used to transmit wireless signals across a few miles. Unlike radio waves microwaves are unidirectional, in which the sending and receiving antennas need to be aligned Microwaves stations or antennas are usually installed on the high towers or buildings. Microwave propagation is line-of-sight. Mobile telephone companies use microwave technology.

SATELLITE MICROWAVE: For long distance communication Satellite Microwave technology is used. A satellite is a device that receives microwave signals from an earth-based station , amplifies the signals, and broadcast the signals back over a wide area to any number of earth-based stations. Satellite microwave transmission is used to transmit signals throughout the world. Satellites have many purposes including dat communications, scientific applications and weather analysis.



There are three types of satellites;

Geostationary Earth Orbit (GEO)	22,000 miles from the earth
Medium Earth Orbit (MEO)	1243 miles from the earth
Low Earth Orbit (LEO)	1200 miles from the earth

INFRARED: It is a short-distance wireless transmission medium. Using infrared light waves. Infrared frequencies are just below visible light. These are high speed data transmission
Examples: Remote control for a TV
Can be affected by objects obstructing sender or receiver.
Used in devices such as the mouse, wireless keyboard and printers.

With infrared computers can transfer files and other digital data bi-directionally.

WI-FI (WIRELESS FIDELITY): Wi-Fi is a wireless technology used to connect computers, tablets, smartphones and other devices to the internet. Wi-Fi is the radio signal sent from a wireless router to a nearby device, which translates the signal into data you can see and use.

BLUETOOTH: Bluetooth is a short-range wireless technology standard that is used for exchanging data between fixed and mobile devices over short distances. In the most widely used mode, transmission power is limited to 2.5 milliwatts, giving it a very short range of up to 10 metres.

Q24. WHAT IS A CONNECTOR AND ITS TYPES?

Ans: CONNECTOR: A device that terminates a segment of cabling or provides a point of entry fo networking devices such as computers, hubs, and routers.

TYPES of CONNECTORS: There are three types of connectors:

i. RJ45 Connector
ii. RJ11 Connector
iii. BNC Connector

1. RJ45 CONNECTOR: RJ45 is a type of connector commonly used for Ethernet networking. It looks similar to a telephone jack, but is slightly wider.

Ethernet cables have an RJ45 connector on each end. Ethernet cables are sometimes also called RJ45 cables. The "RJ" in RJ45 stands for "registered jack," since i is a standardized networking interface. The "45" simply refers to the number of the interface standard Each RJ45 connector has eight pins, which means an RJ45 cable contains eight separate wires.

II. RJ11 CONNECTOR: RJ-11. (Registered Jack-11) A telephone interface that uses a cable of twisted wire pairs and a modular jack with two, four or six contacts. RJ-11 is the common connector for plugging a telephone into the wall and the handset into the telephone.

DIFFERENCE BETWEEN RJ11 AND RJ45:

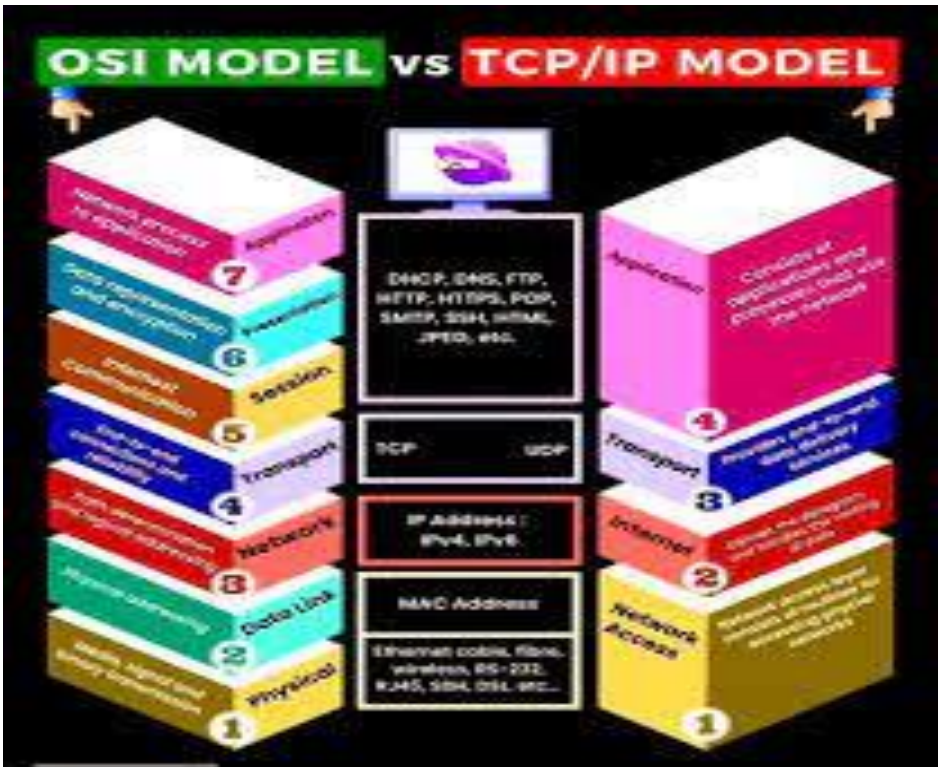
RJ45 jacks are used in networking, where you connect computers or other network elements to each other. RJ11 is the cable connector that is being used in telephone sets.

