Times asked: 8 times
7 times
6 times
5 times
4 times
3 times
2 times
1 time

Computer Networks Question bank

1. Introduction to Networking (10-15 marks)

1. Explain ISO OSI reference model with diagram.
2. State and explain the design issues of OSI Layer.
3. List two ways in which the OSI reference model and the TCP/IP reference model are the same. Now list two ways in which they differ.
4. What are three reasons for using layered protocols? (OR Explain the need of layering for communication and networking). What are two possible disadvantages of using layered protocols?
5. Differentiate between connection oriented and connectionless services.
6. What is topology? Explain the types of topologies with diagram, advantages and disadvantages.
7. Write a short note on Internetworking devices

2. Physical Layer (5-10 marks)

1. Explain different types of guided transmission media in detail.
2. Compare the performance characteristics of coaxial, twisted pair and fibre optic transmission media.

3. Data Link layer (15-25 marks)

1. What is channel allocation problem?
2. Explain CSMA Protocols. Explain how collisions are handled in CSMA/CD .
3. Explain sliding window protocol using selective repeat technique.
4. Compare the performance of Selective repeat & Go-back-N protocol.
5. Explain the Go-back-N protocol.
6. Explain one-bit sliding window protocol (Stop and Wait).
7. Explain different framing methods? What are the advantages of variable length frame over fixed length frame?
8. Explain design issues of data link layer.
9. List the types of Error detection and correction techniques with the help of example.
10. 4-bit data bits with binary value 1010 is to be encoded using even parity Hamming code. What is the binary value after encoding?

11. Numerical on CSMA/CD and ALOHA, Slotted ALOHA:

i. Consider building a CSMA/CD network running at 1Gbps over a 1 km cable with no repeaters. The signal speed of the cable is 200,000 km/sec. What is the minimum frame size?

ii. A network with CSMA/CD has 10 Mbps bandwidth and 25.6 ms maximum propagation delay. What is the minimum frame size?

iii. What is the throughput of the system both in Pure ALOHA and Slotted ALOHA, if the network transmits 200 bits frames on a shared channel of 200 Kbps and the system produces:

a) 1000 frames per second

b) 500 frames per second

iv. A 5 km long broadcast LAN uses CSMA has 10^7 bps bandwidth and uses CSMA/CD. The signal travels along the wire at 5×10^8 m/s. What is the minimum packet size that can be used on this network?

4. Network Layer (45-75 marks)

1. Explain IPv4 header format in detail.
2. Explain classful and classless IPv4 addressing .
3. What is subnetting? Compare subnetting and super netting. What are the default subnet masks? Explain the need for subnet mask in subnetting.
4. Explain Link State Routing with suitable example.
5. Explain Distance vector routing protocol. What is count to infinity problem. How to overcome it?
6. Explain ARP and RARP protocols in detail.
7. Write a short note on ICMP protocol.
8. What is Congestion control? Explain Open loop and closed loop congestion control.
9. What is traffic shaping? Explain leaky bucket algorithm and compare it with token bucket algorithm
10. Numerical on subnetting: (Asked in 3 of the last 4 exams)

1) An ISP is granted a block of addresses starting with 190.100.0.0/16 (65,536). The ISP needs to distribute these addresses to three groups of customers as follows:

a) The first group has 64 customers; each needs 256 addresses

b) The second group has 128 customers; each needs 128 addresses.

c) The third group has 128 customers; each needs 64 addresses.

Design the subblocks and find out how many addresses are still available after these allocations.

2) An organization has granted a block of addresses starting with 105.8.71.0/24, organization wanted to distribute this block to 11 subnets as follows:

a) First Group has 3 medium size businesses, each need 16 addresses

b) The second Group has 4 medium size businesses, each need 32 addresses.
c) The third Group has 4 households, each need 4 addresses.

Design the sub blocks and give slash notation for each subblock. Find how many addresses have been left after this allocation.

3) A large number of consecutive IP address are available starting at 198.16.0.0. Suppose that four organizations, A, B, C, and D, request 4000, 2000, 4000, and 8000 addresses, respectively, and in that order. For each of these. give the first IP address assigned. the last IP address assigned, and the mask in the w.x.y.z/s notation.

11. Compare the network layer protocols IPv4 and IPv6.
12. Write a short note on Network Address Translation(NAT).

5. Transport layer (10-25 marks)

1. Explain the TCP connection establishment(Three-Way Handshake technique).
2. Explain TCP Connection release.
3. Differentiate between TCP and UDP.
4. Explain Slow-Start algorithm for TCP's congestion handling policy.
5. Write a shot note on TCP Timers.
6. Explain TCP flow control.

6. Application layer (10-20 marks)

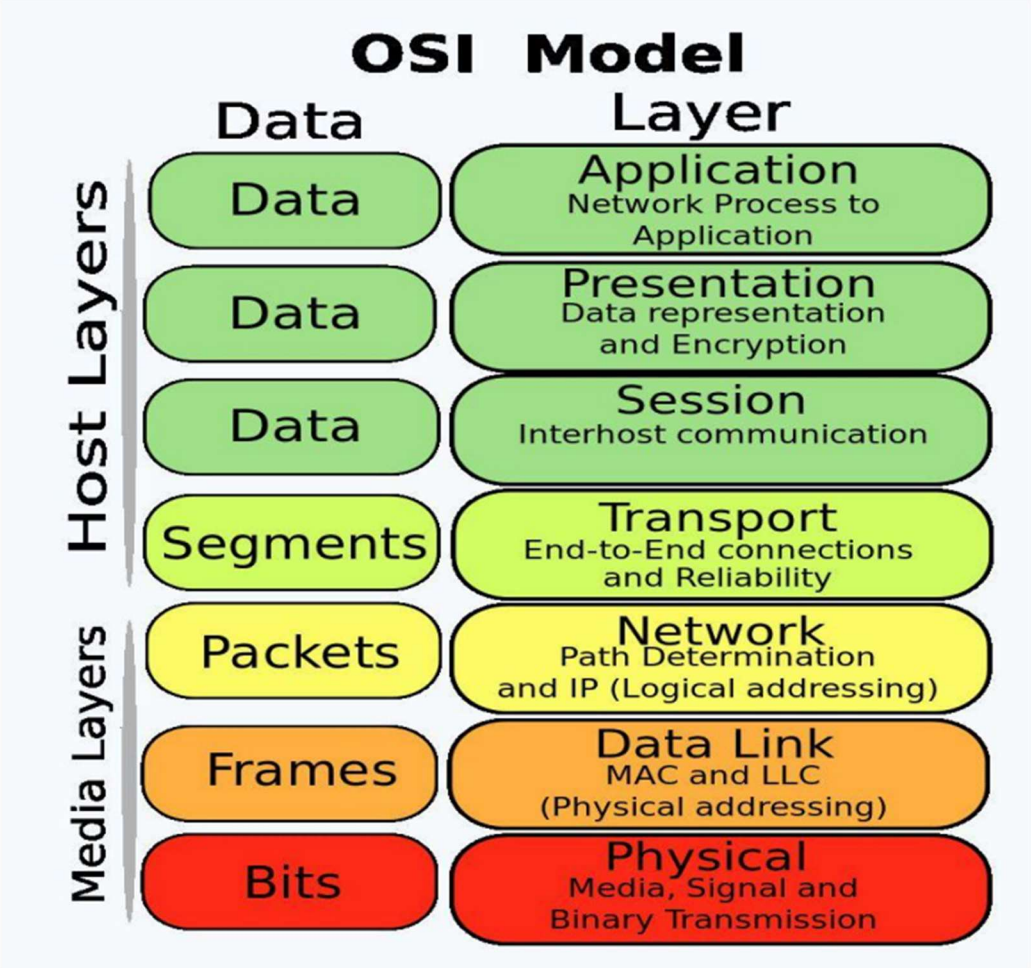
1. What is need of DNS and explain how DNS works(functioning)? Explain DNS namespace.
2. Write a short note on SMTP.
3. Explain HTTP. Draw and summarize the structure of HTTP request and response.
4. Explain working(operation) of DHCP protocol.
5. Explain DHCP message format in detail.

