V2V EDTECH LLP

Online Coaching at an Affordable Price.

OUR SERVICES:

- Diploma in All Branches, All Subjects
- Degree in All Branches, All Subjects
- BSCIT / CS
- Professional Courses

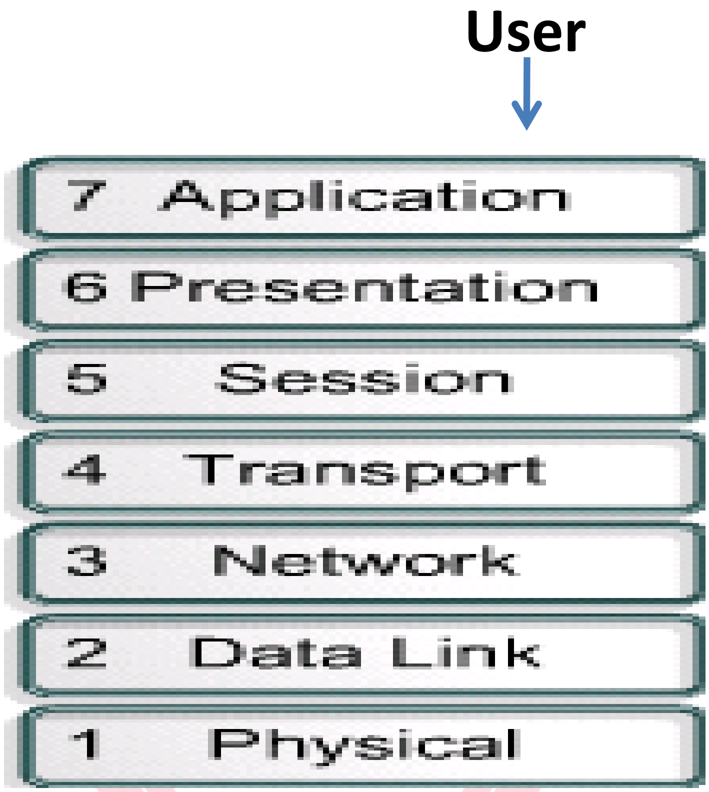
+91 93260 50669

v2vedtech.com

V2V EdTech LLP

v2vedtech

Q1. Explain the functions of the all layers of OSI model with their protocol. (with diagram).
Ans:

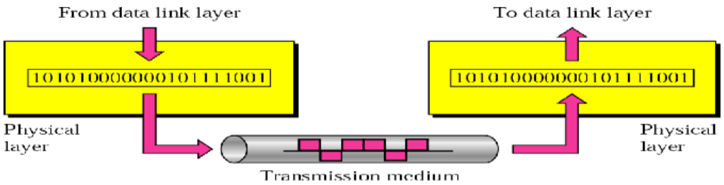


Physical layer:-

- Specifications for the physical components of the network.

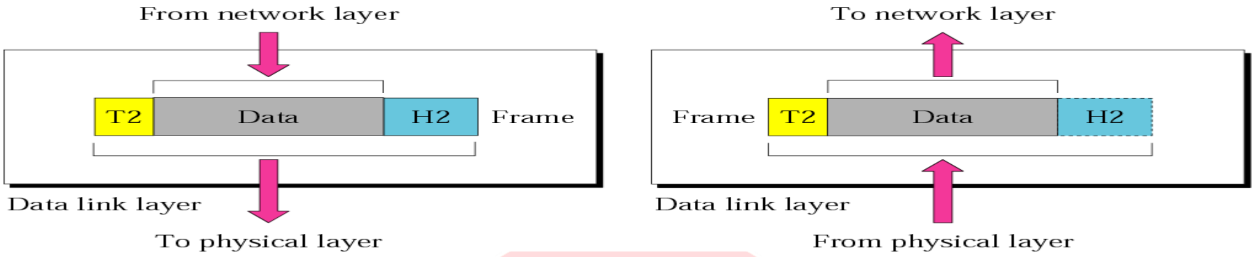
Functions of Physical Layer:

- **Bit representation** – encode bits into electrical or optical signals
- **Transmission rate** – The number of bits sent each second
- Physical characteristics of transmission media
- **Synchronizing** the sender and receiver clocks
- **Transmission mode** – simplex, half-duplex, full duplex
- **Physical Topology** – how devices are connected – ring, star, mesh, bus topology



Data Link Layer

- Data link layer attempts to provide reliable communication over the physical layer interface.
- **Breaks the outgoing data into frames** and **re-assemble the received frames**.
- Create and detect frame boundaries.
- **Handle errors** by implementing an acknowledgement and retransmission scheme.
- **Implement flow control**.



The data link layer is responsible for moving frames from one hop (node) to the next.

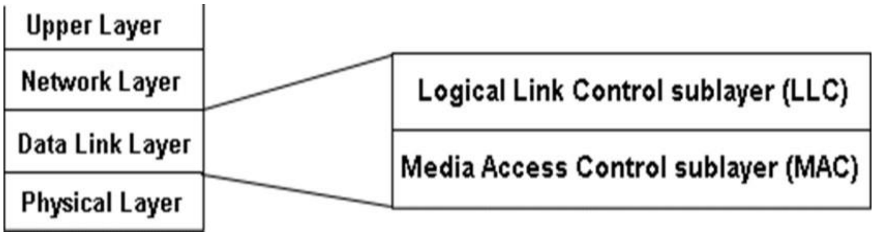
Functions of Data Link Layer

- **Framing-**
  - Divides the stream of bits into manageable data units called frames.
- **Physical addressing-**
  - Adds a header to the frame to define the sender and/or receiver of the frame.
- **Flow control-**
  - Imposes a flow control mechanism to avoid overwhelming the receiver.Synchronization between fast sender and slow receiver.
- **Error control-**
  - Adds mechanisms to detect and retransmit damaged or lost frames (CRC).
- **Access control-**
  - Determine which device has control over the link at any given time.
- **Link establishment and termination**:
  - Establishes and terminates the logical link between two nodes.
- **Frame sequencing**:
  - Transmits/receives frames sequentially.
- **Frame acknowledgment**:
  - Provides/expects frame acknowledgments.

DLL is divided into two Sub-Layers

- **LLC Sub Layer**

- **MAC Sub Layer**


Upper Layer
Network Layer
Data Link Layer
Physical Layer
Logical Link Control sublayer (LLC)
Media Access Control sublayer (MAC)

Logical Link Control Sub Layer

- It is upper portion of the Data Link layer.
- Performs **Flow control** and **management of connection errors**.
- LLC supports three types of connections:

1. **Unacknowledged connectionless service**:
   - does not perform reliability checks or maintain a connection, very fast, mostcommonly used
2. **Connection oriented service**:
   - once the connection is established, blocks of data can be transferred betweennodes until one of the node terminates the connection.
3. **Acknowledged connectionless service**:
   - provides a mechanism through which individual frames can be acknowledged.

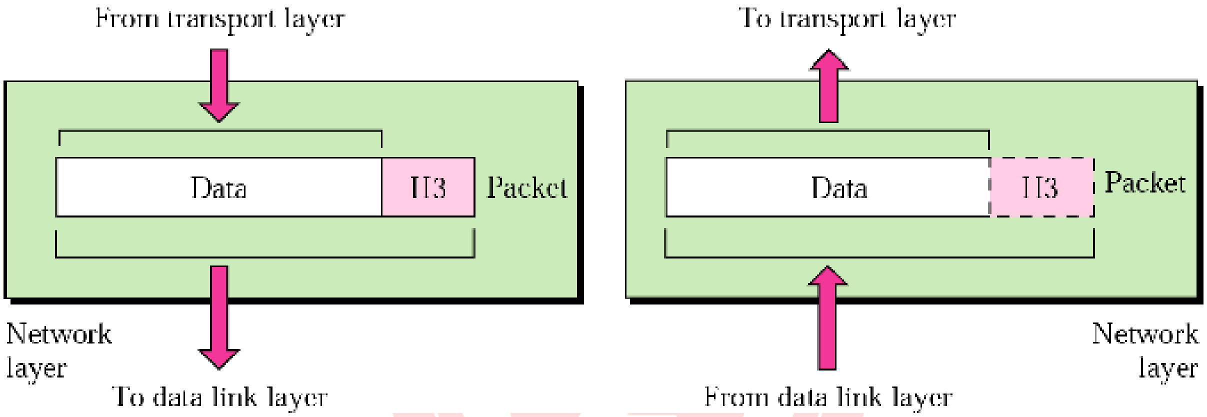
Media Access Control Sub Layer

- This sub layer contains methods to **regulate the timing** of data signals and **eliminatecollisions.**
- The MAC sub layer determines where one frame of data ends and the next one starts -
  frame synchronization.
- There are four means of frame synchronization:
  - Time based,
  - Character counting,
  - Byte stuffing and
  - Bit stuffing.

Network Layer:-

Main functions of this layer are:

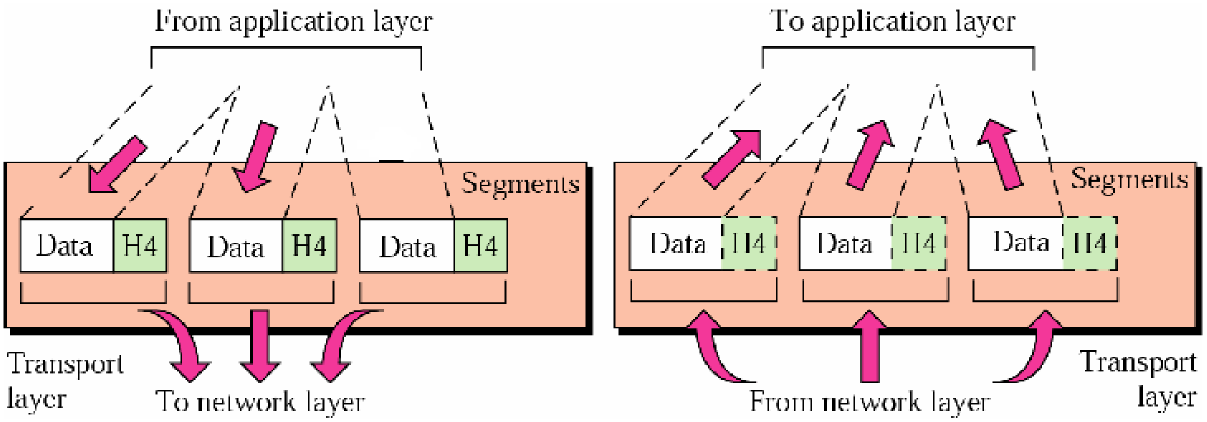
- Responsible for delivery of packets across multiple networks
- Routing – Provide mechanisms to transmit data over independent networks that are linked together.
- Network layer is responsible only for delivery of individual packets and it does not recognize anyrelationship between those packets



Transport Layer:-

Main functions of this layer are:

- Responsible for source-to destination delivery of the entire message
- Segmentation and reassembly – divide message into smaller segments, number them and transmit.Reassemble these messages at the receiving end.
- Error control – make sure that the entire message arrives without errors – else retransmit.

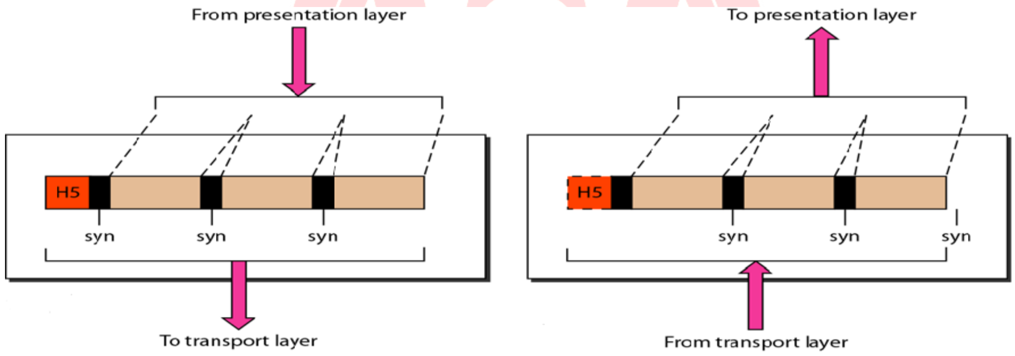


Session Layer:-

Main functions of this layer are:

• **Dialog control** – allows two systems to enter into a dialog, keep a track of whose turn it is to transmit

• **Synchronization** – adds check points (synchronization points) into stream of data.



Presentation Layer:-

Responsibilities of this layer are:

- **Translation**

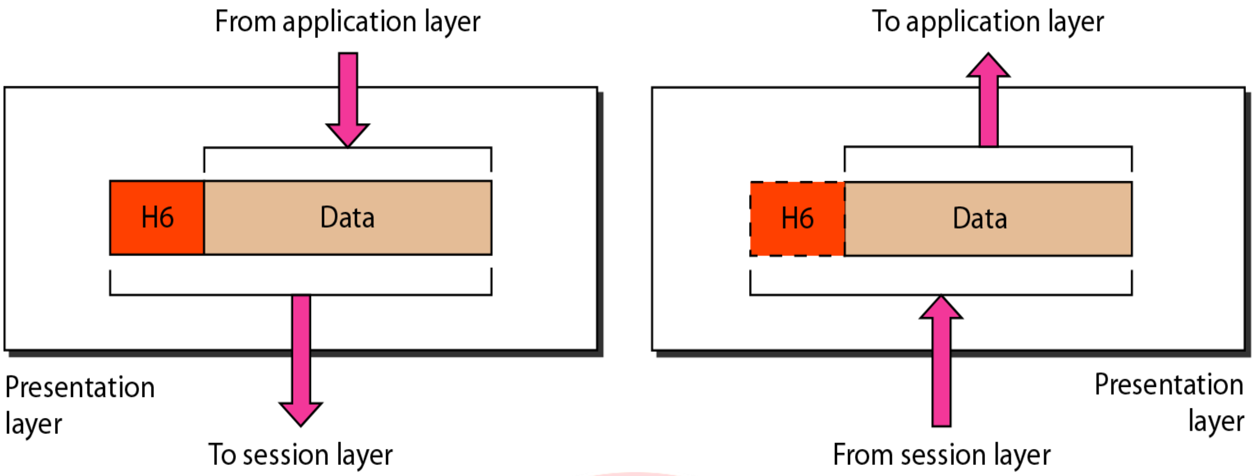
  • Different computers use different encoding systems (bit order translation)

  • Convert data into a common format before transmitting.