III. BNC: Short for Bayonet Neill Concelman connector, (sometimes erroneously called a British Naval Connector or Bayonet Nut Connector, A type of connector used with coaxial cables used with the 10Base-2 Ethernet system.

Unit #5

HOW NETWORK TRANSFER DATE (NETWORK MODELS)

Computer Network



Q25. WHAT IS OSI MODEL?

Ans: OPEN SYSTEM INTERCONNECTION (OSI) MODEL: OSI model is developed by International Standards Organization (OSI). An OSI model covers all aspects of Networl Communication. It is an Open System because it allows two different systems to communicate ove their primary network.

The OSI model deals with the following:

- How a device on a network translates its data and how it knows when and where to send.
- How a node on a network receives its data and how it know where to search.
- How nodes using different languages communicate with each other.
- How nodes on a network are physically connected to each other.
- How different protocols work with devices on a network to arrange data.

OSI MODEL LAYERS: The OSI Model has following seven layers.

1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

Q26. EXPLAIN DIFFERENT LAYERS OF OSI MODEL?

1. **PHYSICAL LAYER:** The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium

FUNCTIONS:

- Define physical means of sending data over network devices.
- Defines the characteristics of the physical medium
- Interfaces between network medium and devices.
- Conversion of the raw bit stream into electrical impulse.
- Manages the encoding and decoding of data.

2. **DATA LINK LAYER:** The data link layer provides reliable transmission of data across a physica link. Data link is used by hubs and switches for their operations.

FUNCTIONS:

- Physical addressing
- Error notification
- Ordered delivery of frames
- Network topology
- Flow control

3. **NETWORK LAYER:** This layer allows the data called packets or datagram to go from on physical network to another. This layer also has its own addressing scheme so that devices ca communicate with other devices across multiple networks. This layer is also responsible for pat determination.

FUNCTIONS:

- Translates logical addresses or names into physical addresses.
- Management of connectivity and routing between hosts or networks
- Determines how data are transferred between network devices
- Routes packets according to unique network device addresses.

4. **TRANSPORT LAYER:** It handles the transparent transport of data segments between networ devices. It is responsible for flow control, error control, data segmentation and communicatio reliability.

FUNCTIONS:

- Accepts a message from the (session) layer above it, splits the message into smaller units, an passes the smaller units down to the network layer. The transport layer at the destination statio reassembles the message.
- Manage reliable end-to-end message delivery with acknowledgments in network.
- Provides connectionless oriented packet delivery.

5. **SESSION LAYER:** The session layer sets up, coordinates and terminates conversations exchanges and dialogues between the application running on different stations.

FUNCTIONS:

- Session establishments, maintenance and termination.
- Session support: performs the functions that allow these processes to communicate over th network, performing security, name recognition, logging.

6. **PRESENTATION LAYER: The presentation converts incoming and outgoing data fron one** presentation format to another. The presentation layer is sometimes called as the syntax layer It can be viewed as the translator for the network.

FUNCTIONS:

- Character code translation: for example ASCII to EBCDIC
- Data compression
- Data encryption
- Architecture-independent data transfer format

7. **APPLICATION LAYER:** The application layer serves as the user interface for users an application processes to access network services. The application layer is responsible fo displaying data and images to the user in a human-recognizable format.