	1	2	3	4	5	6
2024 May	15	5	15	75	10	10
2023 Dec	10	10	25	60	10	10
2023 May	15	10	25	35	15	20
2022 Dec	5	10	25	45	25	15
Last 4 Avg	15	10	25	55	15	15
*2022 May	10		20	20	20	20
2019 Dec	15	10	35	25	15	20
2019 May	20	10	35	45	15	10
2018 Dec	30	5	15	70	20	10
Total	120	60	195	375	130	125

Computer Networks Answer bank

1. Introduction to Networking (10-15 marks)

1. Explain ISO OSI reference model with diagram.



Physical Layer :

The main functionality of the physical layer is to transmit the individual bits from one node to another node.

Functions of a Physical layer:

- Line Configuration
- Data Transmission
- Topology
- Signals

Data-Link Layer :

This layer is responsible for the error-free transfer of data frames. It defines the format of the data on the network.

Functions of the Data-link layer

- Framing
- Flow control
- Error control
- Access control

Network Layer :

It manages device addressing, track the location of devices on the network.
It determines the best path to move data from source to the destination.

Functions of Network Layer:

- Internetworking
- Addressing
- Routing
- Packetizing

Transport Layer:

The Transport layer ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.

Functions of Transport Layer:

- Service-point addressing
- Segmentation and reassembly
- Connection control
- Error control

Session Layer:

The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

- Functions of Session layer
- Dialog control
- Synchronization

Presentation Layer :

A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.

Functions of Presentation layer:

- Translation:
- Encryption:
- Compression:

Application Layer:

An application layer serves as a window for users and application processes to access network service.

Functions of Application layer:

- File transfer, access, and management (FTAM)
- Mail services

2. State and explain the design issues of OSI Layer.

1. **Addressing :** At a particular time, innumerable messages are being transferred between large numbers of computers. So, a naming or addressing system should exist so that each layer can identify the sender and receivers of each message.
2. **Direction of Transmission :** Depending on the ability of a system to communicate only in one direction or both the directions, the communication systems are classified as:
    i. Simplex systems.
    ii. Half duplex systems.
    iii. Full duplex systems.

3. Reliability : Network channels and components may be unreliable, resulting in loss of bits while data transfer.

4. Scalability : Networks are continuously evolving. The sizes are continually increasing leading to congestion.

5. Error Control : Unreliable channels introduce several errors in the data streams that are communicated. So, the layers need to agree upon common error detection and error correction methods so as to protect data packets while they are transferred.

6. Flow Control : If the rate at which data is produced by the sender is higher than the rate at which data is received by the receiver, there are chances of overflowing the receiver.

7. Resource Allocation : The allocation/deallocation should occur so that minimal interference among the hosts occurs and there is optimal usage of the resources.

8. Statistical Multiplexing : It is not feasible to allocate a dedicated path for each message while it is being transferred from the source to the destination.

9. Routing : There may be multiple paths from the source to the destination. Routing involves choosing an optimal path among all possible paths, in terms of cost and time.

10. Security : A major factor of data communication is to defend it against threats like eavesdropping and surreptitious alteration of messages.

3. List two ways in which the OSI reference model and the TCP/IP reference model are the same. Now list two ways in which they differ.

Two similarities Between OSI and TCP/IP Reference Models:

1. **Layered Structure:**
    - Both the OSI and TCP/IP models utilize a layered approach to network communication. Each layer in both models has specific responsibilities and interacts with the layers directly above and below it.
2. **End-to-End Communication:**
    - Both models provide a structure that supports end-to-end communication between devices on a network, ensuring data is successfully transmitted from the source to the destination.

Two differences Between OSI and TCP/IP Reference Models:

1. **Number of Layers:**
    - The OSI model has **seven layers**: Physical, Data Link, Network, Transport, Session, Presentation, and Application.
    - The TCP/IP model has **four layers**: Link, Internet, Transport, and Application.

2. Implementation and Adoption:

- The OSI model is primarily used as a **reference tool** for teaching and understanding networking concepts, but it is not commonly implemented in networking technologies.
- The TCP/IP model is **implemented and widely adopted** in actual networks, including the global internet, making it the de facto standard for networking.

4. What are three reasons for using layered protocols? OR Explain the need of layering for communication and networking.
What are two possible disadvantages of using layered protocols?

Reasons or need for Using Layered Protocols:

1. **Modularity and Simplification**:
    - Layered protocols break down the complex task of network communication into smaller, manageable tasks, each handled by a specific layer. This modular approach simplifies design, development, and troubleshooting.
2. **Interoperability**:
    - With standardized layers, different systems, devices, and vendors can communicate with each other seamlessly. Each layer can operate independently while ensuring compatibility across various hardware and software implementations.
3. **Abstraction and Flexibility**:
    - Each layer abstracts its functionality, allowing changes or improvements within one layer without affecting others. This makes the system more adaptable to new technologies or protocols, such as upgrading the physical medium or adding security at the application level.
4. **Easier Maintenance and Troubleshooting:**
    - Since each layer operates independently, identifying and isolating issues becomes more manageable. Problems can often be pinpointed to a specific layer, making it easier to troubleshoot and perform maintenance without disrupting the entire system.
5. **Scalability:**

- Layered protocols allow networks to grow easily. New devices, technologies, or protocols can be integrated without needing to overhaul the entire communication system.

Two Possible Disadvantages of Using Layered Protocols:

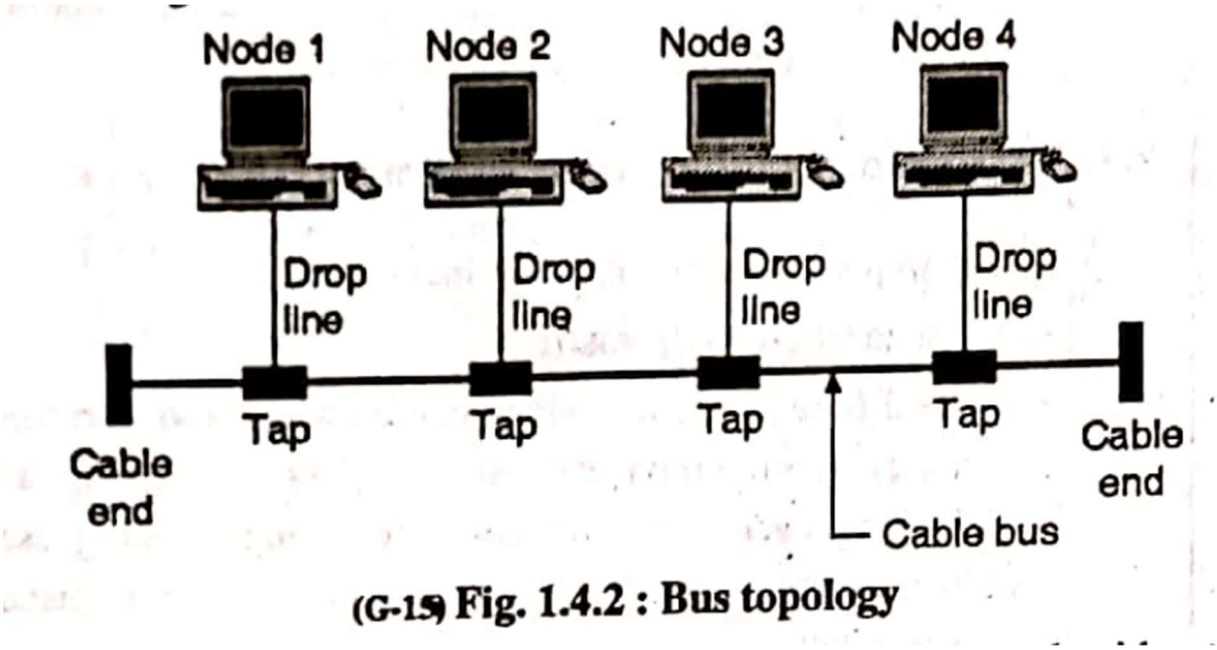
1. **Performance Overhead:**
   - Layering introduces overhead because each layer adds its own headers and processes, which can result in additional processing time and data transmission inefficiencies.
2. **Redundancy and Duplication:**
   - Some functions, such as error handling, flow control, or addressing, may be implemented in multiple layers, leading to redundancy. For instance, both the Data Link and Transport layers may perform error detection, which can increase resource consumption without a proportional gain in performance.

