Give difference between following:

(a) Classification of classes in Binary notation and Dotted Decimal notation

Feature	Binary Notation	Dotted Decimal Notation
Representation	32 bits in binary form	Four decimal numbers separated by periods
Readability	More suitable for computer-based processing and calculations	Easier for humans to read and remember
Usage	Often used in network programming, subnetting, and other technical operations	Used for general IP address representation in everyday contexts
Classification of Classes	Uses the first byte of the IP address to classify the address into one of five classes	Uses the first byte of the IP address to classify the address into one of five classes
Efficiency	More efficient	Less efficient
Human-Readability	Less human-readable	More human-readable

(b) Functions of transport layer and data link layer

Feature	Transport Layer	Data Link Layer
Responsibility	End-to-end communication	Framing, physical addressing, medium access control, error detection and correction, flow control within a link, and reliable delivery within a single hop
Services	Error checking, flow control, multiplexing, segmentation and reassembly, connection establishment and termination	Error detection and correction, flow control, framing, physical addressing

Protocols	TCP, UDP	Ethernet, Wi-Fi
Scope	Across multiple networks	Within a single network

(c)Overlay networks and frame relay networks.

Feature	Overlay Network	Frame Relay Network
Purpose	Create a virtual network on top of an existing physical network	Provide a reliable and efficient way to transmit data between two points
Architecture	Software-based	Hardware-based
Performance	Can provide better performance for applications that require low latency or high bandwidth	Typically provides lower performance than overlay networks
Security	Can provide better security by creating isolated virtual networks	Typically provides lower security than overlay networks
Cost	Can be more expensive than frame relay networks	Typically less expensive than overlay networks

(d)Star and Mesh Topologies

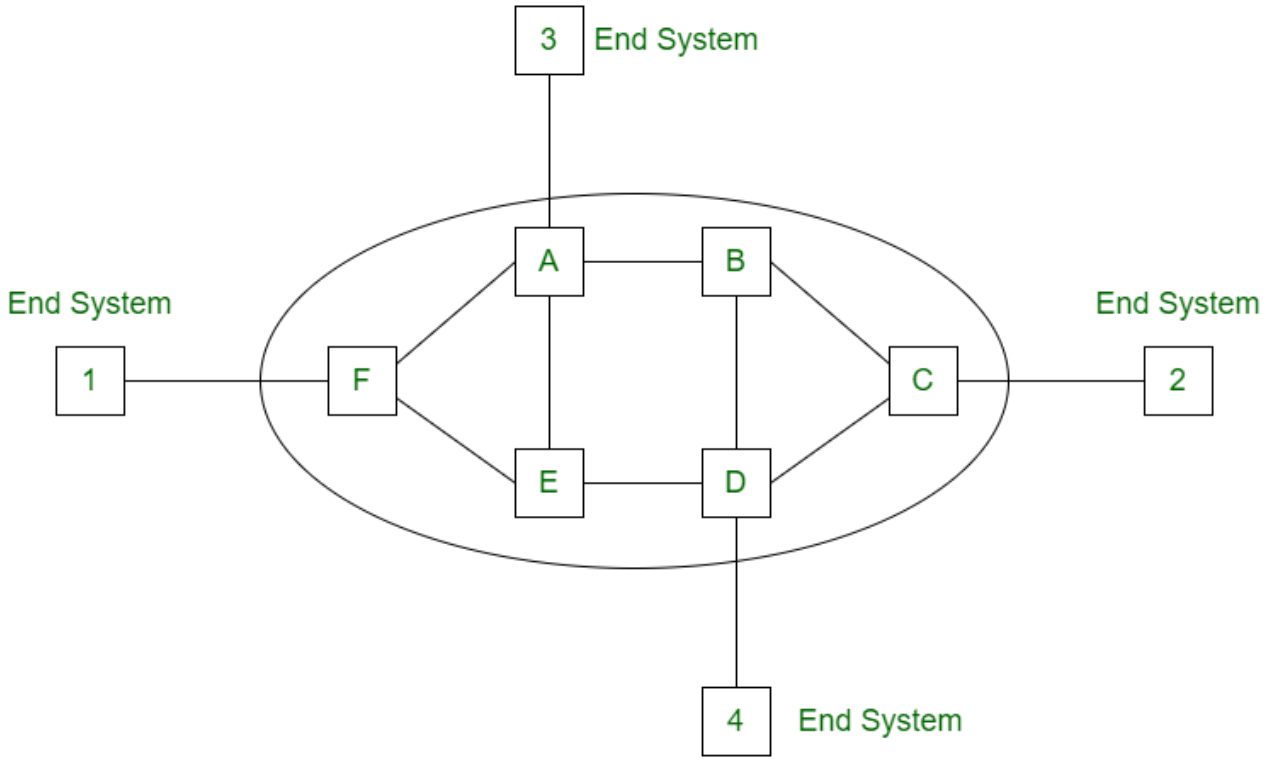
Feature	Star Topology	Mesh Topology
Connection	Devices are connected to a central hub or switch.	Devices are connected to each other.
Fault tolerance	Fault tolerant, as the failure of one device will not affect the rest of the network.	More fault tolerant than star topology, as there are multiple paths for data to travel between any two devices.
Scalability	Easy to scale, as new devices can be added by connecting them to the hub or switch.	More difficult to scale, as new connections must be made between all devices in the network.