  • Syntax represents info such as character codes - how many bits to represent data – 8 or 7 bits

- **Compression** – reduce number of bits to be transmitted Encryption – transform data into anunintelligible format at the sending end for data security

- **Decryption** – at the receiving end

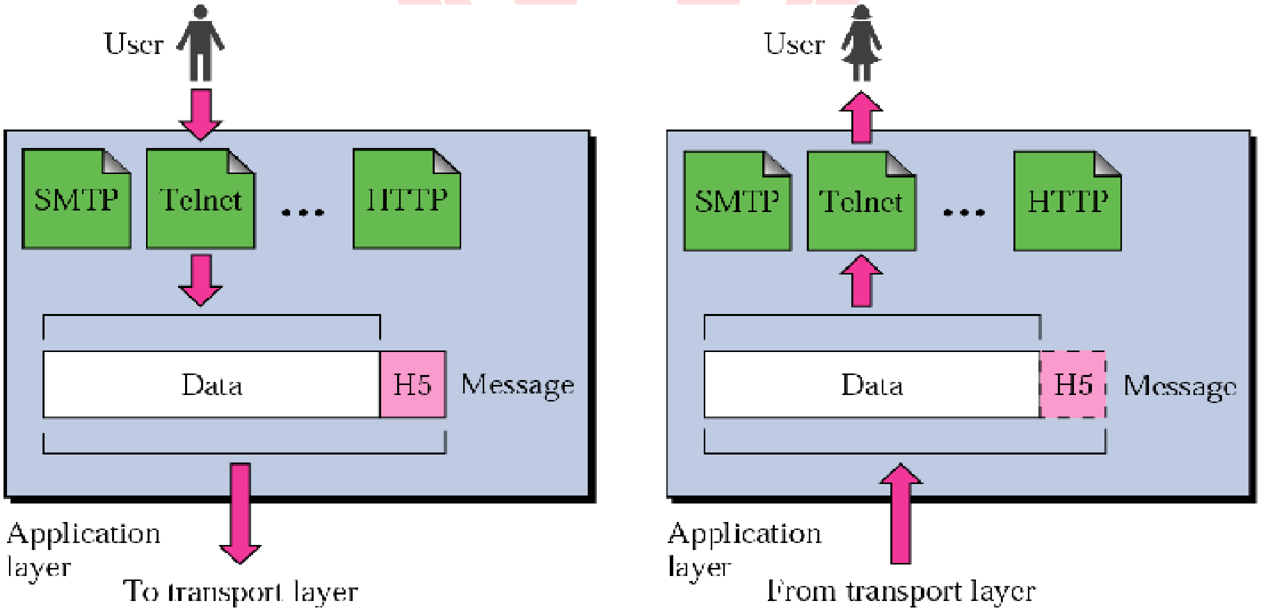


Application Layer:-

•Contains protocols that allow the users to access the network (FTP, HTTP, SMTP, etc)

• Does not include application programs such as email, browsers, word processing applications, etc.

• Protocols contain utilities and network-based services that support email via SMTP, Internet access viaHTTP, file transfer via FTP, etc



Q2. Describe network operating system in detail.
Ans:
A Network Operating System (NOS) is a specialized operating system that provides network services and capabilities to devices connected within a network. It serves as the backbone of a network infrastructure, facilitating communication, resource sharing, security, and management among networked devices. Here's a detailed overview of a Network Operating System:

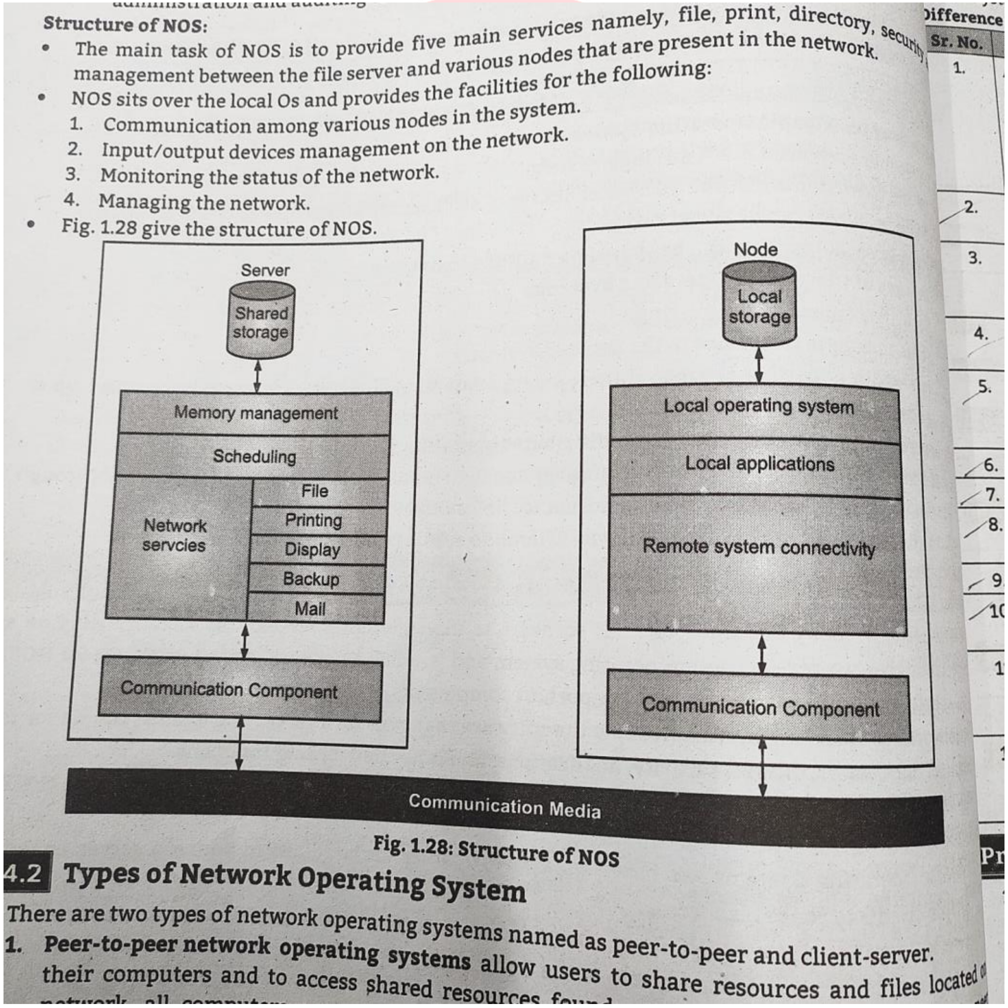
1. **Basic Functions**:
  - **Network Communication**: A NOS enables devices within a network to communicate with each other by providing protocols and services for data transmission, routing, and addressing.
  - **Resource Sharing**: It facilitates the sharing of hardware resources such as printers, scanners, storage devices, and software resources like files, databases, and applications among networked devices.
  - **User Authentication and Access Control**: NOS implements security mechanisms to authenticate users and control their access to network resources, ensuring data confidentiality, integrity, and availability.
  - **Network Management**: It includes tools and utilities for monitoring network performance, configuring network settings, diagnosing network issues, and managing network devices centrally.
  - **Fault Tolerance and Redundancy**: NOS may include features like fault tolerance, redundancy, and failover mechanisms to ensure uninterrupted network operation and data availability.

2. **Components of Network Operating System**:
  - **Kernel**: The core component of the NOS responsible for managing hardware resources, process scheduling, memory management, and device drivers.
  - **Networking Services**: Includes protocols and services for network communication, such as TCP/IP stack, DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), and SNMP (Simple Network Management Protocol).
  - **File and Print Services**: Enables sharing of files and printers across the network, providing centralized storage and access control mechanisms.
  - **Security Services**: Implements authentication mechanisms, encryption, access control lists (ACLs), firewalls, and intrusion detection/prevention systems to secure the network from unauthorized access and attacks.
  - **Directory Services**: Provides centralized user authentication, authorization, and directory management services, such as LDAP (Lightweight Directory Access Protocol) or Active Directory.
  - **Management Tools**: Includes utilities and graphical interfaces for network configuration, monitoring, troubleshooting, and performance optimization.

3. **Types of Network Operating Systems**:
  - **Client-Server NOS**: Designed for environments where servers provide services to client devices. Examples include Windows Server, Linux/UNIX servers, and Novell NetWare.
  - **Peer-to-Peer NOS**: Suitable for small networks where all devices can act as both clients and servers. Examples include Windows Workgroup, macOS, and Linux distributions.

4. **Examples of Network Operating Systems**:
   - **Windows Server**: Microsoft's server operating system providing a comprehensive suite of network services and features.
   - **Linux/UNIX Servers**: Various distributions of Linux and UNIX operating systems offer robust network services and customization options.
   - **Novell NetWare**: An early NOS renowned for its reliability, security, and file/print sharing capabilities (now discontinued).
   - **macOS Server**: Apple's server operating system offering network services such as file sharing, Time Machine backups, and profile management.

In summary, a Network Operating System is a specialized operating system designed to provide network services and capabilities, including communication, resource sharing, security, and management, to devices within a network infrastructure. It plays a critical role in ensuring the efficient and secure operation of modern computer networks.



Structure of NOS:

- The main task of NOS is to provide five main services namely, file, print, directory, security management between the file server and various nodes that are present in the network.
- NOS sits over the local Os and provides the facilities for the following:
  1. Communication among various nodes in the system.
  2. Input/output devices management on the network.
  3. Monitoring the status of the network.
  4. Managing the network.
- Fig. 1.28 give the structure of NOS.

Fig. 1.28: Structure of NOS

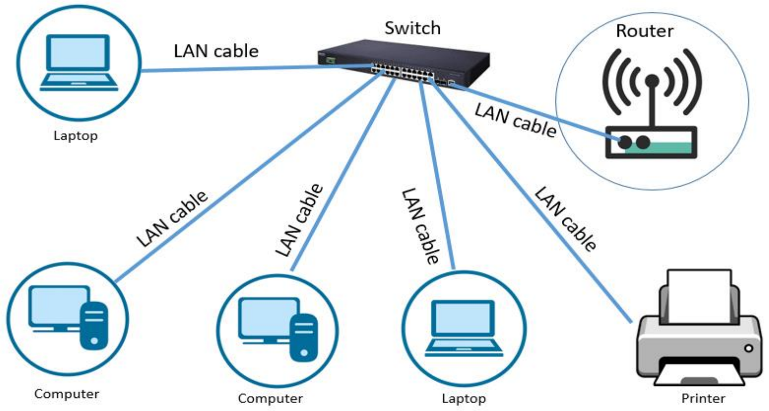
4.2 Types of Network Operating System

There are two types of network operating systems named as peer-to-peer and client-server.

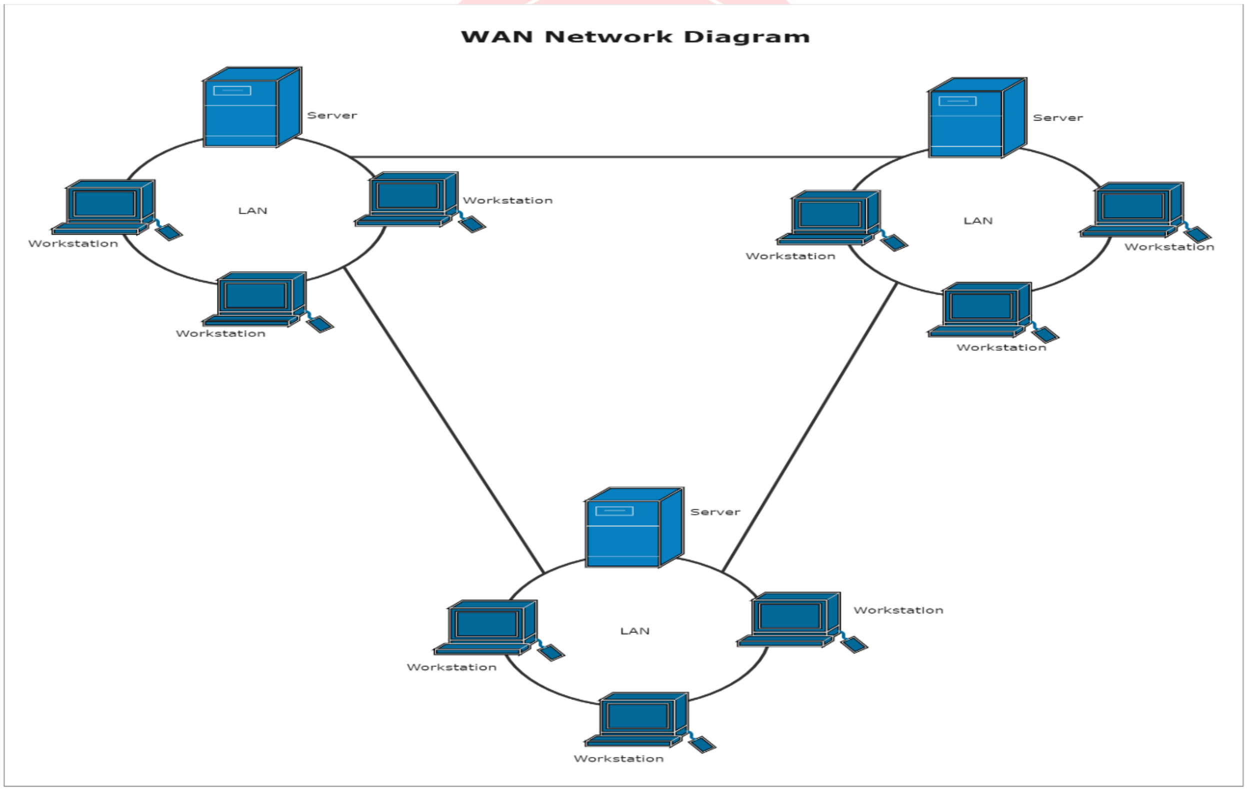
1. **Peer-to-peer network operating systems** allow users to share resources and files located on their computers and to access shared resources found

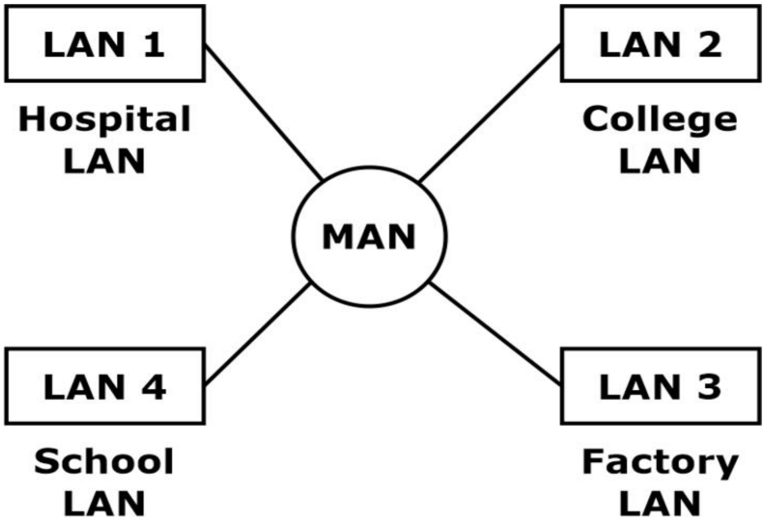
Q3. Difference between LAN MAN and WAN. (including diagram)
Ans:

Parameter	**LAN**	**MAN**	**WAN**
Full Form	LAN is an acronym for Local Area Network.	MAN is an acronym for Metropolitan Area Network.	WAN is an acronym for Wide Area Network.
Definition and Meaning	LAN is a network that usually connects a small group of computers in a given geographical area.	MAN is a comparatively wider network that covers large regions- like towns, cities, etc.	The WAN network spans to an even larger locality. It has the capacity to connect various countries together. For example, the Internet is a WAN.
Network Ownership	The LAN is private. Hospitals, homes, schools, offices, etc., may own it.	The MAN can be both private or public. Many organizations and telecom operators may own them.	The WAN can also be both private or public.
Maintenance and Designing	Very easy to design and maintain.	Comparatively difficult to design and maintain.	Very difficult to design and maintain.
Speed	LAN offers a very high Internet speed.	MAN offers a moderate Internet speed.	WAN offers a low Internet speed.
Delay in Propagation	It faces a very short propagation delay.	It faces a moderate propagation delay.	It faces a high propagation delay.



Local Area Network





Q4. Define following term: 1. Physical address 2. Logical address 3. Port address 4. Access point.
Ans:
Here are the definitions for each term:

1. **Physical Address**:
  - A physical address, also known as a hardware address or MAC (Media Access Control) address, is a unique identifier assigned to a network interface controller (NIC) or network adapter by its manufacturer. It is expressed as a series of hexadecimal digits and is used at the data link layer of the OSI model to uniquely identify devices within a local network. Physical addresses are hardcoded into the hardware and typically cannot be changed.

2. **Logical Address**:
  - A logical address, also known as an IP (Internet Protocol) address, is a numeric label assigned to each device connected to a network that uses the Internet Protocol for communication. Logical addresses are used to uniquely identify devices within a network and facilitate communication between them. Unlike physical addresses, logical addresses can be dynamically assigned (using DHCP) or manually configured, and they can change as devices move between networks.