5. Differentiate between connection oriented and connectionless services.

Sr. No.	Parameter	Connection oriented	Connectionless
1.	Reservation of resources	Necessary	Not necessary
2.	Utilization of resources	Less	Good
3.	State information	Lot of information required	Not much information is required to be stored
4.	Guarantee of service	Guaranteed	No guarantee
5.	Connection	Connection needs to be established	Connection need not be established
6.	Delays	More	Less
7.	Overheads	Less	More
8.	Packets travel	Sequentially	Randomly
9.	Congestion due to overloading	Not possible	Very much possible

6. What is topology? Explain the types of topologies with diagram, advantages and disadvantages.

1. Bus topology:



(G-15) Fig. 1.4.2 : Bus topology

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.

Advantages of Bus topology:

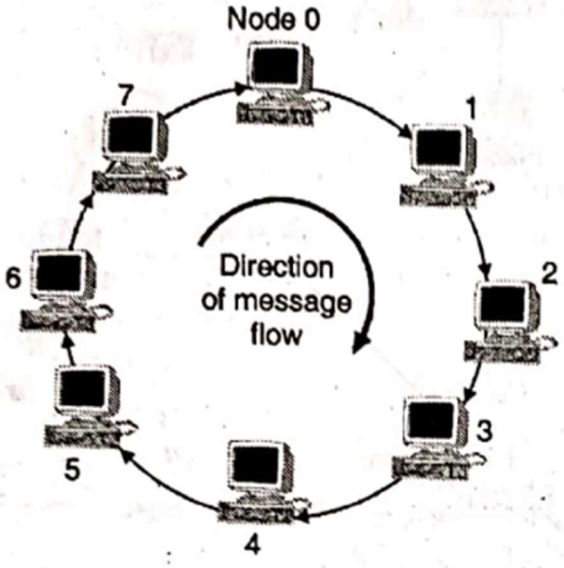
- **Low-cost cable:** Nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.

Disadvantages of Bus topology:

- **Extensive cabling:** A bus topology is quite simple, but still, it requires a lot of cabling.
- **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.

2. Ring topology:

- Ring topology is like bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.



(G-16) Fig. 1.4.3 : Ring topology

Advantages of Ring topology:

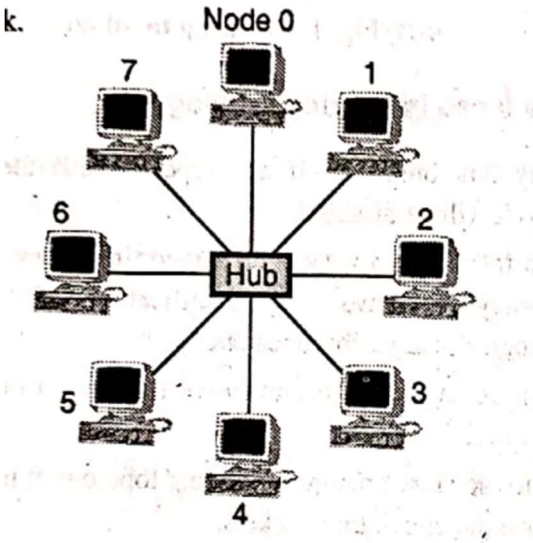
- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.

Disadvantages of Ring topology:

- **Failure:** The breakdown in one station leads to the failure of the overall network.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.

3. Star topology:

- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a server, and the peripheral devices attached to the server are known as clients.
- Star topology is the most popular topology in network implementation.



(G-18) Fig. 1.4.5 : Star topology

Advantages of Star topology:

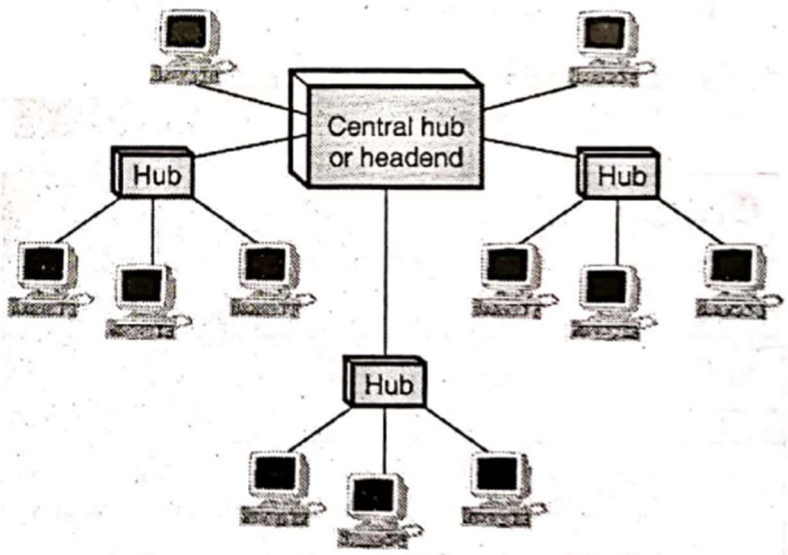
- **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
- **Cost effective:** Star topology networks are cost effective as it uses inexpensive coaxial cable.

Disadvantages of Star topology

- **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
- **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

4. Tree Network Topology:

- Tree topology is a hierarchical structure where multiple star networks are interconnected.
- A central root node connects to intermediate nodes, which further connect to other nodes or devices, forming a tree-like structure.



(G-22) **Fig. 1.4.9 : Tree topology**

Advantages of Tree Topology:

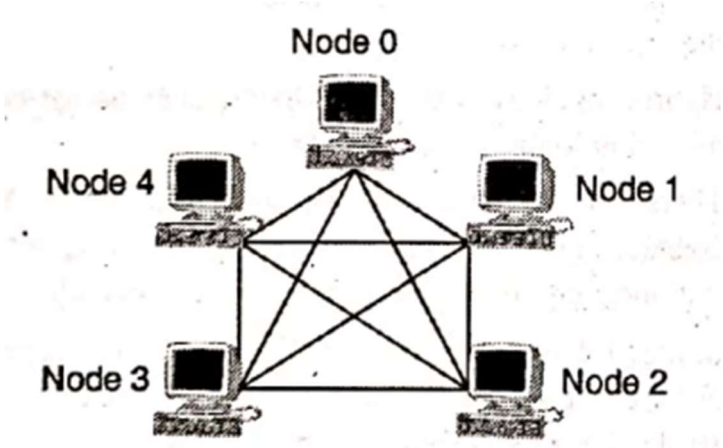
- **Scalability**: New nodes can easily be added by extending the tree branches without affecting the overall structure.
- **Segmentation**: Each branch or segment of the tree can be independently managed, which improves network organization and performance.

Disadvantages of Tree Topology:

- **Single Point of Failure**: If the root node or a major branch fails, the entire network, or a large segment of it, can go down.
- **High Cost**: The cabling and hardware requirements (hubs, switches) increase with the network's size, leading to higher costs.

5. Mesh Network Topology:

In mesh topology, each node is connected to every other node in the network, either fully or partially. This ensures multiple paths for data to travel between nodes.



(G-21) Fig. 1.4.8 : Mesh topology

Advantages of Mesh Topology:

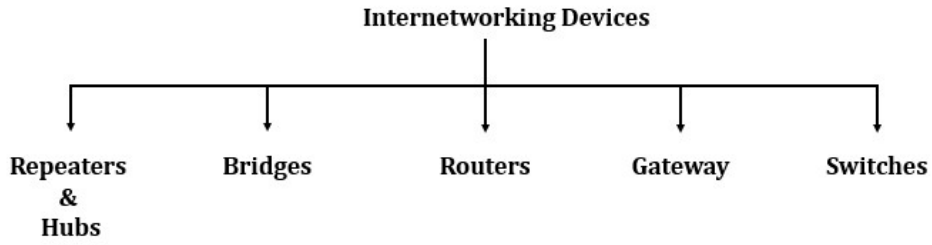
- **Redundancy and Reliability**: Mesh networks offer high fault tolerance, as multiple paths between nodes ensure that even if one link fails, data can still be transmitted via alternate routes.
- **No Single Point of Failure**: Unlike centralized topologies, mesh networks are highly resilient, reducing the risk of total network failure.