FUNCTIONS:

- Resource sharing
- Remote file access
- Network management
- Directory services
- Electronic messaging (such as e-mail)

Q27. EXPLAIN TCP/IP MODEL?

Ans: It loosely defines a four-layer model, with the layers having names, not numbers, as follows:

1. **The Application layer**: is the scope within which applications create user data an communicate this data to other applications on another or the same host. The applications, o processes, make use of the services provided by the underlying, lower layers, especially th Transport Layer which provides reliable or unreliable pipes to other processes. Th communications partners are characterized by the application architecture, such as the client server model and peer-to-peer networking. This is the layer in which all higher level protocols such as SMTP, FTP, SSH, HTTP, operate. Processes are addressed via ports which essentiall represent services.
2. **The Transport Layer**: performs host-to-host communications on either the same or differen hosts and on either the local network or remote networks separated by routers. It provides channel for the communication needs of applications. UDP is the basic transport layer protocol

providing an unreliable datagram service. The Transmission Control Protocol provides flow control, connection establishment, and reliable transmission of data.

3. **The Internet layer**: has the task of exchanging datagrams across network boundaries. I provides a uniform networking interface that hides the actual topology (layout) of th underlying network connections. It is therefore also referred to as the layer that establishe internetworking; indeed, it defines and establishes the Internet. This layer defines th addressing and routing structures used for the TCP/IP protocol suite. The primary protocol i this scope is the Internet Protocol, which defines IP addresses. Its function in routing is t transport datagrams to the next IP router that has the connectivity to a network closer to th final data destination.
4. **The Link layer**: defines the networking methods within the scope of the local network link o which hosts communicate without intervening routers. This layer includes the protocols use to describe the local network topology and the interfaces needed to effect transmission o Internet layer datagrams to next-neighbor hosts.

Unit #6

IP ADDRESSES

Computer Network

Q28. EXPLAIN IP ADDRESSING

Ans: IP ADDRESSING: An Internet Protocol address (IP Address) is a number that is used to identif a device on the network. Each device on a network must have a unique IP address to communicat with other network devices. A host (usually a computer) is a device that sends or receives informatio on the network.

Q29. WHAT IS IPv4?

Ans: IPv4 was the first version of IP. It was deployed for production in the ARPANET in 1983. Toda it is most widely used IP version. It is used to identify devices on a network using an addressin system. The IPv4 uses a 32-bit address scheme allowing to store 2^32 addresses which is more than billion addresses. Till date, it is considered the primary Internet Protocol and carries 94% of Interne traffic.

Q30. WHAT IS IPv6?

Ans: It is the most recent version of the Internet Protocol. Internet Engineer Taskforce initiated it i early 1994. The design and development of that suite is now called IPv6. This new IP address versio is being deployed to fulfill the need for more Internet addresses. It was aimed to resolve issues whic are associated with IPv4. With 128-bit address space, it allows 340 undecillion unique address space IPv6 also called IPng (Internet Protocol next generation).

Q31. DIFFERENTIATE BETWEEN IPv4 and IPv6.

Ans:

BASIS FOR DIFFERENCES	**IPV4**	**IPV6**
Size of IP address	32-Bit IP Address.	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 classes	IPv4 offers five different classes of IP Address. Class A to E.	lPv6 allows storing an unlimited number of IP Address.
Type of Addresses	Unicast, broadcast, and multicast.	Unicast, multicast, and anycast.
Example	12.244.233.165	2001:0db8:0000:0000:0000:ff00:0042:7879

Q32. EXPLAIN CLASSES OF IPv4 Addresses
Ans: Classes of IPv4: IPv4 has 5 different classes;

CLASS A: Class A is used for the large networks and is implemented by large companies with many network devices. Binary address for the class A starts with 0. Its range is between 1 to 126. Its network part consists of 1 octet and Host part consists of 3 octets.
Example: An example of the class A is 100.10.11.1

CLASS B: Class B addresses scheme is used for the medium sized networks. The binary address for the class B starts with 10. The range of the IP address in the class B is between 128 to 191. Its Network part consists of 2 octets and Host part also consists of 2 octets.
Example: An example of the class B is 150.101.110.120

CLASS C: Class C is used for small networks. The binary address for the class C starts with 110. The range addresses in the class C is between 192 to 223. Its network part consists of 3 octets and Host part consists of 1 octect.
Example: An example of the Class C is 210.190.100.150