3. **Port Address**:
  - A port address, also known as a port number, is a numerical value used to identify specific communication endpoints within a device in a network. In the context of TCP/IP networking, ports are associated with either TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) communication protocols. Port numbers range from 0 to 65535, with well-known ports (0-1023)

reserved for standard services like HTTP (port 80) and FTP (port 21), and dynamic or private ports (49152-65535) available for use by applications.

4. **Access Point**:
   - An access point (AP) is a device that serves as a central hub for wireless communication within a wireless local area network (WLAN). Access points typically connect wireless devices, such as laptops, smartphones, and tablets, to a wired network infrastructure, allowing them to access resources and services on the network. Access points may also provide security features such as encryption and authentication to protect the WLAN from unauthorized access.

Q5. Define following term 1. Define computer network with its advantages and disadvantages. 2. Describe NIC with its features 3. Concept of data encapsulation
Ans:

1. **Computer Network:**
   - **Definition**: A computer network is a collection of interconnected computers and other devices that can communicate with each other and share resources, such as data, applications, and hardware peripherals. The primary purpose of a computer network is to facilitate communication and resource sharing among users and devices, regardless of their physical locations.

Advantages:
1. File sharing: The major advantage of computer network is that it allows file sharing and remote file access. A person sitting at one workstation that is connected to a network can easily see files present on another workstation, provided he/she is authorized to do so.
2. Resource Sharing: A computer network provides a cheaper alternative by the provision of resource sharing. All the computers can be interconnected using a network and just one modem & printer can efficiently provide the services to all users.
3. Inexpensive set-up: Shared resources means reduction in hardware costs. Shared files means reduction in memory requirement, which indirectly means reduction in file storage expenses.
4. Flexible Handling: A user can log on to a computer anywhere on the network and access his/her files. This offers flexibility to the user as to where he/she should be during the course of his/her routine.

Disadvantages:
1. Security concerns: One of the major drawback of computer network is the security issues that are involved.
2. Virus and malware: Viruses can spread on a network easily because of the interconnectivity of workstations.
3. Lack of robustness: If the main file server of a computer network breaks down, the entire system becomes useless.
4. Needs an efficient handler: The technical skills and knowledge required to operate and administer a computer network.

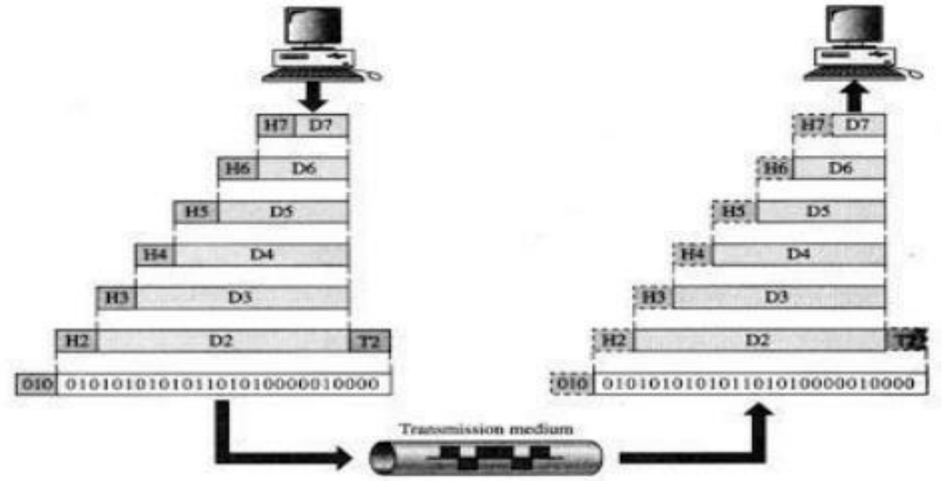
2. **Network Interface Card (NIC)**:

NIC: NIC is a Network Interface Card which is a small card inserted or plugged on the motherboard of the host. It has a small CPU, memory and a limited instruction set required for the network related functions. Each NIC has a unique hardware address or physical address to identify the host uniquely, which ensures that its unique all over world.

The functions include:

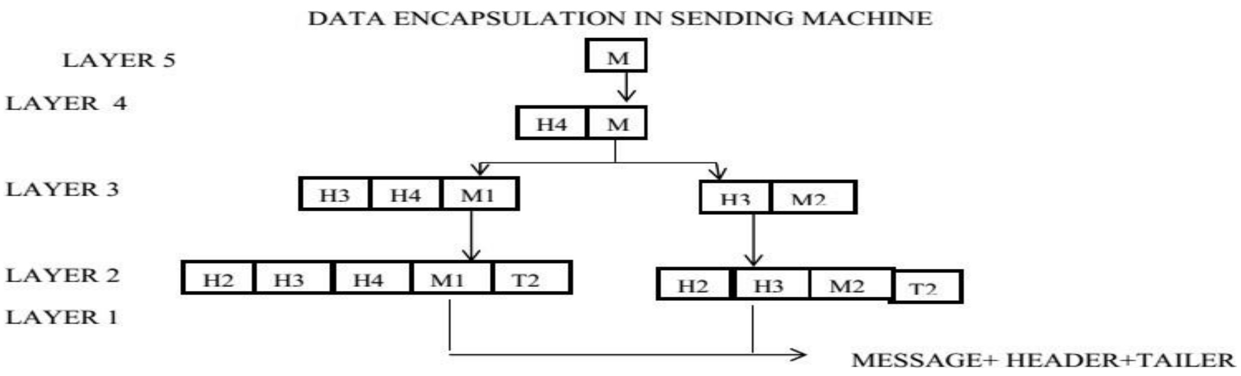
- It accepts instructions from host to transfer data to/ from cable.
- It checks the status of the bus with the help of the transceiver and waits till the bus is busy.
- It sends the data bit by bit once the bus is idle.
- It inserts the CRC in the header of the frame while transmitting.
- While accepting the data, NIC compares the destination address in the frame with its own hardware address; If matches then only it is accepted otherwise rejected.
- Validating the input frame by checking its CRC to ensure that the data is error free.

3. **Data Encapsulation**:

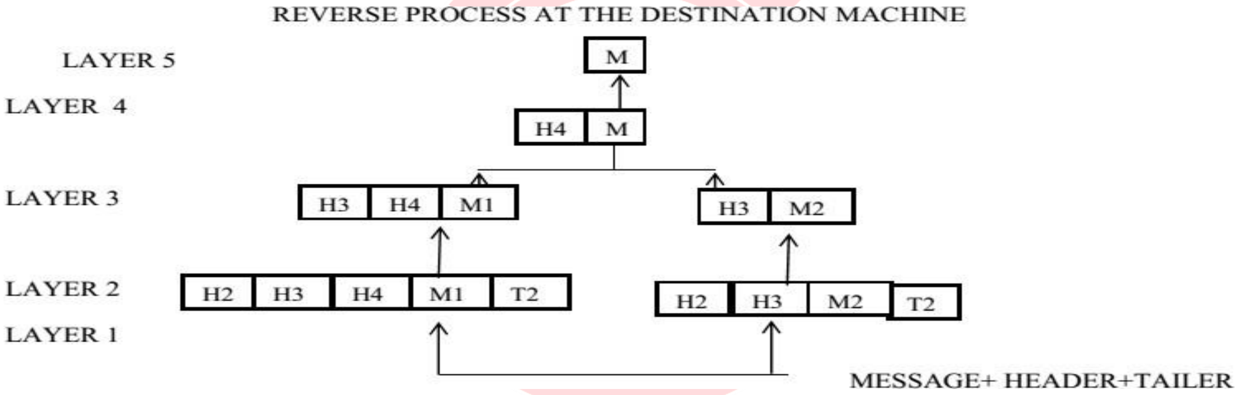


Each layer in the layered architecture provides service to the layers which are directly above and below it. The outgoing information will travel down through the layers to the lowest layer. While moving down on the source machine, it acquires all the control information which is required to reach the destination machine. The control information is in the form of headers and trailers which surrounds the data received from the layer above. This process of adding headers and trailers to the data is called as data encapsulation. The headers and trailers contain control information in the individual fields. It is used to make message packet reach the destination. The headers and trailers form the envelope which carries the message to the desired destination.

Example:



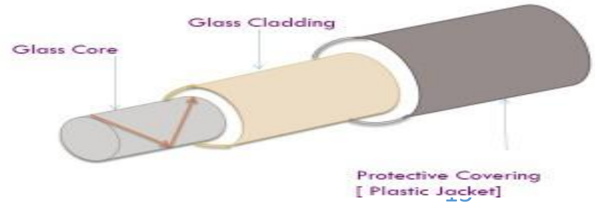
H4 = LAYER 4 HEADER
H3 = LAYER 3 HEADER
H2 = LAYER 2 HEADER
T2 = LAYER 2 TAILER



The figure shows the example of five layer stack for data encapsulation. The fifth layer of sending machine wants to send a message M to the fifth layer of destination machine. The message M is produced by layer 5 of machine 1 and given to layer 4 for transmission. Layer 4 adds header H4 in front of the message and pass it to layer 3. Layer 3 breaks up the incoming message into small units as M1 and M2 and pass these packets to layer 2. Layer 2 adds the header as well as footer to each packet obtained from layer 3 and pass it to layer 1 for physical transmission.

Q6. Describe the construction of Fiber optic cable and coaxial with a neat diagram.

Ans: **Fiber Optic Cable**

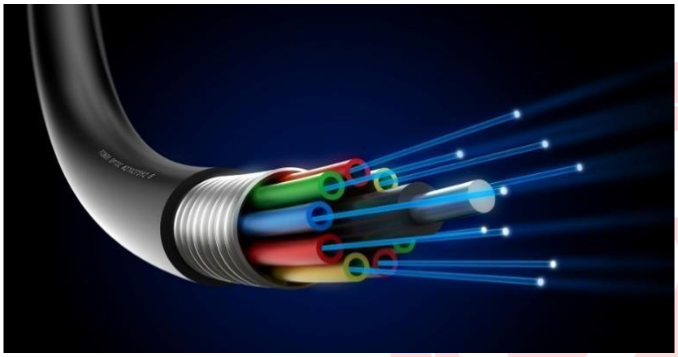


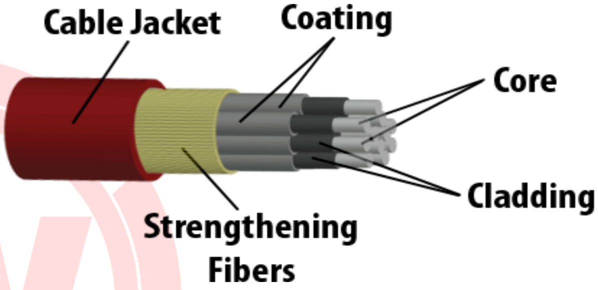
- A fibre optic cable is made of high quality of thin glass or plastic and is used to transfer digital data signals in the form of light up to distance of thousands of miles.

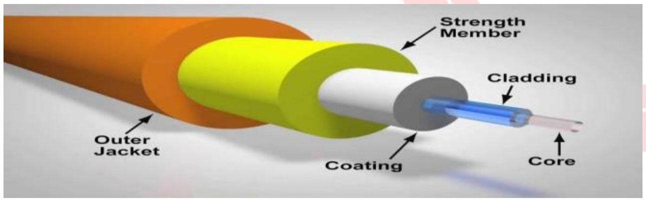
- Fibre optic cables are not affected by electromagnetic interference, so noise and distortion is very less.

- Fibre optic cables carry communication signals using pulses of light generated by small lasers or light-emitting diodes (LEDs).

- The cable consists of one or more strands of glass, each only slightly thicker than a human hair. The centre of each strand is called the core, which provides the pathway for light to travel. The core is surrounded by a layer of glass called cladding that reflects light inward to avoid loss of signal and allow the light to pass through bends in the cable. No light escapes the glass core because of this reflective cladding.



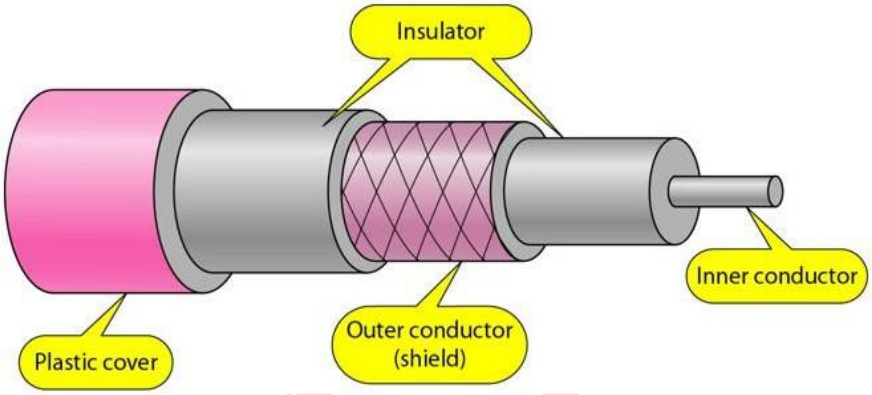




Coaxial Cable

- Coaxial cables are copper cables with better shielding than twisted pair cables, so that transmitted signals may travel longer distances at higher speeds.
- The shield minimizes electrical and radio frequency interference.

- Coaxial cabling is the primary type of cabling used by the cable television industry and is also widely used for computer networks, such as Ethernet



- Coaxial cable has two wires of copper.

- The core/inner copper wire in centre and is made of solid conductor. It is enclosed in an insulating sheath.

- The second/outer copper wire is wrapped around, and is used to protect from external electromagnetic interference (Noise).

- This all is covered by plastic cover used to protect the inner layers from physical damage such as fire or water.

Coaxial Cable Standards

- Coaxial cables are categorized by their Radio Government (RG) ratings. Each RG number denotes a unique set of physical specifications

• 50-Ohm	RG-7 or RG-11	: used with thick Ethernet.
• 50-Ohm	RG-58	: used with thin Ethernet
• 75-Ohm	RG-59	: used with cable television

Q7. Explain following topology in detail with its advantages, disadvantage and diagram 1. Ring topology 2. Mesh topology 3. Start topology 4. Hybrid topology

Ans: 1. Ring Topology:

In Ring topology each node is connected to the two nearest nodes so the entire network forms a circle. Rings are used in high performance network. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along. Every PC is connected to next computer in the ring and each transmits what it receives from the previous PC. The message flows around the ring in one direction. Since each PC retransmits what it receives a ring is an active network. There is no termination because there is no end to the ring.

Advantages of ring topology

i. A ring is relatively easy to install and configure (for fix number of devices).

ii. Fault isolation is simplified- generally in a ring a signal is circulating at all time if any device does not receive a signal within the specified period. It can issue an alarm. Alarm alerts the network operator to the problem of its location.

iii. To add or delete a device requires moving only two connections.