Disadvantages of Mesh Topology:

- **Expensive Setup**: Due to the large number of connections required, costs are high because of the extensive cabling and hardware.
- **Difficult Scalability**: Adding new nodes requires careful planning and additional connections to maintain the mesh structure.

7. Write a short note on Internetworking devices.

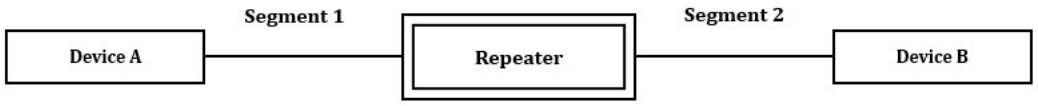
- Connectivity devices are devices used to make physical network connections.
- They do not make changes to the data or transmission route.
- Connectivity devices operate at the physical layer of the OSI Model.



1. Repeater:

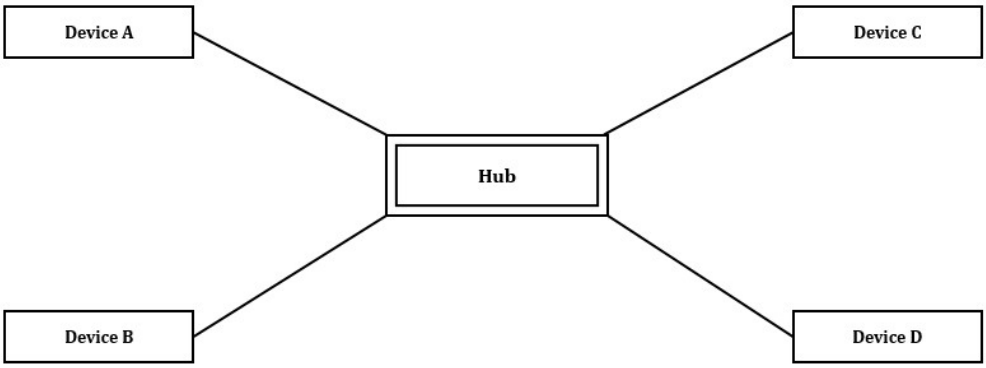
- **Function**: Amplifies or regenerates signals in a network to extend the distance they can travel.
- **Operation**: Operates at the **Physical layer** (Layer 1).

- **Benefit**: Useful in extending network range, especially for long-distance communication.



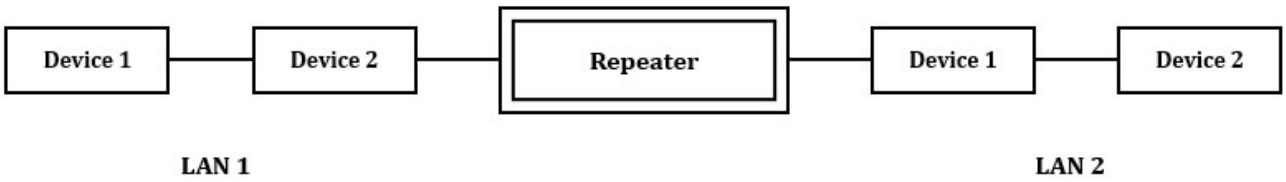
2. Hub:

- **Function**: A basic networking device that connects multiple devices in a network, operating at the **Physical layer** (Layer 1 of the OSI model).
- **Operation**: Broadcasts data to all devices connected, without distinguishing the destination.
- **Drawback**: Inefficient due to high collision rates; all devices share the same bandwidth.



3. Bridge:

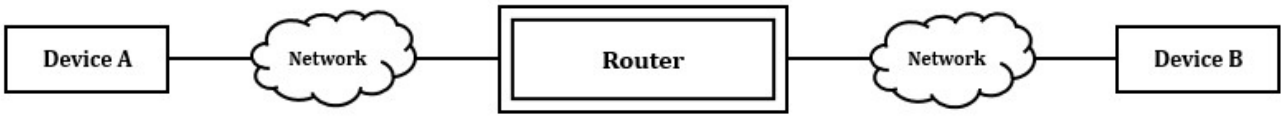
- **Function**: Used to divide a large network into smaller segments, reducing traffic.
- **Operation**: Operates at the **Data Link layer** (Layer 2) and filters traffic based on MAC addresses.
- **Benefit**: Reduces collision domains, improving network efficiency.



Internetworking using bridge

4. Router:

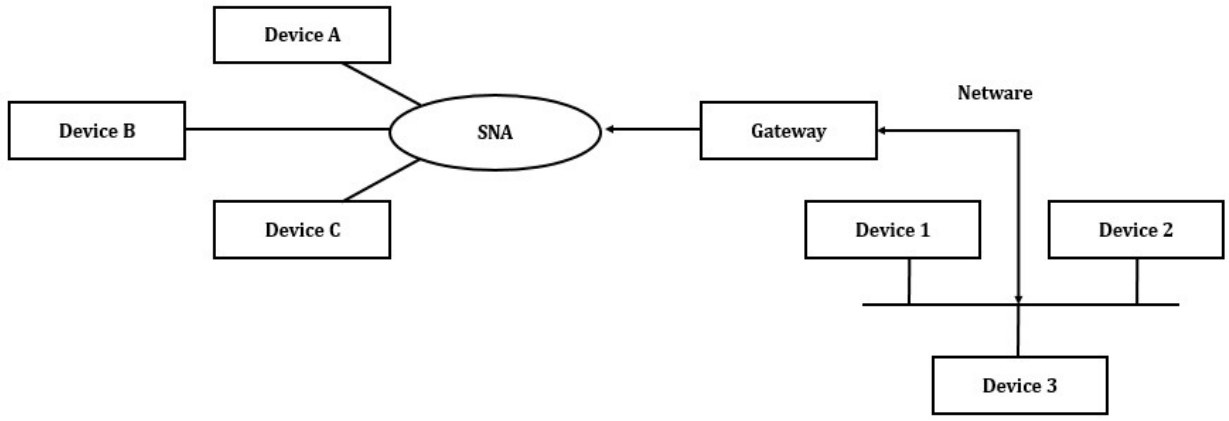
- **Function**: Routes data between different networks and operates at the **Network layer** (Layer 3).



- **Operation**: Uses IP addresses to determine the best path for data to travel between networks.
- **Benefit**: Enables communication between different LANs or WANs, including the internet.

5. Gateway:

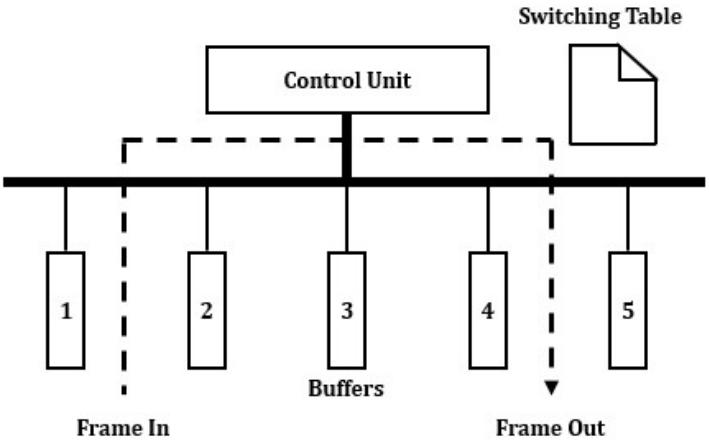
- **Function**: Acts as an entry and exit point in a network, enabling communication between different network protocols (e.g., IPv4 to IPv6).