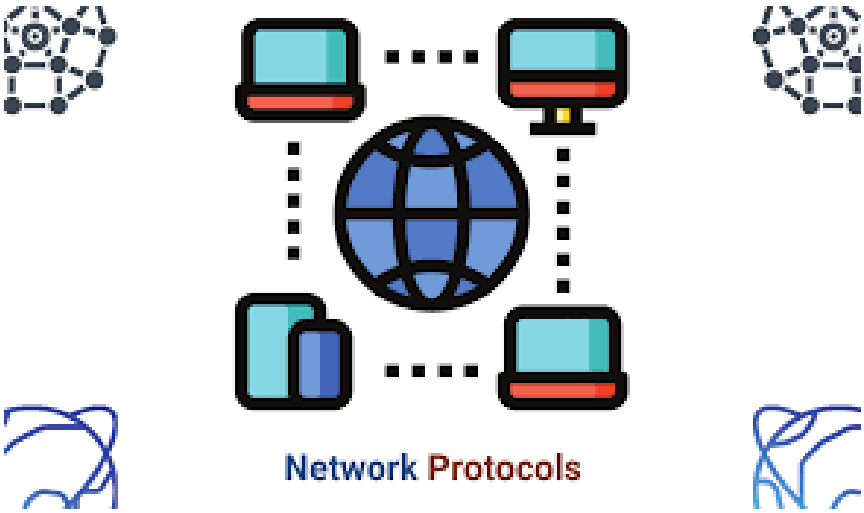
CLASS D: Class D is for special use for multicasting. The binary addresses for the class D starts with 1110. The IP address ranges from 224 to 239.
Example: An example of Class D is 230.150.110.11

CLASS E: Class E is under experimental research. The binary address can start with 1111 and the IP address ranges from 240 to 255.
Example: An example of class E IP address is 245.101.110.110

Unit #7

PROTOCOLS

Computer Network



Q33. WHAT IS PROTOCOL?

Ans: PROTOCOL: A protocol is a set of rules that governs the communications between computer on a network. It is a digital language through which we communicate with others on the Internet. By adopting these rules, two devices can communicate with each other and can interchange information We can't even think of using the Internet without Protocols.

One of the most common and known protocol example is HTTP, that is used over the world wide web There are different protocols used in internet that are

- TCP/IP (Transmission Control Protocol/Internet Protocol)
- DNS (Domain Name System)
- FTP (File Transfer Protocol)

Q34. WHAT ARE DIFFERENT TYPES OF PROTOCOLS?

Ans: Types of protocols: following are the different types of protocols;

1. Network Protocols

- **Internet Protocol (IP):** Manages addressing and routing of data packets across the internet.
- **Transmission Control Protocol (TCP):** Ensures reliable, ordered, and error-checked delivery of a stream of data between applications.
- **User Datagram Protocol (UDP):** A simpler, connectionless protocol that allows fast transmission without error-checking.

2. Data Transfer Protocols

- **File Transfer Protocol (FTP):** Used for transferring files over a network.
- **Hypertext Transfer Protocol (HTTP):** Governs the communication between web browsers and web servers.
- **HTTP Secure (HTTPS):** HTTP with encryption (SSL/TLS) for secure web browsing.
- **Simple Mail Transfer Protocol (SMTP):** Protocol for sending email messages.
- **Post Office Protocol 3 (POP3):** Allows retrieval of emails from a server, usually deleting them afterward.

3. Security Protocols

- **Secure Sockets Layer (SSL)/Transport Layer Security (TLS):** Protocols that provide encrypted communication over networks.

4. Wireless and Mobile Protocols

- **Wi-Fi (IEEE 802.11):** A family of protocols for wireless local area networking.
- **Bluetooth:** A protocol for short-range wireless data exchange.

Q35. WHAT IS ROUTING PROTOCOL?

Ans: A routed protocol is used to deliver application traffic. It provides appropriate addressing information in its internet layer or network layer to allow a packet to be forwarded from one network to another. Examples of routed protocols are the Internet Protocol (IP) and Internetwork Packet Exchange (IPX).

Q36. WHAT IS ROUTED PROTOCOL:

Ans: A routed protocol is a type of protocol used in network communications that carries user data—such as files, emails, and web pages—across different networks. Routed protocols are responsible for encapsulating data and providing addressing information so that data packets can be sent from one network to another, effectively enabling communication across various network boundaries.