Cost	More expensive, as each device must be connected to the hub or switch.	Less expensive, as devices do not need to be connected to a central hub or switch.

Compare coaxial cable, FOX, microwave and Infra-'Red with respect to frequency range and application.

Medium	Frequency Range	Application
Coaxial cable	50 MHz to 1 GHz	Cable television, computer networking, and high-definition television
FOX	2 GHz to 10 GHz	Microwave ovens, satellite television, and point-to-point communications
Microwave	300 MHz to 300 GHz	Cellular networks, radar, and satellite communications
Infrared	300 GHz to 400 THz	Remote controls, night vision, and medical imaging

Draw labelled diagram of virtual circuit network and describe working.



Working of Virtual Circuit:

- In the first step a medium is set up between the two end nodes.
- Resources are reserved for the transmission of packets.
- Then a signal is sent to sender to tell the medium is set up and transmission can be started.
- It ensures the transmission of all packets.
- A global header is used in the first packet of the connection.
- Whenever data is to be transmitted a new connection is set up.

Differentiate between repeater, amplifier, bridge, router, hub, switch and gateway. Clearly identify the position of each of the element in OSI layer protocol.

Device	Description	OSI Layer
Repeater	A device that amplifies and regenerates signals, extending the range of a network.	Physical layer
Amplifier	A device that increases the power of a signal, improving its quality.	Physical layer
Bridge	A device that connects two networks that use the same protocol.	Data link layer
Router	A device that connects two networks that use different protocols.	Network layer
Hub	A device that connects multiple devices on the same network.	Physical layer
Switch	A device that connects multiple devices on the same network, filtering and forwarding traffic based on MAC addresses.	Data link layer
Gateway	A device that connects two networks that use different protocols and technologies.	Application layer

Describe the IPV4 classful addressing scheme. Find the class of the following IP Addresses. (i) 10000000 11110000 11111111 00110011 (ii) 117.28.32.16

https://www.youtube.com/watch?v=VkgfyLf1raY

Draw ARP and RARP header and explain its working with example. Is the size of the ARP packet is fixed? Explain.

ARP Packet

Hardware Type		Protocol Type
Hardware length	Protocol length	Operation Request 1, Reply 2
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled in a request)		
Target protocol address (For example, 4 bytes for IP)		

RARP Packet

Hardware type		Protocol type
Hardware length	Protocol length	Operation Request 3, Reply 4
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP) (It is not filled for request)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled for request)		
Target protocol address (For example, 4 bytes for IP) (It is not filled for request)		

Working of ARP with example:

1. Host A wants to send a packet to Host B.
2. Host A does not know the MAC address of Host B, so it sends an ARP request packet to the local network.
3. The ARP request packet contains Host A's IP address and hardware address.
4. Host B receives the ARP request packet and responds with an ARP reply packet.
5. The ARP reply packet contains Host B's IP address and hardware address.
6. Host A now knows the MAC address of Host B, so it can send the packet to Host B.