- **Operation**: Operates across all layers of the OSI model, from the **Application layer** (Layer 7) down to the **Physical layer** (Layer 1).
- **Benefit**: Allows interoperability between networks that use different protocols or architectures.

6. Switch:

- **Function**: Connects multiple devices within a LAN and operates at the **Data Link layer** (Layer 2).
- **Operation**: Sends data directly to the intended device using MAC addresses, reducing collisions and improving efficiency.
- **Benefit**: Increases bandwidth for connected devices compared to hubs.



2. Physical Layer (5-10 marks)

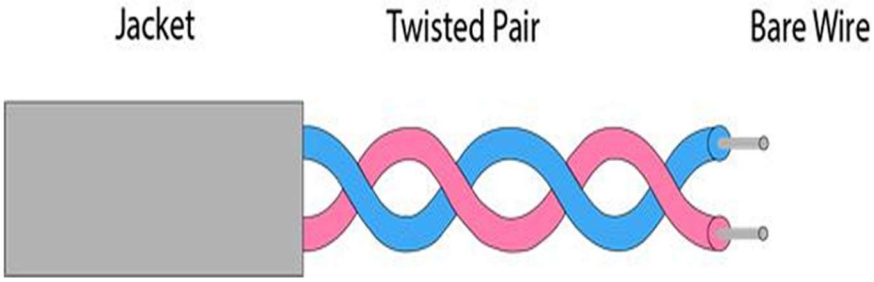
1. Explain different types of guided transmission media in detail.

Guided transmission media are of 3 types:

1. Twisted pair cable
    a. Unshielded twisted pair(UTP)
    b. Shielded twisted pair(STP)
2. Coaxial cable
3. Fibre-optic cable

1. Twisted pair:

- Twisted pair is a physical media made up of a pair of cables twisted with each other.
- A twisted pair cable is cheap as compared to other transmission media.
- Installation of the twisted pair cable is easy, and it is a lightweight cable.
- The frequency range for twisted pair cable is from 0 to 3.5KHz.



a) Unshielded Twisted Pair: An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

- Category 1: Category 1 is used for telephone lines that have low-speed data.
- Category 2: It can support up to 4Mbps.
- Category 3: It can support up to 16Mbps.
- Category 4: It can support up to 20Mbps. Therefore, it can be used for long-distance communication.
- Category 5: It can support up to 200Mbps.

Advantages Of Unshielded Twisted Pair:

- It is cheap.
- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.

Disadvantage: This cable can only be used for shorter distances because of *attenuation*.

b) Shielded Twisted Pair :

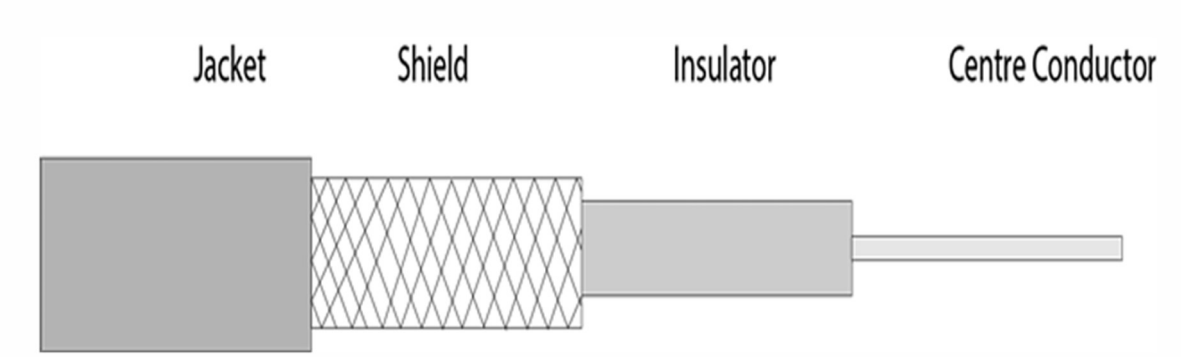
A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

Characteristics Of Shielded Twisted Pair:

- The cost of the shielded twisted pair cable is higher than UTP but not very high.
- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.

- It has a higher attenuation.
- It is shielded that provides higher data transmission rate.

2. Coaxial Cable :



- Coaxial cable is a very commonly used transmission media, for example, TV wire is usually a coaxial cable.
- The name of the cable is coaxial as it contains two conductors parallel to each other.
- It has a higher frequency as compared to Twisted pair cable.
- The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh.
- The middle core is made up of non-conductive cover that separates the inner conductor from the outer conductor.
- The middle core is responsible for the data transferring whereas the copper mesh prevents from the EMI(Electromagnetic interference).
- Coaxial cable is of two types:
    1. Baseband transmission: It is defined as the process of transmitting a single signal at high speed.
    2. Broadband transmission: It is defined as the process of transmitting multiple signals simultaneously.

Advantages of Coaxial cable:

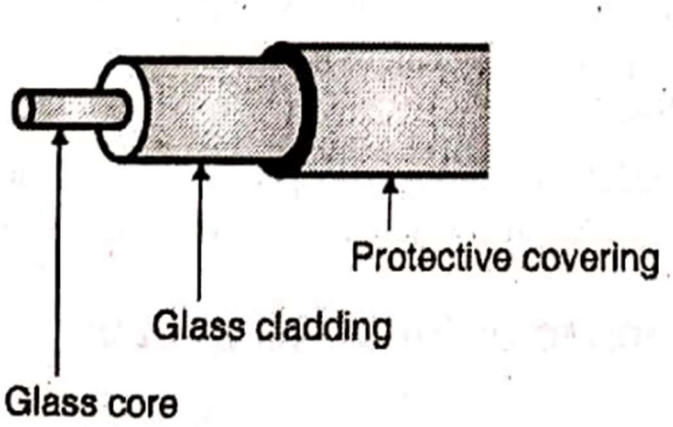
- **High Bandwidth:** Offers greater bandwidth than twisted pair cables, making it suitable for television and broadband internet.
- **Less Interference:** The shielding reduces interference from external signals.

Disadvantages Of Coaxial cable:

- **Cost:** It is more expensive as compared to twisted pair cable.
- **Failure:** If any fault occurs in the cable causes the failure in the entire network.

3. Optical Fiber Cable :

- Fiber optic cable is a cable that uses electrical signals for communication.
- Fiber optic is a cable that holds the optical fibres coated in plastic that are used to send the data by pulses of light.
- The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.
- Fiber optics provide faster data transmission than copper wires.



Advantages:

- **High Speed and Bandwidth**: Supports very high data rates (in Gbps) and is ideal for high-speed internet and long-distance communications.

Disadvantages:

- **High Cost**: Fiber optic cables and the equipment needed to install and maintain them are more expensive than copper-based media.
- **Fragility**: Fiber optic cables are more fragile and prone to damage compared to twisted pair and coaxial cables.

2. Compare the performance characteristics of coaxial, twisted pair and fibre optic transmission media.

Sr. No.	Parameter of comparison	Twisted pair cable	Co-axial cable	Fiber optic cable
1.	Transmitted Signal	Electrical	Electrical	Optical
2.	Noise / immunity	Low	High	Very high
3.	Effect of external magnetic field	Yes	Less	No effect
4.	Conductor short circuit	Possible	Possible	Not applicable
5.	Band width	Low	Moderate	Very large
6.	Attenuation	High	Medium	Low
7.	Ease of installation	Easy	Easy	Difficult
8.	Cost	Low	Medium	High

OR

Sr. No.	Twisted pair cable	Co-axial cable	Optical fiber
1.	Transmission of signals takes place in the electrical form over the metallic conducting wires.	Transmission of signals takes place in the electrical form over the inner conductor of the cable.	Signal transmission takes place in an optical form over a glass fiber
2.	Noise immunity is low. Therefore more distortion.	Higher noise immunity than the twisted pair cable due to the presence of shielding conductor.	Highest noise immunity as the light rays are unaffected by the electrical noise.
3.	Affected due to external magnetic field.	Less affected due to external magnetic field.	Not affected by the external magnetic field.
4.	Short circuit between the two conductors is possible.	Short circuit between the two conductors is possible.	Short circuit is not possible.
5.	Cheapest	Moderately expensive	Expensive
6.	Can support low data rates.	Moderately high data rates	Very high data rates.
7.	Power loss due to conduction and radiation.	Power loss due to conduction	Power loss due to absorption, scattering, dispersion and bending.
8.	Low bandwidth	Moderately high bandwidth	Very high bandwidth
9.	Node capacity per segment is 2	Node capacity per segment is 30 to 100	Node capacity per segment is 2.
10.	Attenuation is very high	Attenuation is low	Attenuation is very low.
11.	Installation is easy	Installation is fairly easy	Installation is difficult.
12.	Electromagnetic interference (EMI) can take place	EMI is reduced due to shielding	EMI is not present.