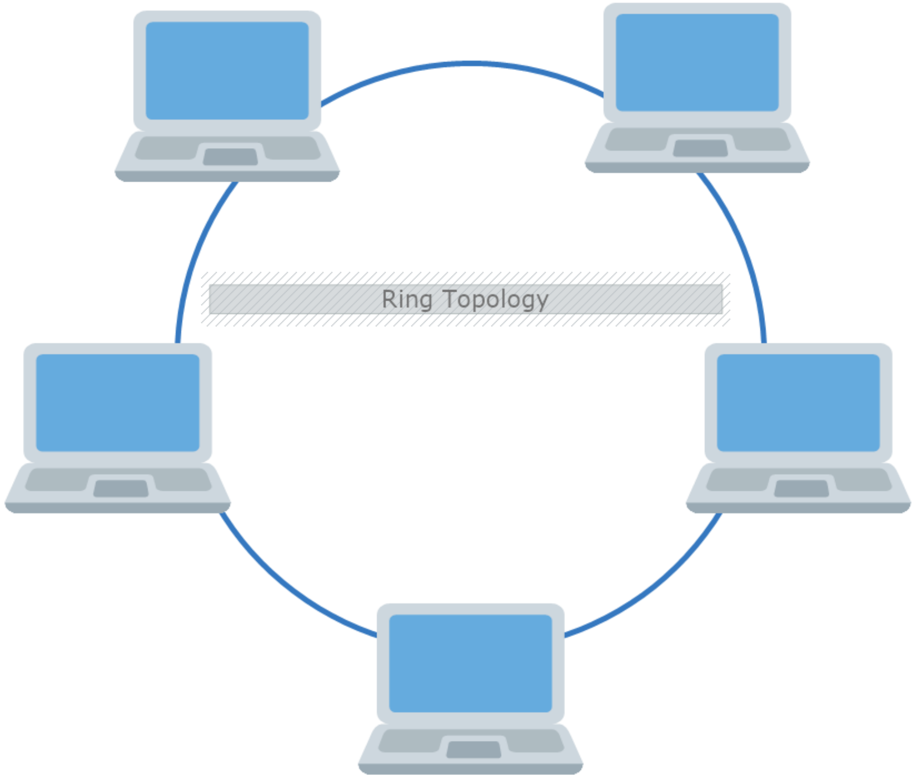
iv. Time to send data is known: that is package delivery time is fixed and guaranteed because every PC is given to the token. No one PC can monopolies network. v. No data collisions.

Disadvantages of ring

1. A single node failure leads to the collapse of the full network.

2. Unidirectional traffic can be disadvantage in a simple ring. A break in the ring can disable the entire network; using dual ring can solve the weakness.

3. Expansion to the network can cause network disruption



2. Mesh topology :

In a mesh topology every device has dedicated point-to-point link to every other device. The term dedicated means that the link carries only between the two devices it connects. A fully connected mesh network has n (n-1)/2 physical connections to link devices.

To accommodate that many links every device on the network must have (n-1) output ports because each device requires an interface for every other on the network. Mesh topology are not usually practical. In addition unless each station frequently sends signal to all the other stations and excessive amount of network bandwidth is wasted.

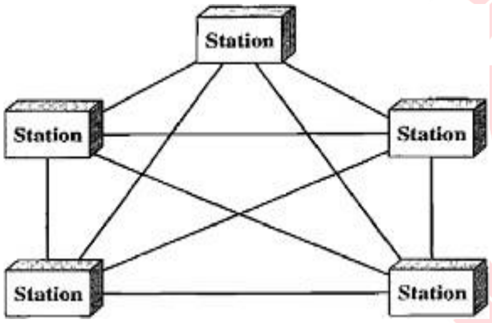
Mesh gets unmanageable beyond a very small number of devices. Most mesh topology networks are not true mesh networks.

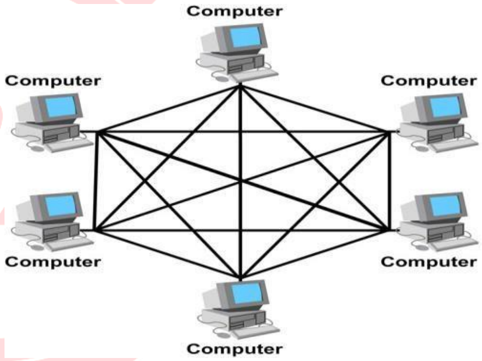
Advantages:-

¬ The use of dedicated links guaranties that connections can carry its own data load. Thus eliminating the traffic problem that can occur when links must be shared by multiple devices.

¬ Mesh topology is Robust (strong) if one link becomes unusable. It doesn’t incapacitate the entire n/w.

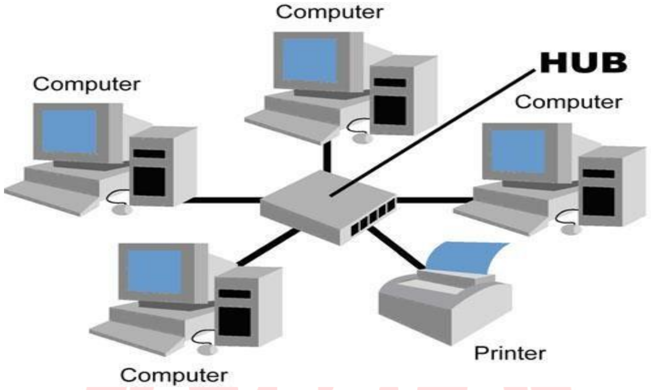
¬ Another advantage is privacy and security when every message sent travels along a dedicated line only the intended recipients sees it. Physical boundaries prevent other users from gaining access to message.
¬ Point to point link make fault identification and fault isolation easy. Traffic can be routed to avoid links with respected problems. This facility enables the n/w manager to discover the precise location of the fault and aids it finding its cause and solution.
¬ Extremely fault tolerant.
¬ It is more reliable compare to other topologies.
¬ In case of heavy traffic data can be routed around busy root.
Disadvantages
¬ As it involves a lot of connection. The total no. of physical links and the no. of I/O ports require to connect will be more and hence is prohibitively expensive.
¬ Difficult to install and reconfigure specially as no. of devices increases.
¬ Hardware required to connect each device is highly expensive.
¬ The sheer bulk of the wiring can be greater than the available space (walls, ceiling and floors) can accommodate. For these reasons a mesh topology is usually implemented in a limited fashion.



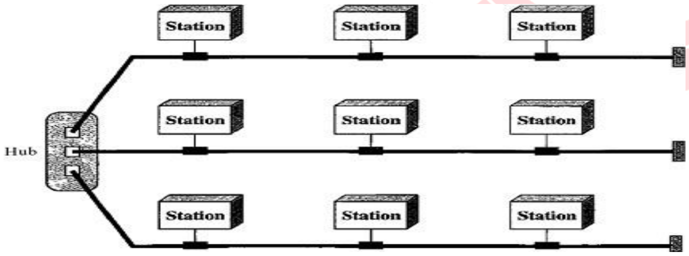


3. Start topology:
Physical star topology uses a central device or controller with drop cables extending in all direction. The devices are not directly linked to one another. Each network device is connected via point-to-point link to central device called ‘HUB’ multipoint repeater or concentrator. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.
When network expansion is expected and a greater reliability is expected then star topology is needed.
Advantages of star topology
There are several advantages to a star topology.
i. Addition, Moving and deletion involves only one connection between that device and hub.
ii. When the capacity of central hub is exceeded you can replace it with one that has larger number of ports to plug lines into new hub.
iii. The center of the star network is a good place to diagnose network faults, intelligent hub (the hub with microprocessor) also provide for centralize monitoring and management of network.

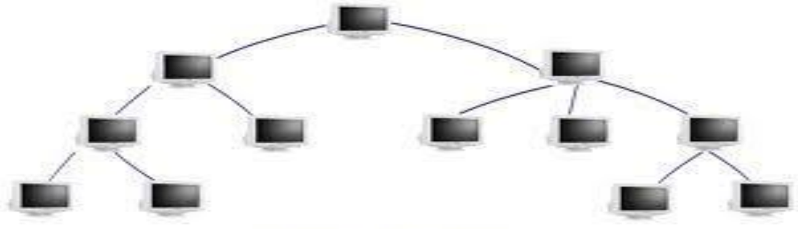
iv. Single PC failures do not necessarily bring down whole star network. The hubs can detect a network fall and isolate the defected PC or network cable and allow the rest of the network to continue operating.
v. You can use several cable types in the same network with a hub that can accommodate multiple cable types.
Disadvantages of star topology
1. If the central hub fails the whole network fails to operate.
2. Many star networks requires a devices at the central point to rebroadcast or switched network traffic.
3. It cost more to cable a star networks because all the network cables must be pulled to one central point requiring more cable than other networking topologies.



4. Hybrid topology:
A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in Figure



Star Bus (Tree Topology)

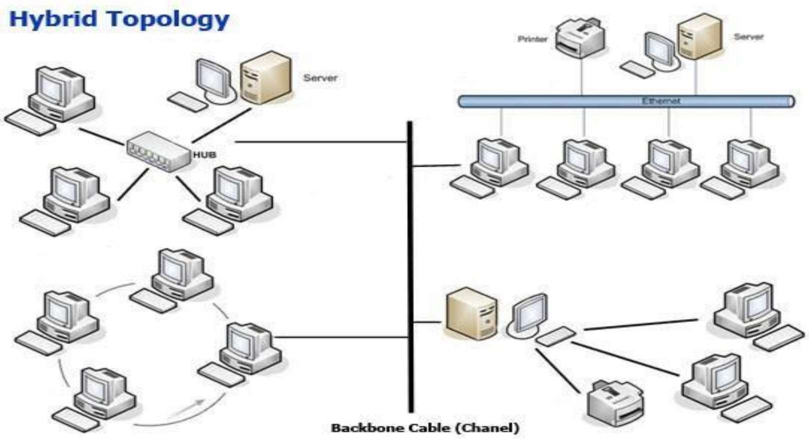


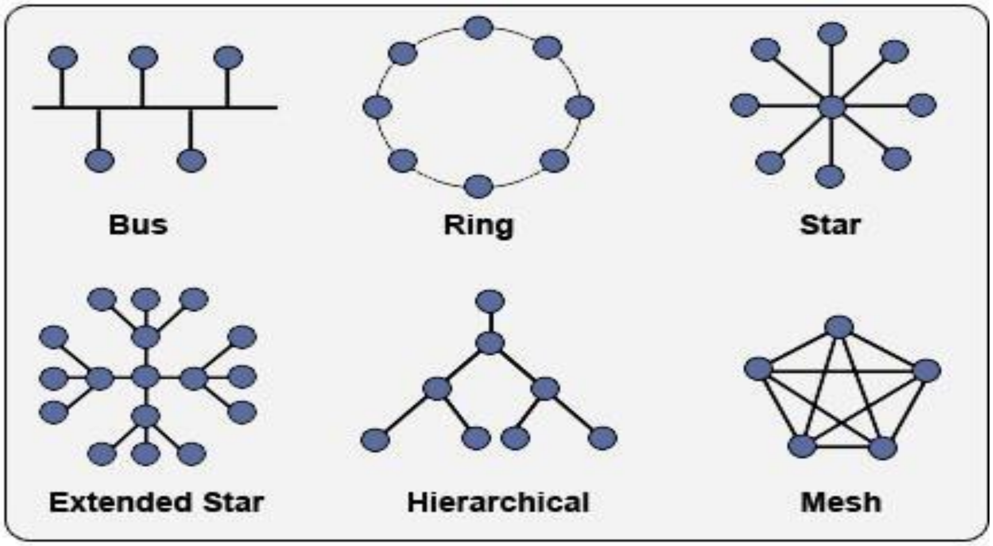
Digram - Tree Topology

Star bus topology combines the bus and the star linking several stars hubs together with the bus trunk. If one computer fails, the hub can detect the fault and isolate the PC. If a hub fails PC connected to it will not be able to communicate and the bus n/w will be broken into two segments that can’t reach each other.

Star ring

This is also called as star wired ring. The n/w cables are laid out much like a star n/w but a ring is implemented in the central hub outgoing hubs can be connected through the inner hubs effectively extending a loop of the ring. E.g. Token ring is considered a star ring although its topology is physical a start its function logically in a ring.





Q8. Compare IPv4 & IPv6 address (8 points).
Ans:

IPv4	IPv6
IPv4 has a 32-bit address length	IPv6 has a 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end, connection integrity is Unachievable	In IPv6 end-to-end, connection integrity is Achievable
It can generate 4.29×109 address space	The address space of IPv6 is quite large it can produce 3.4×1038 address space
The Security feature is dependent on the application	IPSEC is an inbuilt security feature in the IPv6 protocol
Address representation of IPv4 is in decimal	Address Representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation is performed only by the sender
In IPv4 Packet flow identification is not available	In IPv6 packet flow identification are Available and uses the flow label field in the header

Q9. State the internet layer protocols in TCP/IP suite.
Ans:

- Function: Handles the movement of data packets between networks. It is responsible for IP addressing, routing, and packet forwarding.

- Protocols: IP (Internet Protocol), ICMP (Internet Control Message Protocol)
- Advantages: Enables global communication by routing packets across interconnected networks.
- Disadvantages: Lack of built-in security features in IP, which can be addressed by additional protocols like IPSec.
- Diagram: (Internet) <-> IP, ICMP

Q10. Explain the function of ARP and ICMP.
Ans:

1. **Address Resolution Protocol (ARP)**:
  - **Function**: ARP resolves the mapping between IP addresses and MAC addresses within a local network segment. When a device wants to communicate with another device on the same network, it uses ARP to determine the MAC address associated with the IP address of the destination device.
  - **Operation**:
    - When a device needs to send a packet to another device whose IP address it knows but whose MAC address it does not, it broadcasts an ARP request packet to the network.
    - The ARP request contains the IP address of the target device.
    - The device with the corresponding IP address responds with an ARP reply packet containing its MAC address.
    - Once the requesting device receives the ARP reply, it can use the MAC address to send packets to the destination device.

2. **Internet Control Message Protocol (ICMP)**:
  - **Function**: ICMP is used for various purposes, including error reporting, network diagnostics, and management. It enables network devices to communicate status and error information to each other, facilitating the detection and resolution of network-related issues.
  - **Operation**:
    - ICMP messages are encapsulated within IP packets and are typically used to report errors such as "Destination Unreachable" or "Time Exceeded."
    - ICMP messages can also be used for diagnostic purposes, such as the "Echo Request" and "Echo Reply" messages used by the ping utility to test network connectivity.
    - ICMP messages are sent by network devices in response to abnormal conditions or requests from other devices on the network.
    - ICMP plays a crucial role in ensuring the efficient and reliable operation of IP networks by providing feedback about network status and facilitating communication between network devices.

Q10. Explain the working of subnetting and supernetting with diagram and example.
Ans:
Subnetting:

Subnetting is the process of dividing a larger network into smaller sub-networks (subnets). It helps in efficiently utilizing IP addresses and managing network traffic by logically grouping devices into smaller segments.

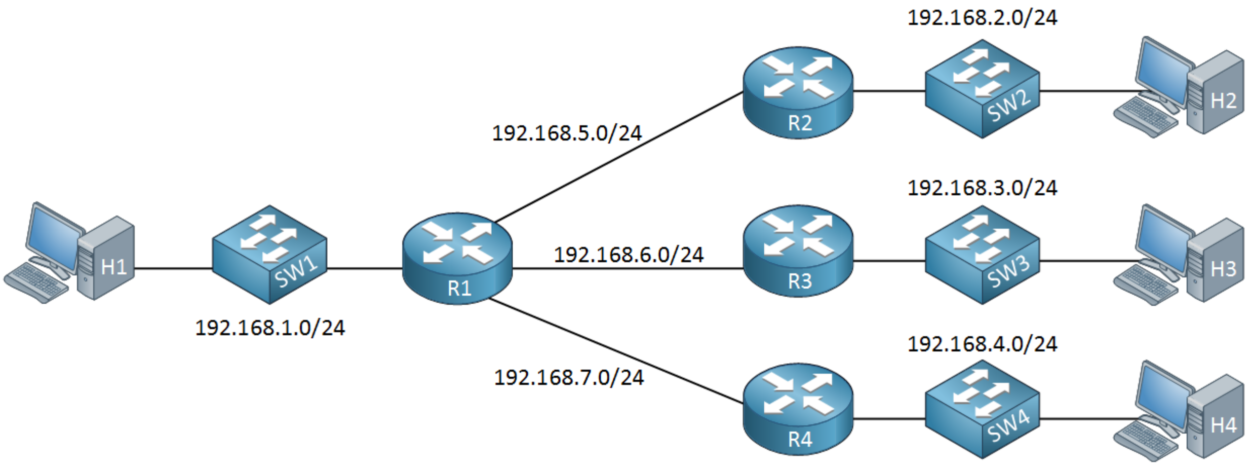
Example:

Consider a network with IP address range 192.168.1.0/24. Here, /24 indicates that the network has 24 bits dedicated to the network portion (192.168.1) and 8 bits for host addresses (0-255). With subnetting, you can further divide this network into smaller subnets. For instance, you can create two subnets:

- Subnet 1: 192.168.1.0/25 (with addresses 192.168.1.0 to 192.168.1.127)

- Subnet 2: 192.168.1.128/25 (with addresses 192.168.1.128 to 192.168.1.255)

By subnetting, you can efficiently allocate IP addresses and manage network traffic within each subnet.