E X E R C I S E

OBJECTIVE TYPE QUESTIONS

1. STATE TRUE OR FALSE

i. In the data communication model, the 'Sender' is the device that receives the message. (T/F

ii. Protocols are not necessary for data communication. (T/F)

iii. The receiver decodes the message during the data communication process. (T/F)

iv. A LAN (Local Area Network) is typically used to connect devices over a large geographical area. (T/F

v. WAN (Wide Area Network) covers large geographical distances, often spanning cities, countries, or continents. (T/F)

vi. In a star topology, all nodes are connected to a central hub. (T/F)

vii. A mesh topology provides redundancy by connecting each node to every other node. (T/F)

viii. In a ring topology, data travels in both directions simultaneously. (T/F)

ix. A bus topology requires terminators at both ends of the network. (T/F)

x. In a bus topology, if one node fails, it does not affect the rest of the network. (T/F)

xi. A router connects different networks and forwards data between them. (T/F)

xii. A switch operates at the physical layer of the OSI model. (T/F)

xiii. An access point provides a wired connection to devices on a network. (T/F)

xiv. A modem converts digital signals into analog signals and vice versa. (T/F)

xv. A router works at the data link layer of the OSI model. (T/F)

2. CHOOSE THE CORRECT ANSWER

1. **Which of the following is a component of the data communication model?**

   a) Protocols b) Sender c) Receiver d) All of the above

2. **Which term refers to the physical path between the sender and receiver in a dat communication system?**

   a) Protocol b) Transmission medium c) Encoder d) Message

3. **What is the function of a 'protocol' in data communication?**

   a) To encrypt the message b) To establish rules for data transmission

   c) To decode the message d) To amplify the signal

4. Which type of network typically covers a small geographic area like a building or campus?

a) LAN b) WAN c) MAN d) PAN

5. What type of network is the internet classified as?

a) LAN b) PAN c) WAN d) MAN

6. In which topology are all devices connected to a central device like a hub or switch?

a) Mesh b) Ring c) Star d) Bus

7. What is the main disadvantage of a bus topology?

a) Difficult to expand b) Expensive to implement

c) High risk of failure d) Complex configuration

8. In which topology does data travel in a circular path, passing through each node before reaching its destination?

a) Bus b) Star c) Mesh d) Ring

9. In which topology are terminators used to prevent signal bounce?

a) Mesh b) Bus c) Star d) Ring

10. Which of the following topologies is most commonly used in modern Ethernet networks?

a) Ring b) Bus c) Star d) Mesh

11. Which device connects different networks and determines the best path for data to travel?

a) Hub b) Switch c) Router d) Access point

12. Which device operates at the Data Link layer of the OSI model and forwards data based on MAC addresses?

a) Firewall b) Switch c) Router d) Modem

13. Which device provides a wireless connection to devices within a network?

a) Modem b) Access point c) Switch d) Router

14. Which network device broadcasts incoming data to all ports, without filtering?

a) Router b) Switch c) Hub d) Firewall

15. Which of the following converts digital signals into analog signals for data transmission over phone lines?

a) Router b) Modem c) Switch d)Hub

3. FILL IN THE BLANKS

1. The primary components of a data communication system are the sender, the _____, the message, the transmission medium, and the protocol.
2. In the data communication process, the device that initiates the message is called the _____
3. _____ is the set of rules that governs data communication between devices.
4. A _____ network is used to connect devices within a small geographical area such as building or office.
5. The internet is an example of a _____, which connects networks over large distances.
6. In a _____ topology, all devices are connected to a central hub or switch.
7. In a _____ topology, every node is connected to every other node, providing high redundancy.
8. A _____ topology uses a single central cable to which all network devices are connected
9. The main disadvantage of a _____ topology is that if the central hub fails, the entire network goes down.
10. The _____ topology uses terminators at both ends of the backbone cable to prevent signa bounce.
11. A _____ connects different networks and forwards data packets between them.
12. A _____ is a device that connects multiple devices in a network and forwards data base on MAC addresses.
13. A _____ broadcasts data to all devices connected to it, regardless of the intende recipient.
14. A _____ converts digital signals to analog signals and vice versa, allowing interne access over telephone lines.
15. An _____ is a network device that provides wireless access to a wired network.