3. Data Link layer (15-25 marks)

1. What is the channel allocation problem?

1. In a broadcast network, a single broadcast channel is to be allocated to one transmitting user at a time.
2. When multiple users use a shared network and want to access the same network. Then channel allocation problem occurs.
3. So, to allocate the same channel between multiple users, techniques are used, which are called channel allocation techniques.
4. There are three types of channel allocation techniques that you can use to resolve channel allocation problem as follows:
    - Static channel allocation
    - Dynamic channel allocation
    - Hybrid channel allocation.

a) **Static Channel Allocation:** The traditional way of allocating a single channel between multiple users is called static channel allocation. Channels are permanently assigned to specific users or uses. Static channel allocation is also called fixed channel allocation. Such as a telephone channel among many users is a real-life example of static channel allocation.

b) **Dynamic Channel Allocation**: The technique in which channels are not permanently allocated to the users is called dynamic channel allocation. In this technique, no fixed frequency or fixed time slot is allotted to the user.

c) **Hybrid Channel Allocation:** The mixture of fixed channel allocation and dynamic channel allocation is called hybrid channel allocation.

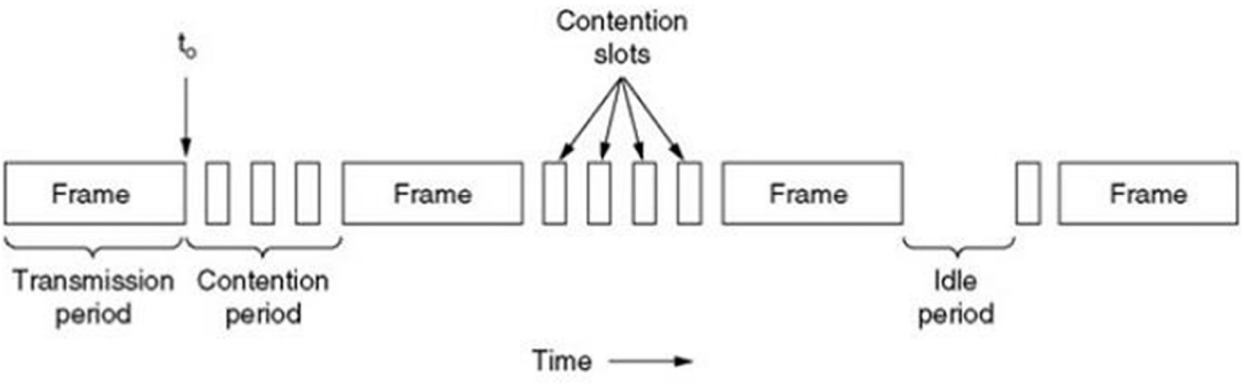
2. Explain CSMA Protocols. Explain how collisions are handled in CSMA/CD .

CSMA(Carrier Sense Multiple Access) is based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data.

It means that if the channel is idle, the station can send data to the channel. Otherwise, it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a network protocol used in the Medium Access Control (MAC) layer to manage carrier transmission and reduce collisions in shared network channels. Its primary goal is to reduce the likelihood of data collisions and ensure efficient data transmission on the network.

Steps for collision handling in CSMA/CD:



1) At t_0, a station has finished transmitting its frame. Any other station having a frame to send may now attempt to do so. If two or more stations have decided to transmit simultaneously , there will be a collision.
2) If the station detects a collision, it aborts the transmission , waits a random period of time and then tries it again. Therefore, the model shown consists of alternating contention and transmission periods, with idle periods occurring when all stations are quiet.

By terminating frames, it would save time and bandwidth. This is called CSMA/CD.
It is mainly used LAN in the MAC sub player (part of data link layer network) and Ethernet.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is a network protocol used primarily in wireless networks to manage how devices access a shared communication channel while minimizing data collisions. Unlike CSMA/CD, which detects collisions after they occur, CSMA/CA tries to avoid collisions before they happen, making it more suitable for wireless environments where detecting collisions can be challenging.

It is performed in the following steps:

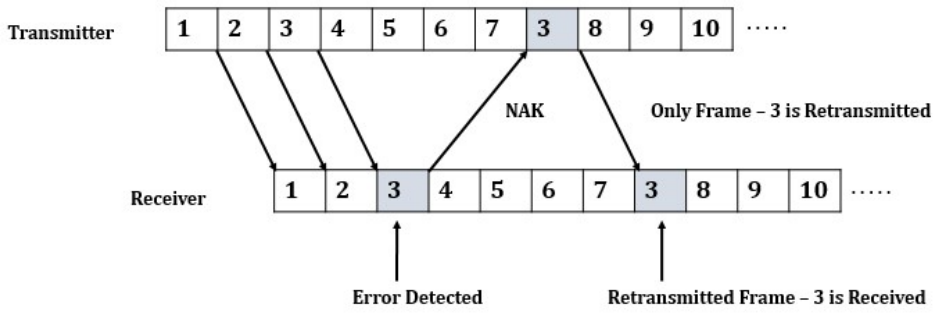
1. **Carrier Sensing**: Before sending data, a device listens to ensure the channel is idle. If it's busy, the device waits.
2. **Collision Avoidance**: When the channel is clear, the device waits a random backoff time before transmitting. This delay reduces the chance of simultaneous transmissions.
3. **Acknowledgment**: After data is sent, the receiver sends an acknowledgment (ACK). If no ACK is received, the sender assumes a collision and retries after another backoff period.

3. Explain sliding window protocol using selective repeat technique.

Selective repeat protocol, also known as Selective Repeat Automatic Repeat Request (ARQ), is a data link layer protocol that uses the sliding window technique for reliable data frame delivery. Only erroneous or lost frames are retransmitted in this case, while good frames are received and buffered.

Selective Repeat ARQ is used in the data link layer for error detection and control. The sender sends several frames specified by a window size in the selective repeat without waiting for individual acknowledgement from the receiver as in Go-Back-N ARQ.

Working:



1. In this system the transmitter does not wait for the ACK signal for the transmission of the next code word.

2. It transmits the code words continuously till it receives the “NAK” signal from the receiver.

3. The receiver sends the NAK signal back to the transmitter when it detects an error in the received frame.

4. For example, the receiver detects an error in the third frame.

5. By the time this NAK signal reaches the transmitter, it had transmitted the frames up to 7 as shown in figure.

6. On reception of NAK signal, the transmitter will retransmit only frame 3 and then continues with the sequence 8, 9 & so on.

7. The frames 4, 5, 6 & 7 received by the receiver are not discarded by the receiver.

8. The receiver receives the retransmitted frames in between the regular frames.

9. Therefore, the receiver will have to maintain the frames sequentially.

10. Thus, in selective repeat ARQ only the frame which is damaged or lost is retransmitted by the transmitter.

11. The lost ACK or NAK frames are treated in the same manner as the go-back-n method.

12. Hence the Selective Repeat ARQ is the most efficient but the most complex protocol.

Advantage: It gives the best throughput efficiency due to use of pipelining.
Unnecessary transmission by sending only the damaged or missing frames.

Disadvantage: Due to complexity of sorting and storage and the extra logic needed by the transmitter to select frames for retransmission, the system becomes more expensive.

4. Explain the Go-back-N protocol.

In Go-Back-N ARQ, N is the sender's window size. Suppose we use Go-Back-3, which means that three frames can be sent at a time before expecting an acknowledgment from the receiver.