Supernetting:

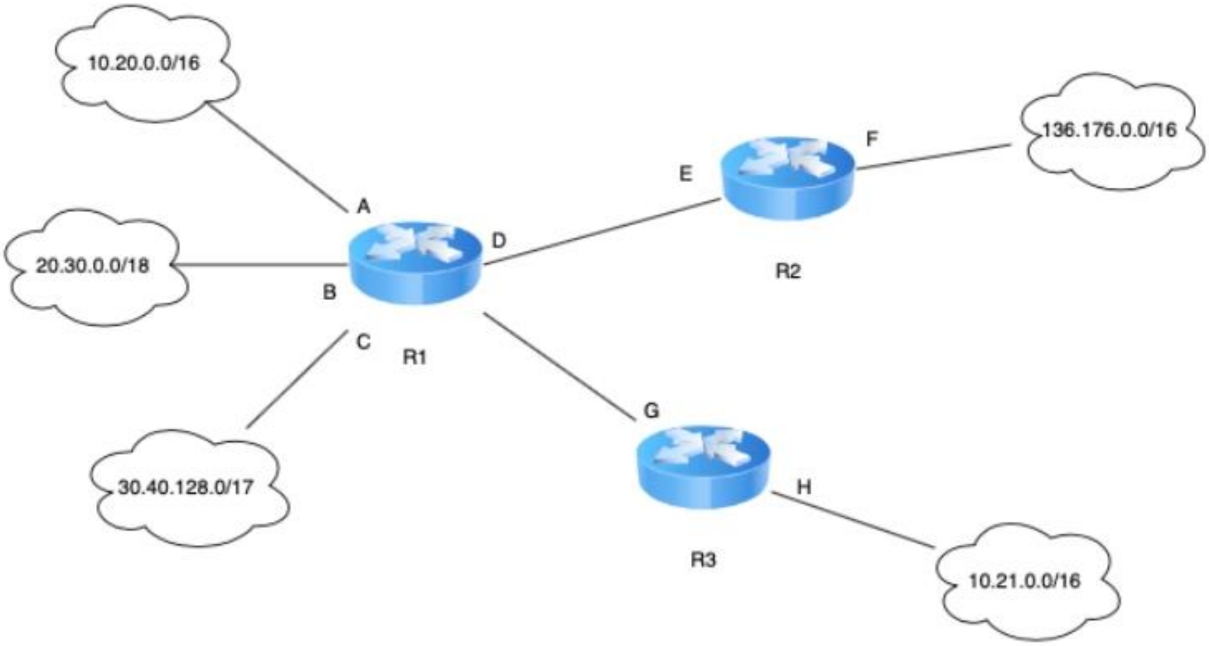
Supernetting (or route aggregation) is the opposite of subnetting. It involves combining multiple smaller IP address ranges (subnets) into a larger range, reducing the number of routing table entries and improving routing efficiency.

Example:

Suppose you have two smaller IP address ranges: 192.168.1.0/25 and 192.168.1.128/25. These can be combined into a single supernet:

- Supernet: 192.168.1.0/24

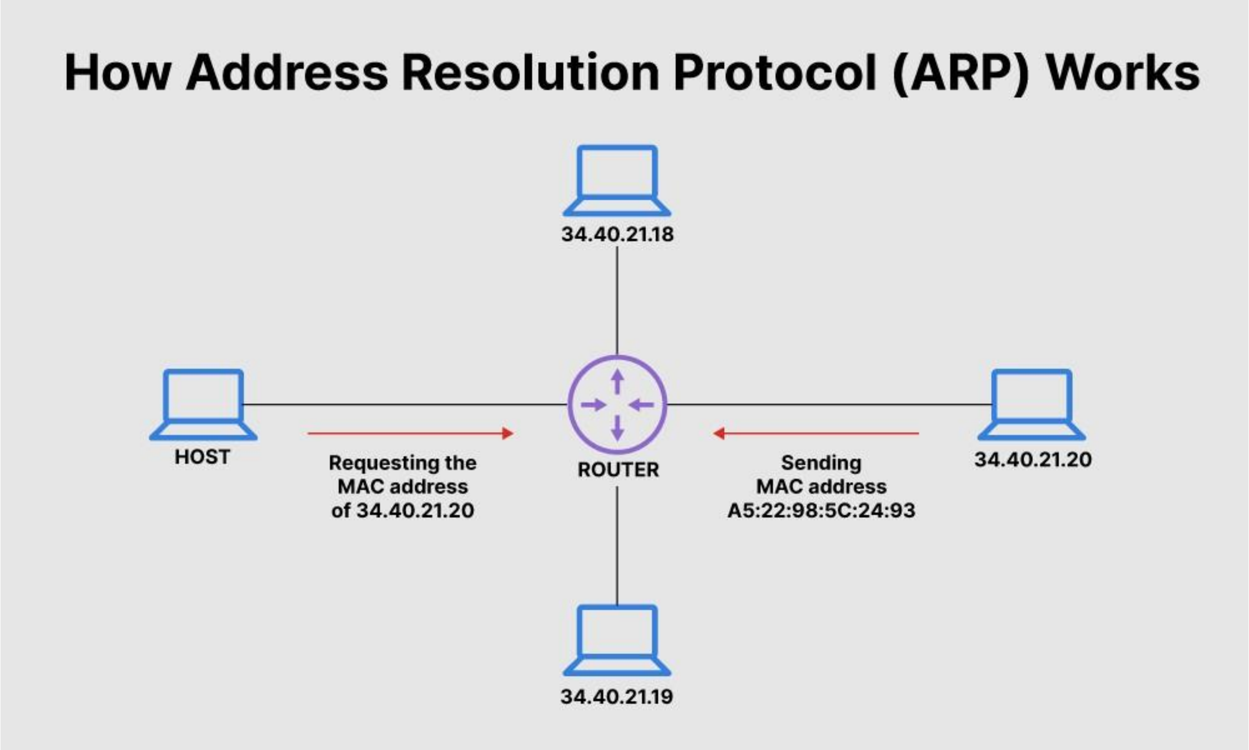
In this example, both smaller subnets fit within the larger supernet range of 192.168.1.0/24. This simplifies routing information and reduces the number of entries in routing tables.



Q11. Explain working of following term with its function, advantages, disadvantages and diagram. 1. ARP 2. RARP 3. FTP 4. HTTP 5. DHCP configuration
Ans:

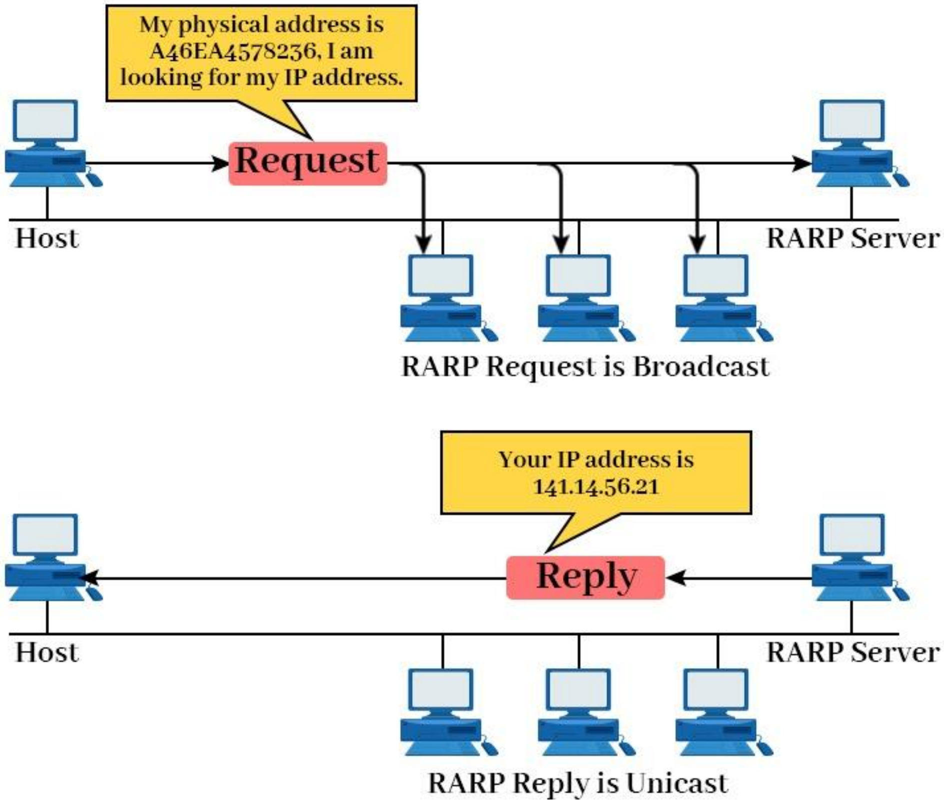
ARP (Address Resolution Protocol):

- **Function**: ARP is used to map IP addresses to MAC addresses in a local network. It resolves the MAC address of a device when only its IP address is known, allowing devices to communicate with each other on the same network.
- **Advantages**:
- Enables communication between devices on the same network segment.
- Simplifies network communication by providing a way to resolve IP addresses to MAC addresses.
- **Disadvantages**:
- Vulnerable to ARP spoofing attacks, where an attacker sends fake ARP messages to associate their MAC address with the IP address of another device, leading to potential security breaches.
- **Diagram**:


How Address Resolution Protocol (ARP) Works
34.40.21.18
HOST
Requesting the MAC address of 34.40.21.20
ROUTER
Sending MAC address A5:22:98:5C:24:93
34.40.21.20
34.40.21.19

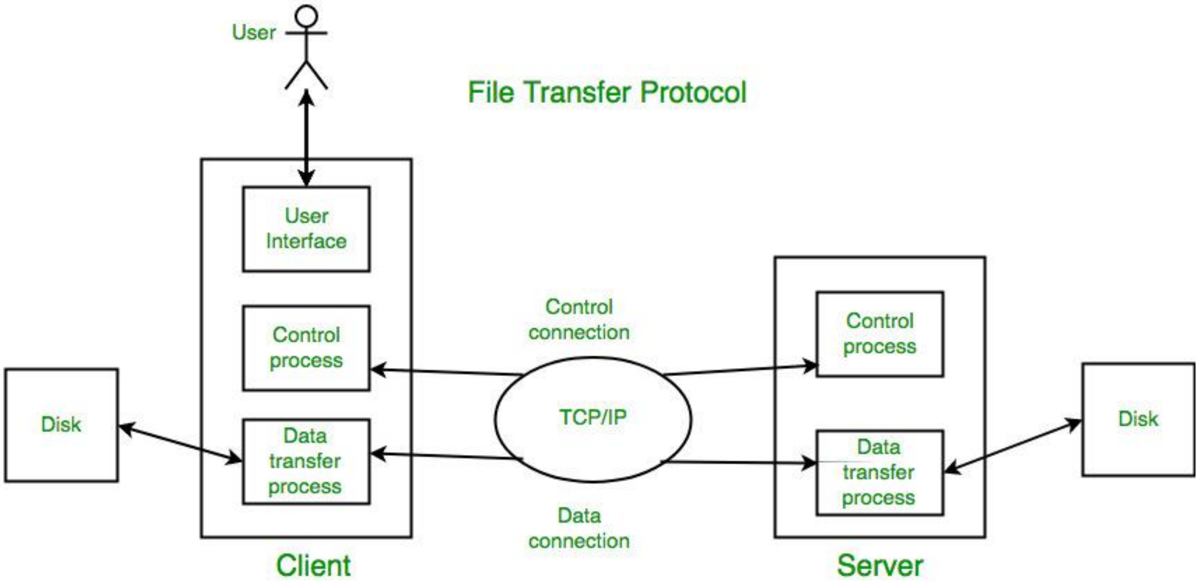
RARP (Reverse Address Resolution Protocol):

- **Function**: RARP is used to obtain an IP address when only the MAC address of a device is known. It allows a diskless workstation to discover its IP address from a RARP server on the network.
- **Advantages**:
- Useful for diskless workstations or devices without permanent storage to obtain their IP addresses dynamically.
- **Disadvantages**:
- Less commonly used compared to DHCP (Dynamic Host Configuration Protocol) for dynamic IP address assignment.
- **Diagram**:


My physical address is A46EA4578236, I am looking for my IP address.
Request
Host
RARP Server
RARP Request is Broadcast
Your IP address is 141.14.56.21
Reply
Host
RARP Server
RARP Reply is Unicast

FTP (File Transfer Protocol):

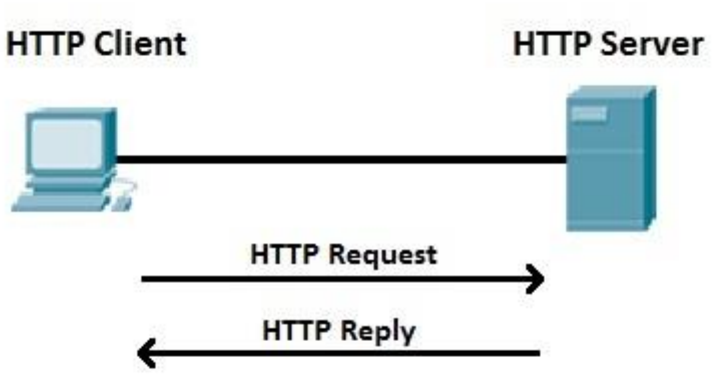
- **Function**: FTP is used to transfer files between a client and a server on a computer network. It allows users to upload, download, and manage files on remote servers.
- **Advantages**:
- Simple and widely supported protocol for file transfer.
- Provides authentication mechanisms for secure file transfer.
- **Disadvantages**:
- Transfers data in plaintext, making it vulnerable to eavesdropping and interception unless used with encryption (e.g., FTPS or SFTP).
- **Diagram**:



HTTP (Hypertext Transfer Protocol):

- **Function**: HTTP is the foundation of data communication on the World Wide Web. It is used to transmit hypertext documents, such as web pages, between web servers and web browsers.
- **Advantages**:

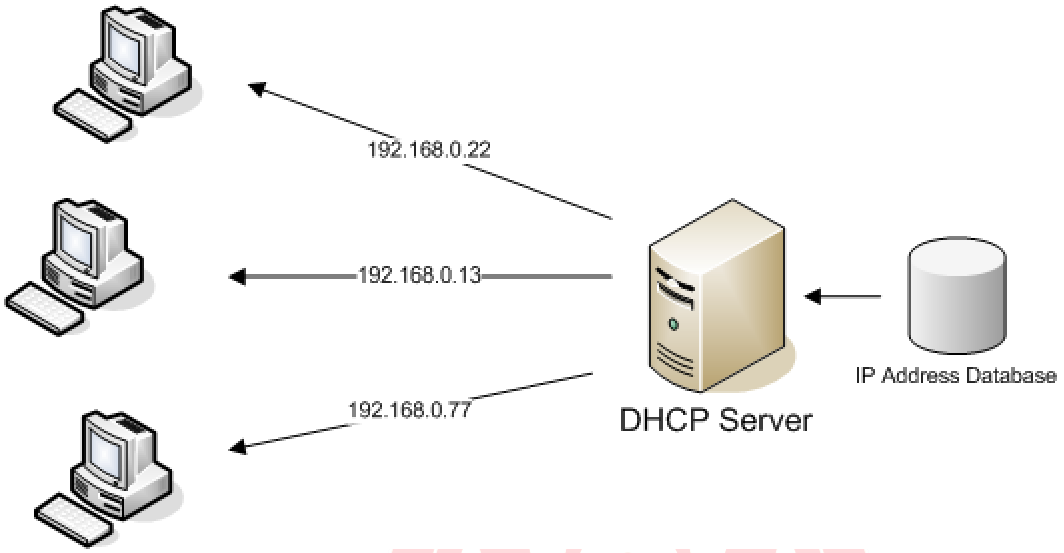
- Simple and flexible protocol for transferring text, images, videos, and other multimedia content over the internet.
- Supports stateless communication, allowing for scalability and efficient use of resources.
- **Disadvantages**:
- Lacks built-in security mechanisms, making it susceptible to various attacks, such as eavesdropping, man-in-the-middle, and cross-site scripting (XSS) attacks.
- **Diagram**:



DHCP Configuration (Dynamic Host Configuration Protocol):

- **Function**: DHCP is used to dynamically assign IP addresses and network configuration parameters to devices on a network. It automates the process of IP address allocation, subnet mask assignment, default gateway configuration, and DNS server assignment.
- **Advantages**:
- Simplifies network administration by centralizing and automating IP address management.
- Reduces the risk of IP address conflicts and configuration errors.
- **Disadvantages**:
- Single point of failure if the DHCP server becomes unavailable, potentially disrupting network connectivity.