Working of RARP with example

- A device boots up and does not know its own IP address.
- The device broadcasts a RARP request packet containing its MAC address.
- A RARP server that is listening on the network receives the request packet.
- The RARP server looks up the MAC address in its database and finds the corresponding IP address.
- The RARP server sends a RARP reply packet containing the IP address to the device.
- The device now knows its own IP address.

The size of an ARP packet is fixed at 28 bytes.

- The ARP header is a standard format that is used by all devices on an Ethernet network.
- The size of the fields in the ARP header is fixed, so the size of the ARP packet is also fixed.
- This allows for efficient communication between devices on an Ethernet network and ensures that all devices are using the same format for ARP packets.

Differentiate between Connection less and connection oriented operations in computer network

Feature	Connectionless	Connection-oriented
Establishment of connection	No connection is established before sending data.	A connection is established before sending data.
Delivery of data	Data is sent as individual packets.	Data is sent as a stream of data.

Reliability	Not reliable. Packets may be lost, duplicated, or delivered out of order.	Reliable. Packets are guaranteed to be delivered in the correct order.
Flow control	No flow control. Sender can send as many packets as it wants.	Flow control is used to ensure that the sender does not send too many packets at once.
Error detection	Error detection is not performed.	Error detection is performed. If a packet is received with errors, it is discarded.
Example protocols	UDP, IP, ICMP	TCP, HTTP, FTP

Differentiate between Link-State routing and Distance-Vector routing.

Feature	Link-State Routing	Distance-Vector Routing
Information sharing	Routers share information about their neighbors and the entire network topology.	Routers share information about their neighbors and the distance to each neighbor.
Convergence time	Fast convergence.	Slow convergence.
Scalability	Scalable to large networks.	Not as scalable to large networks.
Robustness	Robust to network changes.	Not as robust to network changes.
Complexity	More complex.	Less complex.

Explain following in brief and discuss their frame format and control field

(a) PPP (b) HDLC (c) SONET

(a) **PPP (Point-to-Point Protocol)**

- PPP is a data link layer protocol that is used to establish, configure, and manage point-to-point links between two devices.
- PPP **frames** are composed of the following fields:

- Flag: Marks the beginning and end of a PPP frame.
- Address: Specifies the address of the sender and receiver of the frame.
- Control: Indicates the type of frame and the actions that the receiver should take.
- Protocol: Identifies the network layer protocol that is carried in the frame.
- Data: Carries the data that is being transmitted between the two devices.
- Frame check sequence (FCS): Used to detect errors in the frame.
- The **control field** in a PPP frame is 1 byte long and can be one of the following types:
- Asynchronous Control Character (AC): Used to control the flow of data between the two devices.
- Protocol Identification (PID): Indicates the network layer protocol that is carried in the frame.
- Link Control Protocol (LCP): Used to negotiate the parameters of the PPP link.
- Authentication Protocol (CHAP): Used to authenticate the two devices.
- Network Control Protocol (NCP): Used to configure the network layer protocols that will be used on the link.

(b) **HDLC (High-Level Data Link Control)**

- HDLC is a bit-oriented data link layer protocol that is used to establish, maintain, and manage point-to-point links between two devices.
- HDLC **frames** are composed of the following fields:
- Flag: Marks the beginning and end of an HDLC frame.
- Address: Specifies the address of the sender and receiver of the frame.
- Control: Indicates the type of frame and the actions that the receiver should take.
- Information: Carries the data that is being transmitted between the two devices.
- Frame check sequence (FCS): Used to detect errors in the frame.
- The **control field** in an HDLC frame is 1 or 2 bytes long and can be one of the following types:
- I-frame: Carries data.
- S-frame: Used for control purposes, such as flow control and error notification.
- U-frame: Used for miscellaneous purposes, such as testing and debugging.

(c) **SONET (Synchronous Optical Network)**

- SONET is a synchronous optical networking standard that is used to transmit data over optical fibers.
- SONET **frames** are composed of the following fields:
- Header: Contains the frame's control information, such as the source and destination addresses, the frame type, and the frame's length.
- Data: Carries the data that is being transmitted between the two devices.
- Trailer: Contains the frame's error-checking information.
- The header and trailer of a SONET frame are both 9 bytes long. The data field can be up to 8192 bytes long.

Why sub-netting and super-netting is needed while designing the network and assigning the internet addresses? Explain with example.