It uses the principle of protocol pipelining, where multiple frames can be sent before receiving the acknowledgment for the first frame.

If we have five frames and use Go-Back-3, this means that three frames—frame 1, frame 2, and frame 3—can be sent before expecting an acknowledgment for frame 1.

If the acknowledgment for a frame is not received within an agreed-upon time period, all frames in the current window will be retransmitted.

For example, if frame 5 has been sent but its acknowledgment is not received, and the current window holds three frames, then these three frames will be retransmitted.

Working of Go-Back-N ARQ:

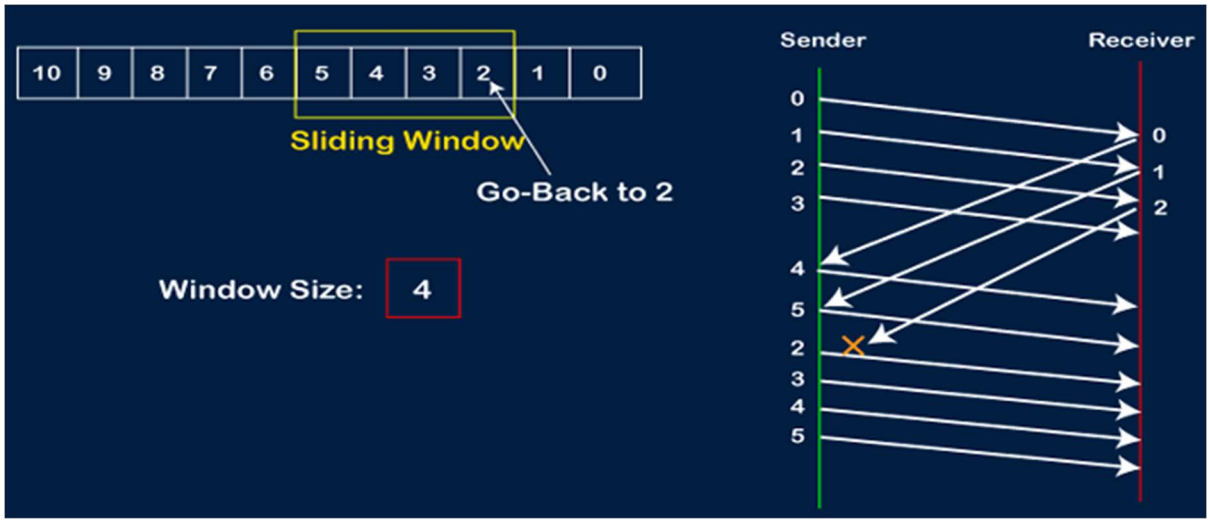
Suppose there is a sender and a receiver, and there are 11 frames to be sent. The sender's window size is 4. These frames are represented as 0,1,2,3,4,5,6,7,8,9,10.

Step 1: The sender sends the first four frames (0, 1, 2, and 3) to the receiver. At this point, the sender expects to receive an acknowledgment for frame 0.

Step 2: Let's assume the receiver successfully receives frame 0 and sends an acknowledgment for it. After receiving the acknowledgment, the sender slides the window forward and sends the next frame, frame 4. Now, the window contains frames 1, 2, 3, and 4.

Step 3: The receiver then sends an acknowledgment for frame 1. Upon receiving it, the sender slides the window again and sends the next frame, frame 5. Now, the window contains frames 2, 3, 4, and 5.

Step 4: Suppose the receiver does not acknowledge frame 2 because either the frame or the acknowledgment was lost. In this case, instead of sending frame 6, the sender "goes back" to frame 2 (the first frame of the current window) and retransmits all frames in the current window: frames 2, 3, 4, and 5.



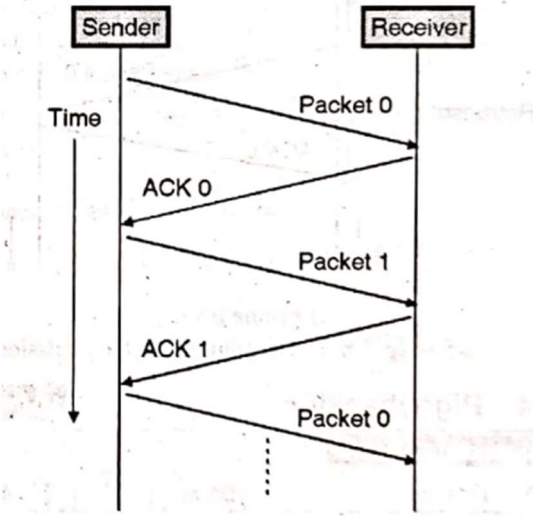
5. Compare the performance of Selective repeat & Go-back-N protocol.

Sr. No.	Parameter	Go back n ARQ	Selective repeat ARQ
1.	Window size	Sending window size : $(2^m - 1)$	Sending window size : 2^{m-1}
2.	Operating principle	It transmits frames continuously till it receives the NAK signal.	Same as Go back n protocol.
3.	Communication type (Direction wise).	Communication is one way (simplex) for the data frames though the NAK frames are allowed to travel in the opposite direction.	Same as Go back n protocol
4.	Retransmission takes place if	1. Received frame is damaged. 2. Transmitted frame is lost. 3. NAK is lost.	Same as Go back n protocol
5.	Retransmission	On reception of the NAK signal, the transmitter retransmits all the frames from the one for which the NAK is obtained.	On reception of NAK, only the damaged or lost frame is retransmitted.
6.	Principle of pipelining.	Used	Used.
7.	Efficiency	Moderately efficient due to pipelining	Most efficient due to pipelining.
8.	Complexity	Moderately complex.	Highly complex.

6. Explain one-bit sliding window protocol (Stop and Wait).

Working :

- If there is a sender and receiver, then sender sends a data packet.
- The sender will not send the second packet without receiving the acknowledgment of the first packet.
- The receiver sends the acknowledgment for the data packet that it has received.
- Once the acknowledgment is received, the sender sends the next packet. This process continues until all the packets are sent.



Advantage:

- Flow control as it is a slow process.
- Simple and easy to implement.

Disadvantages :

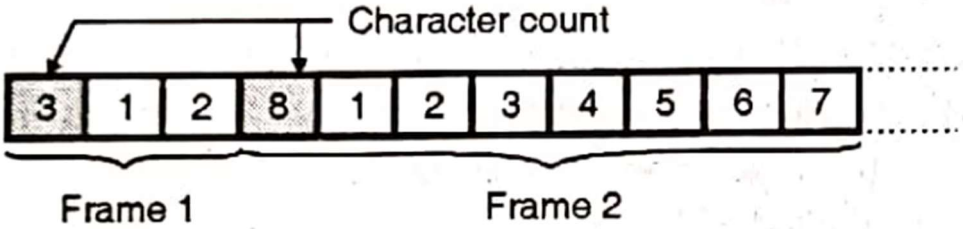
- Inefficient as only one frame can be sent at any time.
- Problems occur due to lost data.
- Problems occur due to lost acknowledgment.

7. Explain different framing methods? What are the advantages of variable length frame over fixed length frame?

- Following methods are used for carrying out framing :
  1. Character count method.
  2. Starting and ending characters, with character stuffing.
  3. Starting and ending flags with bit stuffing.
  4. Physical layer coding violations.

1. Character count

- In this method, a field in the header is used to specify the number of characters in the frame.
- This number helps the receiver to know the exact number of characters present in the frame following this count.
- The character count method is illustrated in Fig. 3.4.2.