- Vulnerable to rogue DHCP servers and DHCP spoofing attacks if proper security measures are not implemented.
- **Diagram**:



These diagrams and explanations illustrate the working, function, advantages, and disadvantages of ARP, RARP, FTP, HTTP, and DHCP configuration in computer networks.

Q12. Describe the classification of networks based on transmission technology.
Ans:
Networks can be classified based on the transmission technology they utilize. Here are the main classifications:

1. **Guided Transmission Media**:
  - Guided transmission media, also known as wired or bounded media, use physical cables or wires to transmit data signals. Examples include:
    - **Twisted Pair Cable**: Consists of pairs of insulated copper wires twisted together. Commonly used in Ethernet networks.
    - **Coaxial Cable**: Consists of a central conductor surrounded by a layer of insulation, a metallic shield, and an outer insulating layer. Used in cable television (CATV) and broadband internet connections.
    - **Fiber Optic Cable**: Uses optical fibers made of glass or plastic to transmit data signals using light pulses. Offers high bandwidth and is immune to electromagnetic interference. Used in high-speed internet connections and long-distance communication networks.

2. **Unguided Transmission Media**:
   - Unguided transmission media, also known as wireless or unbounded media, transmit data signals through the air using electromagnetic waves. Examples include:
     - **Radio Waves**: Used for wireless communication in Wi-Fi networks, Bluetooth devices, and cellular networks.
     - **Microwaves**: Utilized for point-to-point communication links in long-distance telephone networks and satellite communication systems.
     - **Infrared Waves**: Used for short-range communication in remote controls, wireless keyboards, and infrared data transfer between devices.

3. **Mixed Transmission Media**:
   - Some networks may use a combination of guided and unguided transmission media to meet specific requirements or overcome limitations. For example:
     - Hybrid Fiber-Coaxial (HFC) networks use a combination of fiber optic and coaxial cables to deliver high-speed internet and cable television services.
     - Wi-Fi networks may utilize both twisted pair cables for wired connections to access points and radio waves for wireless communication between devices.

These classifications based on transmission technology provide insights into the physical infrastructure and medium used to transmit data within a network. The choice of transmission technology depends on factors such as bandwidth requirements, distance, cost, and environmental considerations.

Q13. Describe working of DNS and SMTP protocols with suitable example.
Ans:
Sure, let's describe the working of DNS (Domain Name System) and SMTP (Simple Mail Transfer Protocol) protocols with suitable examples:

1. **Domain Name System (DNS)**:

   - **Working**: DNS is a hierarchical distributed naming system used to translate domain names (e.g., www.example.com) into IP addresses (e.g., 192.0.2.1) and vice versa. It operates on a client-server architecture, with DNS servers responsible for storing and managing domain name records.

   - **Example**:
     - Suppose a user wants to access a website by typing its domain name (e.g., www.example.com) into their web browser.
     - The user's device sends a DNS query to a DNS resolver (typically provided by the user's ISP or configured manually), requesting the IP address associated with the domain name.

- The DNS resolver forwards the query to a root DNS server, which refers the resolver to the appropriate top-level domain (TLD) server responsible for the domain name's extension (.com, .org, etc.).
- The TLD server then directs the resolver to the authoritative DNS server for the specific domain (e.g., example.com).
- The authoritative DNS server responds to the resolver with the IP address associated with the domain name.
- Finally, the resolver returns the IP address to the user's device, allowing it to establish a connection with the website's server.

2. **Simple Mail Transfer Protocol (SMTP)**:

- **Working**: SMTP is a protocol used for sending and receiving email messages between mail servers. It operates on a client-server model, with email clients (such as Outlook or Gmail) acting as SMTP clients and mail servers acting as SMTP servers.

- **Example**:
  - Suppose a user wants to send an email message to a friend.
  - The user's email client (SMTP client) composes the email message and specifies the recipient's email address (e.g., friend@example.com) and the sender's email address.
  - The SMTP client establishes a connection to the SMTP server responsible for the sender's domain (e.g., smtp.example.com).
  - The SMTP client sends the email message to the SMTP server, along with the recipient's email address and other necessary information.
  - The SMTP server performs domain name resolution to determine the IP address of the recipient's mail server.
  - The SMTP server establishes a connection to the recipient's mail server (SMTP server) and delivers the email message.
  - The recipient's mail server stores the email message in the recipient's mailbox, where it can be retrieved by the recipient's email client (e.g., Outlook or Gmail) later.

In summary, DNS translates domain names to IP addresses and vice versa, enabling users to access websites and other internet services using human-readable domain names. SMTP facilitates the transfer of email messages between mail servers, allowing users to send and receive emails across the internet.

Q14. Compare between OSI and TCP/IP model (any 8 points).
Ans:

Parameters	OSI Model	TCP/IP Model
Full Form	OSI stands for Open Systems Interconnection.	TCP/IP stands for Transmission Control Protocol/Internet Protocol.
Layers	It has 7 layers.	It has 4 layers.
Usage	It is low in usage.	It is mostly used.
Approach	It is vertically approached.	It is horizontally approached.
Delivery	Delivery of the package is guaranteed in OSI Model.	Delivery of the package is not guaranteed in TCP/IP Model.
Replacement	Replacement of tools and changes can easily be done in this model.	Replacing the tools is not easy as it is in OSI Model.
Reliability	It is less reliable than TCP/IP Model.	It is more reliable than OSI Model.
Encapsulation	Encapsulation in the OSI model involves adding headers and trailers at each layer as data moves down the protocol stack and removing them as data moves up.	Encapsulation in the TCP/IP model is similar but may involve fewer layers, as some functions are combined or omitted.
Complexity	The OSI model is more complex due to the higher number of layers and the strict separation of functions between layers.	The TCP/IP model is simpler and more streamlined, making it easier to implement and troubleshoot in practice.

Q15. Write a procedure for the following with its advantages and disadvantages:
1. To share a file 2. To share printer in network (device)
Ans:
Sure, here's a procedure for sharing a file and sharing a printer in a network, along with their advantages and disadvantages:

1. **Sharing a File**:

Procedure:
Step 1: Identify the file you want to share.
Step 2: Right-click on the file and select "Properties."
Step 3: In the properties window, navigate to the "Sharing" tab.
Step 4: Click on the "Advanced Sharing" button.
Step 5: Check the box that says "Share this folder."
Step 6: Optionally, you can set permissions to control who can access the shared file and what level of access they have (e.g., read-only or read/write).
Step 7: Click "OK" to apply the changes.

Advantages:
- Facilitates collaboration and teamwork by allowing multiple users to access and work on the same file simultaneously.
- Simplifies file management by centralizing storage and access control, reducing the need for multiple copies of the same file.

Disadvantages:
- Security risk if proper access controls and permissions are not configured, potentially exposing sensitive information to unauthorized users.
- Performance issues may arise if too many users access the shared file simultaneously, leading to slowdowns or file corruption.

2. **Sharing a Printer in the Network**:

Procedure:
Step 1: Connect the printer to a computer within the network.
Step 2: Go to "Control Panel" > "Devices and Printers."
Step 3: Right-click on the printer you want to share and select "Printer properties."
Step 4: Navigate to the "Sharing" tab.
Step 5: Check the box that says "Share this printer."
Step 6: Optionally, you can provide a share name for the printer to make it easier for other users to identify.
Step 7: Click "Apply" and then "OK" to save the changes.

Advantages:
- Enables multiple users within the network to print documents from a single printer, reducing the need for individual printers for each user.
- Improves resource utilization by allowing efficient sharing of printing resources across the network.

Disadvantages:
- Security risk if proper access controls and permissions are not configured, potentially allowing unauthorized users to print sensitive documents.
- Performance issues may arise if too many users send print jobs to the shared printer simultaneously, leading to delays or print queue congestion.

By following these procedures, users can easily share files and printers within a network, enabling efficient collaboration and resource utilization. However, it's essential to consider security and performance implications when sharing resources to mitigate potential risks and issues.

Q16. Describe the Host-to-Network layer protocols SLIP and PPP.
Ans:
SLIP (Serial Line Internet Protocol) and PPP (Point-to-Point Protocol) are both protocols used at the Host-to-Network layer (Layer 2) of the TCP/IP model for establishing communication between a computer (host) and a network. Here's a detailed description of each protocol:

1. **SLIP (Serial Line Internet Protocol)**:

- **Function**: SLIP is one of the earliest protocols used to transmit IP packets over serial connections, typically over telephone lines or serial cables. Its primary purpose is to encapsulate IP datagrams for transmission over point-to-point serial links.

- **Working**: SLIP operates by framing IP packets between special control characters, such as the SLIP END character (0xC0) to indicate the start and end of each packet. The SLIP protocol does not include error checking or correction mechanisms, making it a relatively simple and lightweight protocol.

- **Advantages**:
  - Simplicity: SLIP is straightforward and easy to implement, making it suitable for low-resource devices and environments with minimal processing power.
  - Widely Supported: SLIP was widely supported in early networking hardware and software, making it a popular choice for dial-up and serial connections in the early days of the internet.

- **Disadvantages**:

- Lack of Error Handling: SLIP does not include error detection or correction mechanisms, making it vulnerable to data corruption and transmission errors.
- Limited Functionality: SLIP lacks features such as authentication, compression, and multi-link support, limiting its usefulness in modern networking environments.

2. **PPP (Point-to-Point Protocol)**:

- **Function**: PPP is a more advanced and feature-rich protocol than SLIP, designed to establish and maintain connections between two nodes over various physical mediums, including serial links, DSL, and ISDN.

- **Working**: PPP provides a flexible and extensible frame format, allowing for the negotiation of options and parameters between endpoints. It supports features such as error detection, authentication, encryption, compression, and multi-protocol support (including IP, IPv6, and IPX).

- **Advantages**:
  - Reliability: PPP includes error detection and correction mechanisms, reducing the likelihood of data corruption during transmission.
  - Security: PPP supports various authentication methods, including Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP), enhancing security for network connections.
  - Flexibility: PPP supports multiple network layer protocols, allowing for the transmission of different types of traffic over the same physical link.

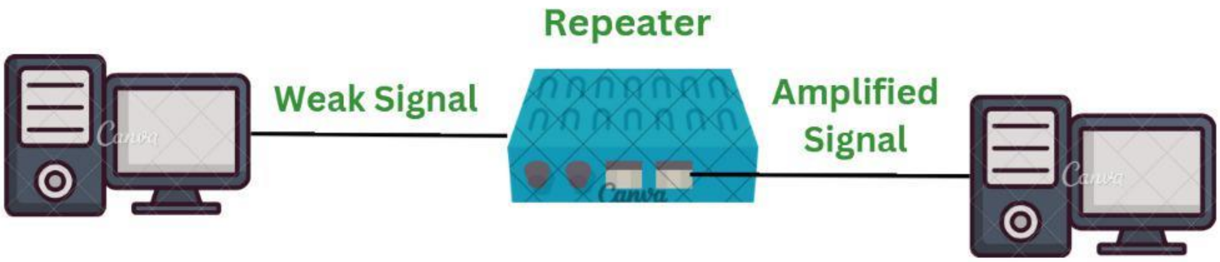
- **Disadvantages**:
  - Complexity: PPP is more complex than SLIP, requiring more processing power and memory resources for implementation.
  - Overhead: PPP headers and control information add overhead to transmitted packets, reducing the overall efficiency of the link, especially for low-speed connections.

In summary, SLIP and PPP are both Host-to-Network layer protocols used for communication over serial connections, with SLIP being simpler and PPP offering more advanced features and capabilities. While SLIP is suitable for basic connectivity in simple environments, PPP is more commonly used in modern networking applications due to its reliability, security, and flexibility.

Q17. Draw the neat labelled diagram of Repeater. State the situation under which repeater is necessary in Networks

Ans:

A repeater is a network device used to regenerate or amplify signals to extend the reach of a network segment. Here's a neat labeled diagram of a repeater:



In the diagram:
- The network segment is represented by the horizontal line.
- The repeater is depicted as a box in the middle of the network segment.

Situation under which a repeater is necessary in networks:

1. **Signal Degradation**: In large networks or over long distances, signals can degrade due to attenuation, resulting in reduced signal strength and increased noise. A repeater can regenerate the signal, amplifying it to compensate for losses and extending the reach of the network.

2. **Length Limitations**: Some network technologies have limitations on the maximum length of the network segment. For example, in Ethernet networks using twisted-pair cables, the maximum cable length is typically 100 meters. A repeater can be used to extend the network beyond this limit by regenerating the signal.

3. **Multiple Segments**: In networks with multiple segments connected by cables or fiber optic links, repeaters can be used to interconnect these segments and extend the overall network coverage.

4. **Interference**: Signal interference from external sources or electromagnetic interference (EMI) within the network environment can degrade signal quality. A repeater can amplify the signal to overcome interference and maintain reliable communication.

5. **Topology Expansion**: When expanding or scaling a network, repeaters can be deployed to bridge gaps between existing network segments or to connect new network devices located beyond the reach of existing infrastructure.

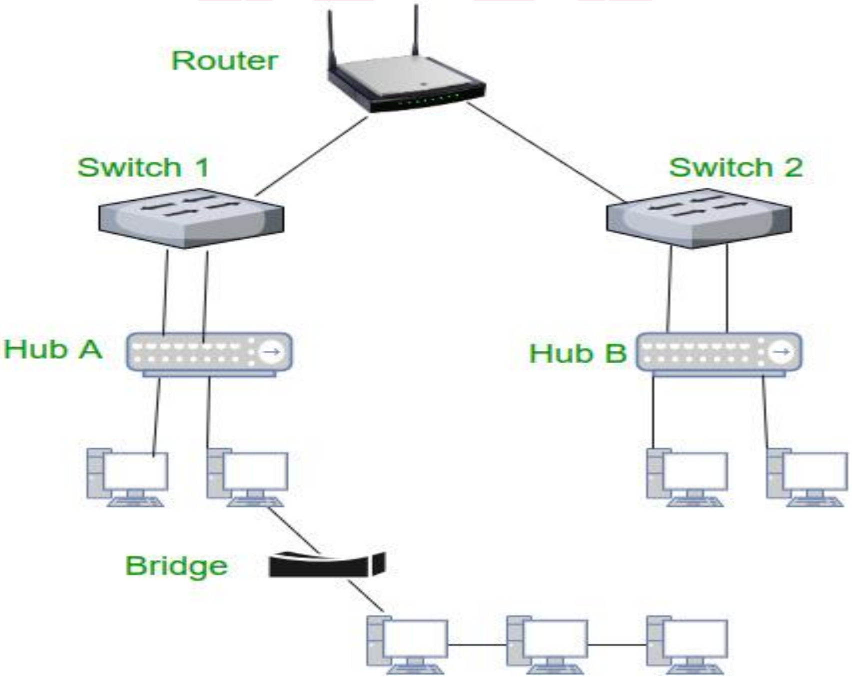
Overall, a repeater is necessary in networks to overcome signal degradation, extend network reach, interconnect multiple segments, overcome interference, and facilitate network expansion.