Feature	Subnetting	Supernetting
Purpose	Divides an IP address space into smaller subnetworks	Combines multiple IP address spaces into a larger network
How it works	Borrows bits from the host portion of the IP address to create the subnet mask	Borrows bits from the network portion of the IP address to create the supernet mask
Benefits	Improves the efficiency of IP address allocation and routing, reduces the size of routing tables	Reduces the size of routing tables, simplifies network administration
Drawbacks	Can be complex to implement and manage	Can be difficult to troubleshoot

Example

- A company with 100 employees might use subnetting to divide its IP address space into 20 subnetworks, each with 5 IP addresses. This would allow the company to assign a unique IP address to each employee's computer.
- A university with multiple campuses might use supernetting to combine the IP address spaces of all of its campuses into a single larger network. This would simplify the routing configuration for the university and reduce the size of its routing tables.

Discuss the principle of Stop and Wait flow control algorithm. Draw time line diagram and explain how the loss of data frame and loss of acknowledge frame is handled. Also discuss the effect of dealy bandwidth product on link utilization.

Stop and Wait is a simple flow control protocol that is used to ensure that data is not lost or corrupted in transit. It works by having the sender send a single frame of data, and then waiting for an acknowledgement from the receiver before sending the next frame. If the acknowledgement is not received, the sender will resend the frame.

Time	Sender	Receiver
0	Send frame 1	-
1	Wait for acknowledge	-
2	No acknowledge received	-
3	Resend frame 1	-
4	Acknowledge received	-
5	Send frame 2	-
6	Wait for acknowledge	-
7	Acknowledge received	-

Loss of data frame

If a data frame is lost, the receiver will not send an acknowledgement. The sender will then time out and resend the frame. This process will continue until the frame is either received or the sender gives up.

Loss of acknowledge frame

If an acknowledgement frame is lost, the sender will not know that the data frame was received. The sender will then continue to send frames, even though the receiver is not receiving them. This can lead to data loss or corruption.

Effect of delay bandwidth product on link utilization

The delay bandwidth product is the product of the delay in the communication channel and the bandwidth of the channel. The higher the delay bandwidth product, the less efficient the Stop and Wait protocol will be. This is because the sender will have to wait longer for acknowledgements, which will reduce the amount of data that can be sent in a given amount of time.

To improve the efficiency of Stop and Wait, the delay bandwidth product should be as low as possible. This can be done by using a communication channel with low delay and high bandwidth.

What is CSMA/CD? How does it work? Distinguish between 1- persistent and non-persistent CSMA.

CSMA/CD stands for Carrier Sense Multiple Access with Collision Detection. It is a media access control (MAC) protocol that is used to control access to a shared medium, such as a bus or Ethernet network.

CSMA/CD works by having each device listen to the medium before transmitting data. If the medium is busy, the device will wait until it is free before transmitting. If two devices transmit at the same time, a collision will occur. When a collision occurs, both devices will stop transmitting and wait a random amount of time before trying again.

Feature	1-persistent CSMA	Non-persistent CSMA
Probability of transmitting after collision	1	Lower than 1
Number of collisions	More likely	Less likely
Efficiency	Lower	Higher

Briefly explain the different types of packet switching techniques with suitable networks. Write each of its advantages and disadvantages.

Datagram Packet Switching: In datagram packet switching, each packet is forwarded independently based on the destination address. This means that packets belonging to the same message may not travel through the same path, and may arrive out of order at the destination. Datagram packet switching is used in the Internet and other connectionless networks.

Advantages:

- Simple and efficient
- Can handle variable-sized packets
- Can be used in networks with a high degree of congestion

Disadvantages:

- Packets may arrive out of order
- Packets may be lost
- Not suitable for real-time applications

Virtual Circuit Packet Switching: In virtual circuit packet switching, a virtual circuit is established between the sender and receiver before any data is sent. This means that all packets belonging to the same message will take the same path through the network, and will arrive in order at the destination. Virtual circuit packet switching is used in X.25 networks.

Advantages:

- Packets arrive in order
- Packets are less likely to be lost
- Suitable for real-time applications

Disadvantages:

- More complex than datagram packet switching
- Not as efficient as datagram packet switching for networks with a high degree of congestion