Q18. Comparison between HUB, Switch, Router, Bridge. (diagram). (8 points)
Ans:

Parameters	HUB	Switch	Router	Bridge
Function	A hub is a basic networking device that connects multiple devices in a network and broadcasts data to all connected devices.	A switch is a more intelligent device that forwards data only to the specific device intended to receive it, improving network efficiency.	A router is a networking device that forwards data packets between computer networks, typically between LANs and the internet.	A bridge connects multiple network segments and forwards data between them, improving overall network performance.
Addressing	Operates at the physical layer and does not understand MAC addresses.	Operates at the data link layer and uses MAC addresses to forward data to specific devices.	Operates at the network layer and uses IP addresses to route data between different networks.	Operates at the data link layer and uses MAC addresses to forward data between network segments.
Broadcasting	Broadcasts data to all connected devices, leading to network congestion and reduced efficiency.	Only broadcasts data to the intended recipient, reducing network congestion and improving efficiency.	Does not broadcast data but forwards packets based on destination IP addresses.	Broadcasts data within the network segment but does not broadcast between segments.
Collision Domain	Forms a single collision domain, where collisions can occur between devices connected to the hub.	Forms multiple collision domains, isolating traffic between individual devices and reducing collisions.	Does not form collision domains as it operates at the network layer and forwards packets between networks.	Forms multiple collision domains between connected segments, reducing collisions within each segment.
Security	Provides no security features and is susceptible to eavesdropping attacks.	Provides some level of security by isolating traffic between devices, but can still be	Provides network segmentation and firewall capabilities, enhancing network security.	Provides segmentation between network segments but offers limited security

		vulnerable to MAC address spoofing.		features compared to routers.
Scalability	Limited scalability due to single collision domain and broadcast domain.	More scalable than hubs due to multiple collision domains and ability to segment traffic.	Highly scalable as it can connect multiple networks and route traffic between them.	Limited scalability compared to routers but can still be used to connect multiple network segments.
Cost	Generally the least expensive networking device.	Moderate cost, depending on the number of ports and features.	Moderate to high cost, depending on features such as routing protocols and security.	Similar cost to switches, depending on features and capabilities.
Deployment	Typically used in small networks or for temporary connectivity needs.	Commonly used in medium to large networks for efficient data transfer.	Essential for connecting networks to the internet and routing traffic between LANs.	Used to connect network segments within a single LAN or to extend network coverage.

Diagram:



Q19. Define the following: (i) client (ii) server (iii) peer (iv) protocol
Ans:

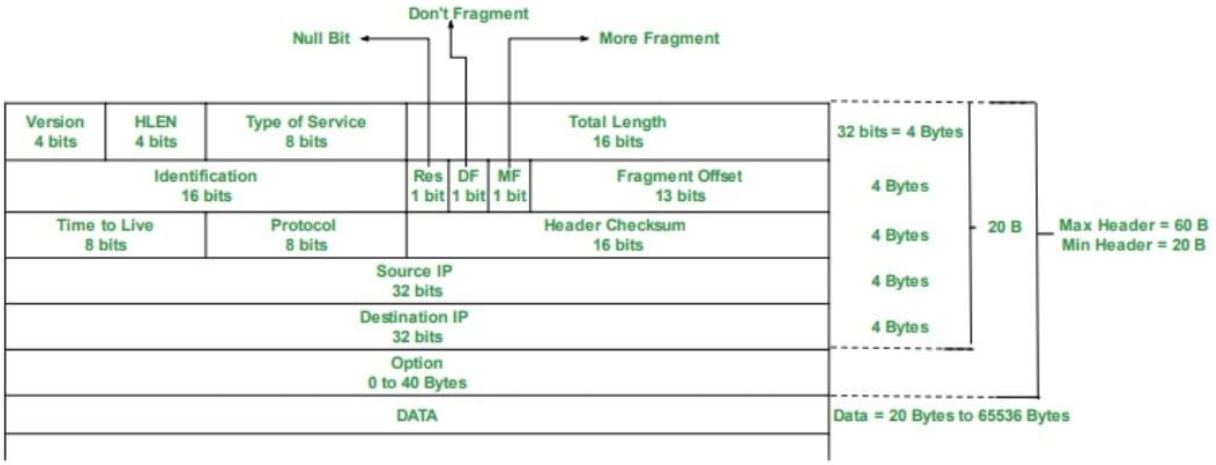
(i) **Client**: A client refers to a computer or device that requests services or resources from another computer or server in a network. In client-server architecture, the client initiates communication by sending requests to the server and receives responses in return. Clients can be software applications, such as web browsers, email clients, or file transfer programs, that interact with servers to access data, files, or services.

(ii) **Server**: A server is a computer or device that provides services, resources, or data to other computers or clients in a network. Servers typically run specialized software applications or server operating systems to respond to client requests. Examples of server types include web servers, email servers, file servers, and database servers. Servers listen for incoming requests from clients, process these requests, and send back appropriate responses.

(iii) **Peer**: A peer refers to any device or entity participating in a peer-to-peer (P2P) network, where all devices have equal privileges and responsibilities. Unlike client-server architecture, where roles are clearly defined (client requests, server responds), peers in a P2P network both request and provide resources or services to each other. Peers can be computers, smartphones, tablets, or any other device connected to the network, and they communicate directly with each other without the need for a centralized server.

(iv) **Protocol**: A protocol is a set of rules, standards, or conventions that govern the communication and interaction between devices or entities in a network. Protocols define the format, sequence, and timing of data exchange, as well as error handling and security mechanisms. Common examples of protocols include TCP/IP (Transmission Control Protocol/Internet Protocol), HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), and FTP (File Transfer Protocol). Protocols ensure interoperability and enable devices and systems from different vendors to communicate effectively over a network.

Q20. Draw IPv6 and IPv4 Frame Format. (message)
Ans:



VERSION: Version of the IP protocol (4 bits), which is 4 for IPv4

HLEN: IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.

Type of service: Low Delay, High Throughput, Reliability (8 bits)

Total Length: Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.

Identification: Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)

Flags: 3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)

Fragment Offset: Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.

Time to live: Datagram's lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.

Protocol: Name of the protocol to which the data is to be passed (8 bits)

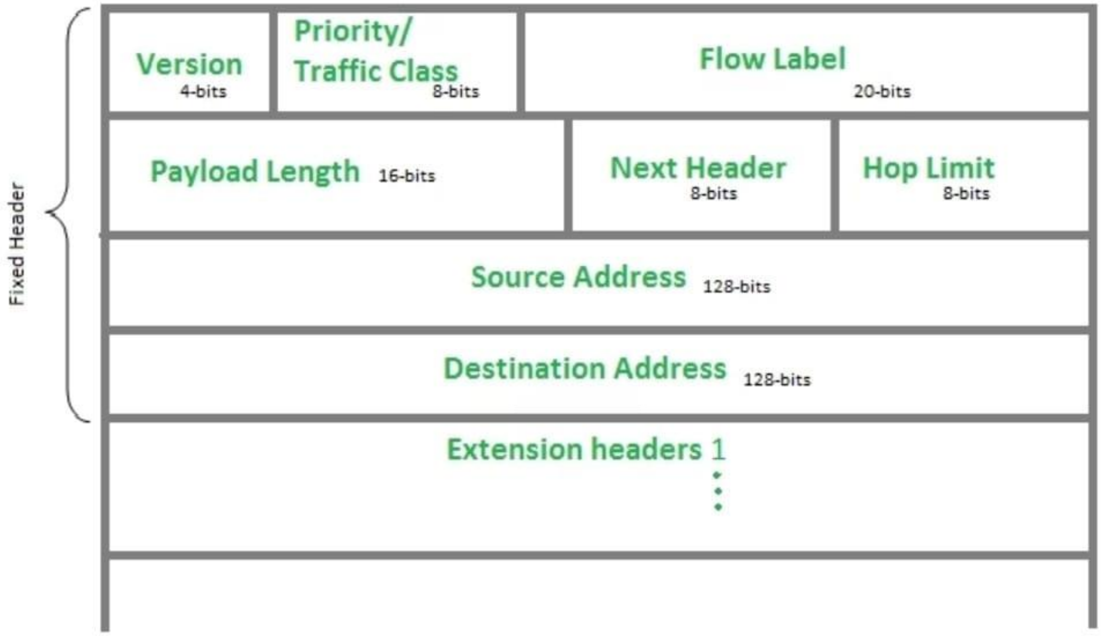
Header Checksum: 16 bits header checksum for checking errors in the datagram header

Source IP address: 32 bits IP address of the sender

Destination IP address: 32 bits IP address of the receiver

Option: Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.

IP version 6 Header Format :



Address is the 128-bit IPv6 address of the original source of the packet.

Destination Address (128-bits): The destination Address field indicates the IPv6 address of the final destination(in most cases). All the intermediate nodes can use this information in order to correctly route the packet.

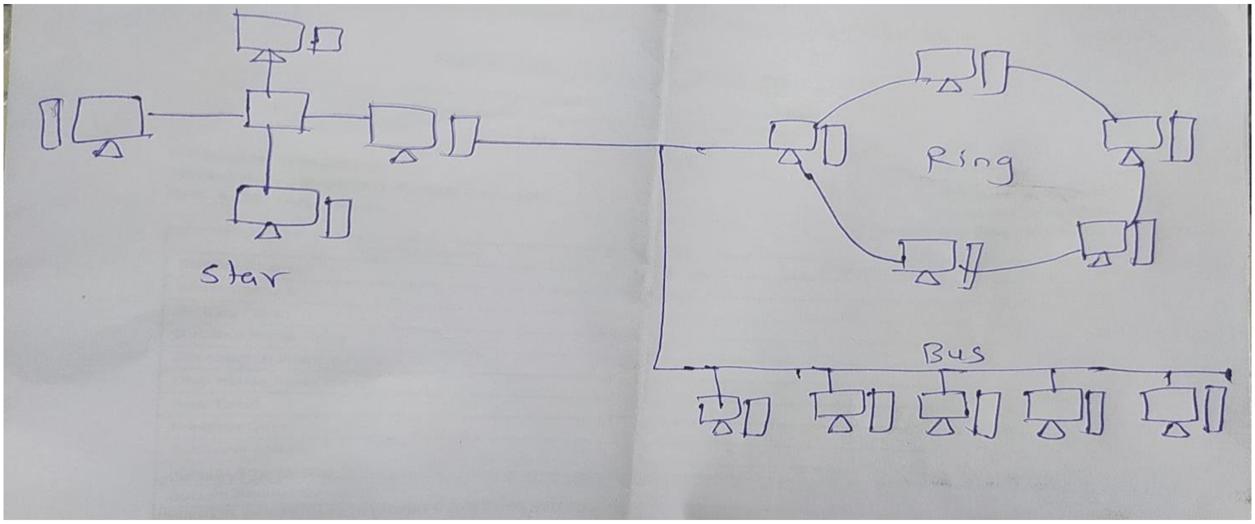
Extension Headers: In order to rectify the limitations of the IPv4 Option Field, Extension Headers are introduced in IP version 6. The extension header mechanism is a very important part of the IPv6 architecture. The next Header field of IPv6 fixed header points to the first Extension Header and this first extension header points to the second extension header and so on.

Q21. A small educational organization situated within a single building want to create a network to share the information of its 5 departments among them, for this network no centralized management is required, also no security is required. Which network is suitable for such organization? Justify

For a small educational organization with 5 departments situated in a single building and no centralized management or security requirements, a **peer-to-peer (P2P) network** is a suitable choice for sharing information among departments. Here's a brief explanation:

- **Decentralized Management**: A P2P network allows each computer (or node) to communicate directly with others without relying on a central server. This setup aligns with the organization's need for no centralized management.
- **Simplicity and Cost-Effectiveness**: P2P networks are easy to set up and maintain, making them suitable for small organizations with limited resources. They don't require specialized network infrastructure or dedicated servers, which keeps costs low.
- **Flexibility**: In a P2P network, each computer can share information directly with others, providing flexibility in connectivity and resource sharing among departments.
- **No Security Requirements**: Since security isn't a priority for this organization, a P2P network can suffice for basic information sharing. However, it's essential to note that P2P networks typically lack robust security features compared to other architectures.

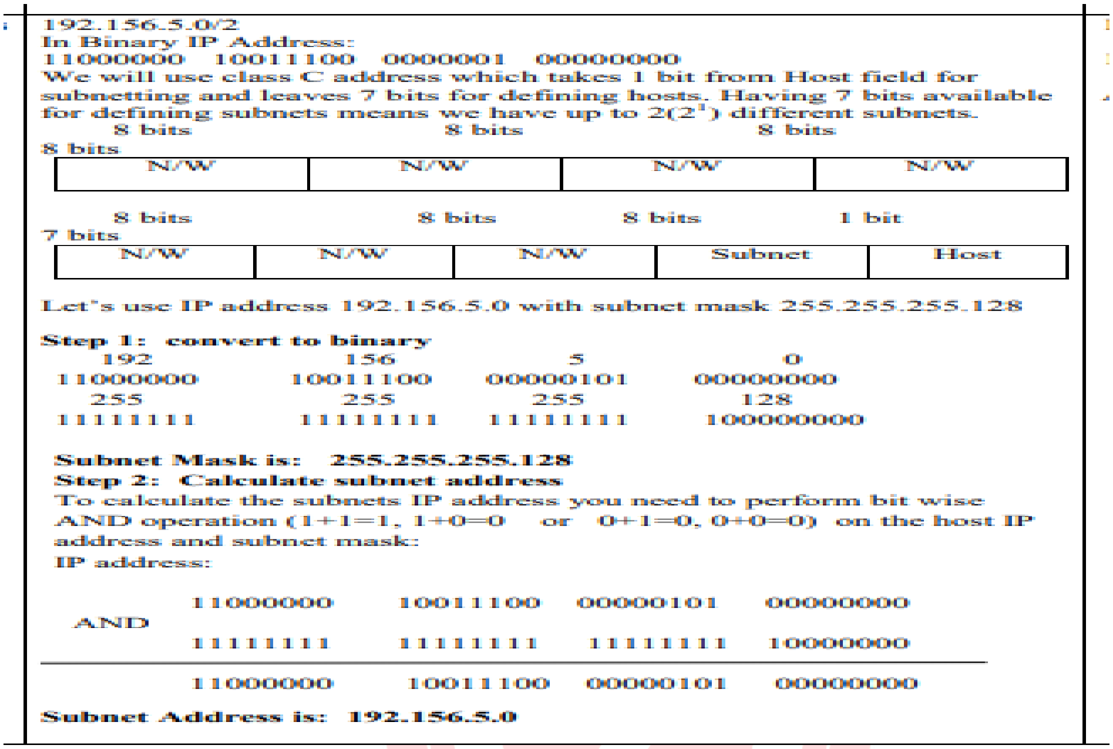
Q22. Draw a neat labelled sketch of hybrid topology connecting one star network of 4 computers, one ring network of 5 computers and one bus network of 5 computers.



Q23. Identify class for following IP address and Justify it : (i) 10.145.14.68 (ii) 222.255.254.253 (iii) 191.168.0.1 (iv) 224.0.0.0

- (i) 10.145.14.68 is Class A
- (ii) 222.255.254.253 is Class C
- (iii) 191.168.0.1 is Class B
- (iv) 224.0.0.0 is a multicast address class D

Q24. Design a Class 'C' Network with network address 192.156.5.0 with 2 subnets. State the subnet mask and subnet address.



192.156.5.0/2

In Binary IP Address:

11000000 10011100 0000001 00000000

We will use class C address which takes 1 bit from Host field for subnetting and leaves 7 bits for defining hosts. Having 7 bits available for defining subnets means we have up to $2(2^1)$ different subnets.

8 bits	8 bits	8 bits	8 bits
N/W	N/W	N/W	N/W

8 bits	8 bits	8 bits	1 bit	7 bits
N/W	N/W	N/W	Subnet	Host

Let's use IP address 192.156.5.0 with subnet mask 255.255.255.128

Step 1: convert to binary

192	156	5	0
11000000	10011100	00000101	00000000
255	255	255	128
11111111	11111111	11111111	100000000

Subnet Mask is: 255.255.255.128

Step 2: Calculate subnet address

To calculate the subnets IP address you need to perform bit wise AND operation (1+1=1, 1+0=0 or 0+1=0, 0+0=0) on the host IP address and subnet mask:

IP address:

```
          11000000    10011100   00000101    00000000
   AND
          11111111    11111111   11111111    10000000
---------------------------------------------------------
          11000000    10011100   00000101    00000000
```

Subnet Address is: 192.156.5.0

Q25. Draw a suitable network layout using Mesh topology to connect 8 computers. How many links are required. What are the advantages and disadvantages of this network ?

In a Mesh topology, the number of links required to connect n devices is calculated using the formula:
Number of links=n(n−1)/2

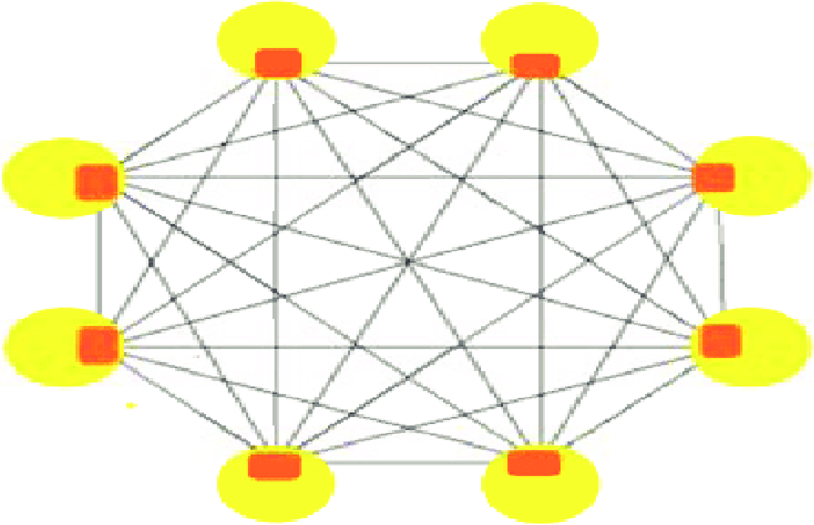
For 8 computers:
Number of links=8(8−1)/2=8(7)/2=28
Number of links=28

Therefore, 28 links are required to connect 8 computers in a Mesh topology.

Advantages of Mesh Topology:
1. Fault Tolerance: Mesh topology offers high redundancy. If one link fails, there are alternative paths available between nodes, ensuring reliability and fault tolerance.
2. High Scalability: It's easy to scale a Mesh network by adding more devices without affecting the overall network performance.
3. Point-to-Point Communication: Each connection is point-to-point, allowing efficient data transfer and reducing congestion.

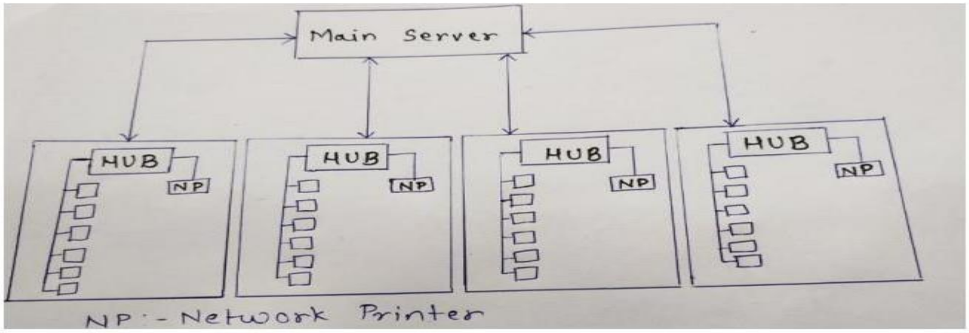
Disadvantages of Mesh Topology:

1. High Cost: Mesh networks require a large number of physical links, which can be costly to implement and maintain.
2. Complexity: As the number of devices increases, managing and configuring a Mesh network can become complex due to the large number of connections.
3. Resource Intensive: Setting up and maintaining a fully connected Mesh network can be resource-intensive in terms of hardware (cables, ports) and management (configuration, monitoring).



Instead if circle you draw computers (each computer connects to each other

Q26. Design suitable network layout for an organization with four departments (6 users each), shared print server, & network server.



NP :- Network Printer

Q27. Elaborate the procedure to divide networks into subnets. Divide given network address in four equal part to hold maximum 50 devices in each subnet. IP address 192.168.14.14/25.

answer=➔

Step 1: Understand the Current Network and Subnet Mask

The IP address given is 192.168.14.14 with a subnet mask of /25.

This means the first 25 bits of the IP address are used for network identification, leaving 32 - 25 = 7 bits for host identification within the subnet.

Step 2: Determine Required Subnet Size

For 50 devices, you'll need at least 6 host bits (2^6 - 2 = 62 usable addresses, considering subnet and broadcast addresses).

Step 3: Determine New Subnet Mask To have 6 host bits per subnet (for ~62 addresses/subnet):

- The new subnet mask will be /25 (original) + 6 (additional bits) = /31

Step 4: Divide the Network

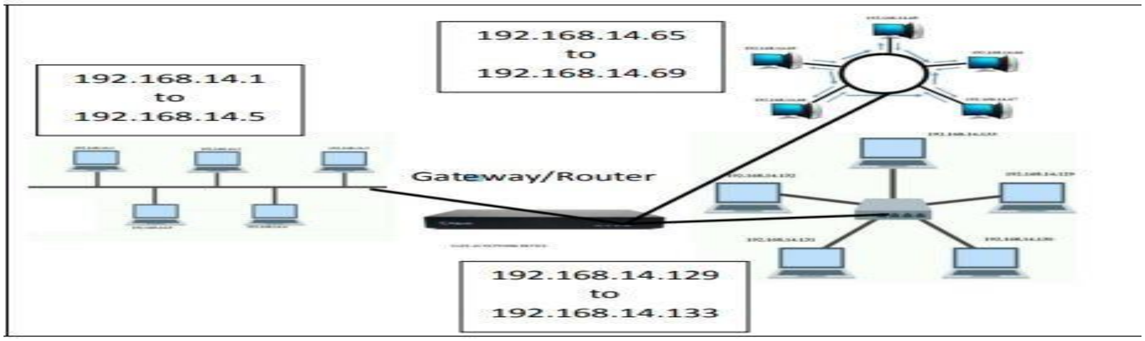
1. **Calculate New Subnet Mask**: The new subnet mask will be /31 (32 bits total: 25 network bits + 6 host bits)

2. **Calculate Subnet Size**:

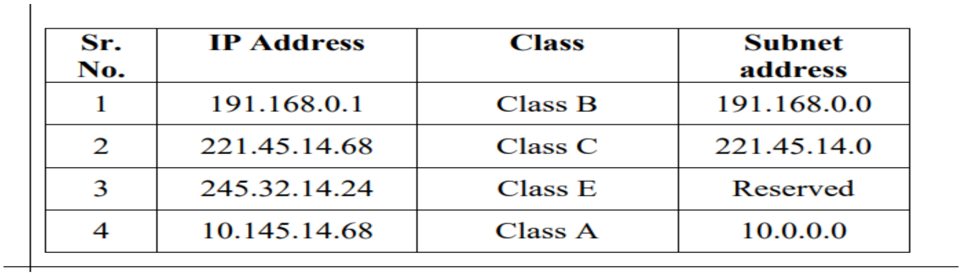
- With a /31 subnet mask, each subnet will have 2^(32 - 31) = 2 IP addresses (1 for network ID, 1 for broadcast), but that's too small. The next step may involve trying a /30

Q28. Design a network with 15 host divided into 3 equal size sub-networks each with different network topology. i.e. bus, star and ring. Connect these subnetworks with suitable network device. Specify IP address to each subnetwork with its Broadcast and Network address.

List of available IP Address, Broadcast and Network Address: Name of Topology Network Address Broadcast Address: Usable Host Range BUS 192.168.14.0 192.168.14.63 192.168.14.1 - 192.168.14.5 RING 192.168.14.64 192.168.14.127 192.168.14.65 - 192.168.14.69 STAR 192.168.14.128 192.168.14.191 192.168.14.129 - 192.168.14.133

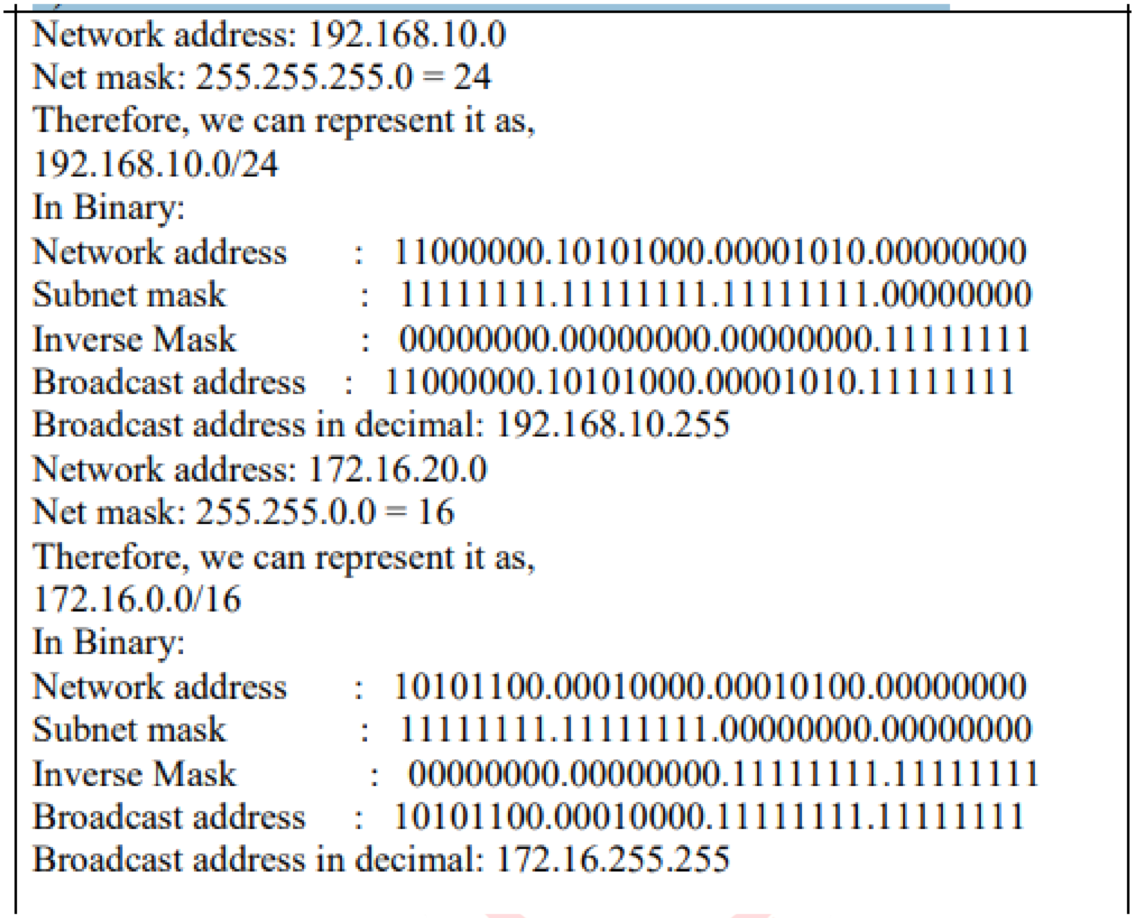


Q29. Give class & subnet address for following IP address : (i) 191.168.0.1 (ii) 221.45.14.68 (iii) 245.32.14.24 (iv) 10.145.14.68



Sr. No.	IP Address	Class	Subnet address
1	191.168.0.1	Class B	191.168.0.0
2	221.45.14.68	Class C	221.45.14.0
3	245.32.14.24	Class E	Reserved
4	10.145.14.68	Class A	10.0.0.0

Q30. Calculate broadcast address for the following: i) Network of class 'C' with network address 192.168.10.0 ii) Network of class 'B' with network address 172.16.20.0



Network address: 192.168.10.0

Net mask: 255.255.255.0 = 24

Therefore, we can represent it as,

192.168.10.0/24

In Binary:

Network address : 11000000.10101000.00001010.00000000

Subnet mask : 11111111.11111111.11111111.00000000

Inverse Mask : 00000000.00000000.00000000.11111111

Broadcast address : 11000000.10101000.00001010.11111111

Broadcast address in decimal: 192.168.10.255

Network address: 172.16.20.0

Net mask: 255.255.0.0 = 16

Therefore, we can represent it as,

172.16.0.0/16

In Binary:

Network address : 10101100.00010000.00010100.00000000

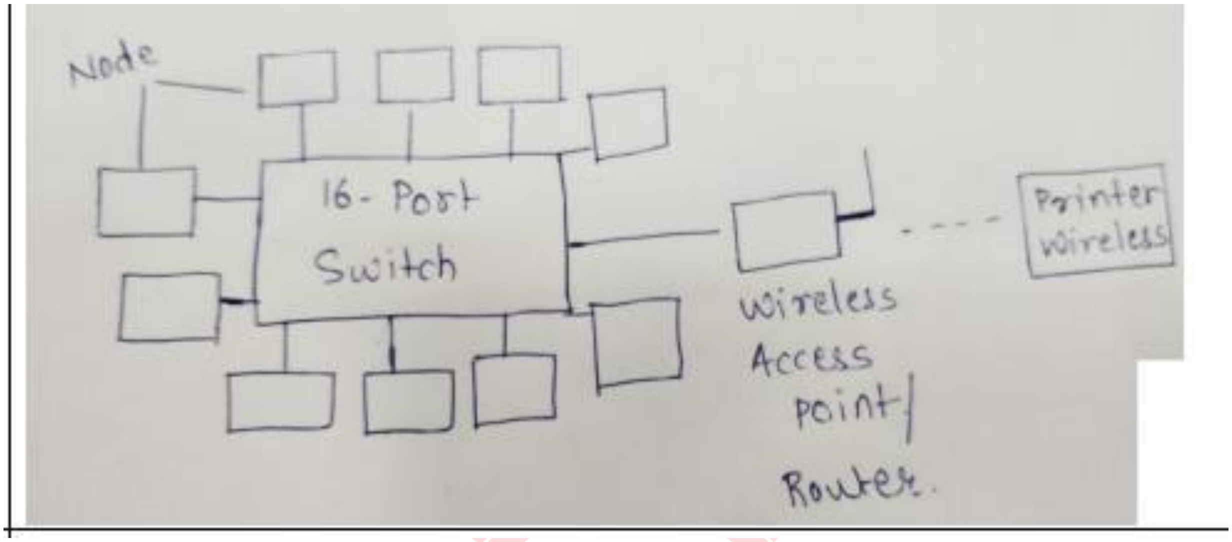
Subnet mask : 11111111.11111111.00000000.00000000

Inverse Mask : 00000000.00000000.11111111.11111111

Broadcast address : 10101100.00010000.11111111.11111111

Broadcast address in decimal: 172.16.255.255

Q31. Draw Suitable network layout with star topology for a computer lab with 10 hosts and a wireless printer. List all components in the layout.


Node
16- Port
Switch
Wireless
Access
point/
Router.
Printer
Wireless