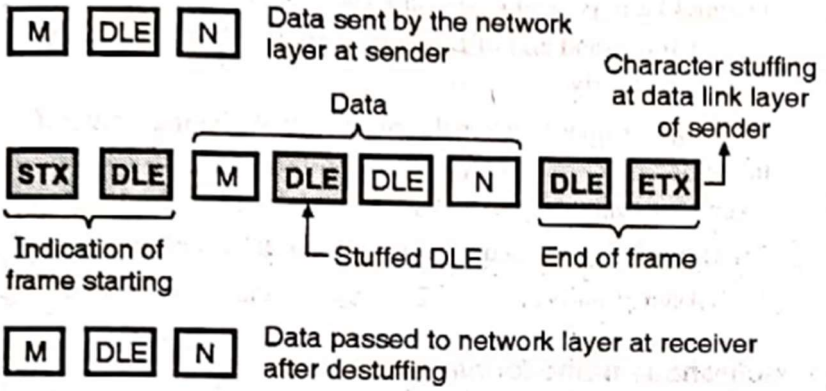


(L-668)**Fig. 3.4.2 : Character count method**

- The two frames shown in Fig. 3.4.2 contain 3 and 8 characters respectively and numbers 3 and 8 are inserted in the headers of the corresponding frames.

2. Character stuffing

- The data link layer at the sending end inserts an ASCII DLE character just before each accidental DLE character in the data being transmitted.
- The data link layer at the receiving end will remove these DLE characters before transferring the data to the network layer.

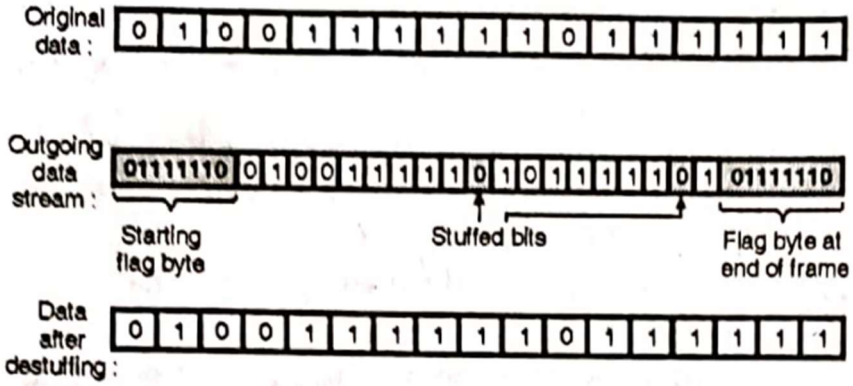


(G-181) **Fig. 3.4.4 : Character stuffing**

- Thus the DLE STX or DLE ETX used for framing purpose can be distinguished from the one in data because DLEs in the data always appear more than once.
- This is called character stuffing and it is shown in Fig. 3.4.4. Note that at the receiving end the destuffing is essential. Destuffing process is exactly opposite to the character stuffing process.

3. Bit stuffing

- Whenever the sender data link layer detects the presence of five consecutive ones in the data stream, it automatically stuffs a 0 bit into the outgoing bit stream. Thus the six consecutive 1s will never appear in the data stream. Hence there is no chance of misinterpretation.
- This is called bit stuffing and it is illustrated in Fig. 3.4.6.

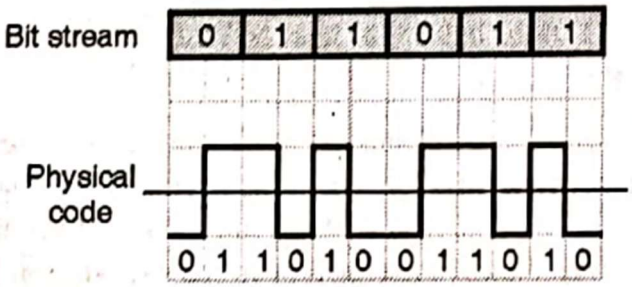


(G-183) **Fig. 3.4.6 : Bit stuffing and destuffing**

- When a receiver detects presence of five consecutive ones in the received bit stream, it automatically deletes the 0 bit following the five ones.
- This is called de-stuffing. It is shown in Fig. 3.4.6.
- Due to bit stuffing, the possible problem if the data contains the flag byte pattern (0111 1110) is eliminated.

4. Physical layer coding violations

- This method of framing is applicable only to those networks in which the encoding on the physical medium contains some redundancy.
- Some LANs encode each bit of data using two physical bits for example the use of the Manchester coding refer Fig. 3.4.7. The physical Manchester code makes a transition at the middle of the bit interval as shown.
- Therefore a 1 bit is encoded into a 10 pair and a 0 bit is encoded into a 01 pair as shown in Fig. 3.4.7. This helps in recognizing the boundaries of bits in a precise manner.
- This use of invalid physical code is a part of 802 LAN standards.



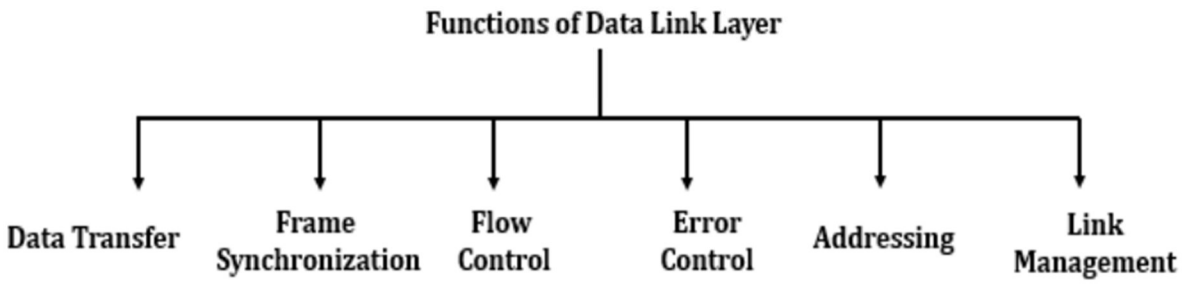
(G-184)**Fig. 3.4.7**

Advantages of Variable-Length Frames over Fixed-Length Frames

- **Efficient Use of Bandwidth**:
  Variable-length frames fit data precisely into the frame, avoiding the padding needed in fixed-length frames. This minimizes wasted space and improves bandwidth utilization.
- **Flexibility**:
  Variable-length frames can handle different data sizes, from small control messages to large files or video streams, making them adaptable to various applications.
- **Reduced Fragmentation**:
  Fixed-length frames require splitting larger data into multiple frames, which increases overhead. Variable-length frames accommodate larger data chunks, reducing the need for fragmentation.
- **Better Handling of Mixed Data Types**:
  Variable-length frames efficiently manage both large and small data packets, preventing wasted resources that result from padding or unnecessary fragmentation.

8. Explain design issues of data link layer.

FUNCTIONS OF DATA LINK LAYER (DESIGN ISSUES):



Design issues with data link layer are :

1. Services provided to the network layer: The data link layer act as a service interface to the network layer. The principal service is transferring data from network layer on sending machine to the network layer on destination machine. This transfer also takes place via DLL (Data link-layer).

2. Frame Synchronization: The source machine sends data in the form of blocks called frames to the destination machine. The starting and ending of each frame should be identified so that the frame can be recognized by the destination machine

3. Flow control: Flow control is done to prevent the flow of data frame at the receiver end. The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.

4. Error control: Error control is done to prevent duplication of frames. The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

9. List the types of Error detection and correction techniques with the help of example.

1. Checksum

Checksum involves summing up the binary values of the data segments and appending the result (the checksum) at the end of the data. The receiver performs the same calculation and checks if the result matches the received checksum.

- **Example**:
  - Data: 1011 1101
  - Sum: 1011 + 1101 = 11000
  - Append checksum: Transmit 1011 1101 1000

The receiver computes the sum of the data again and compares it to the checksum. If they match, no error occurred.

- **Advantages**: Detects multiple-bit errors.
- **Disadvantages**: Cannot correct errors and can miss certain types of errors.

2. Cyclic Redundancy Check (CRC)

CRC is a more robust error detection technique. The data is treated as a large binary number and divided by a predetermined **polynomial**. The remainder from the division (CRC bits) is appended to the data. At the receiver end, the same division is performed to detect errors.

- **Example**:
  - Data: 1101011011
  - Polynomial: 10011
  - Remainder (CRC bits): 1110
  - Transmitted: 11010110111110

If the received data, when divided by the same polynomial, doesn't produce a zero remainder, an error is detected.

(Numerical can be asked, Example:)

Ex. 3.6.12 : If the frame is 1101011011 and generator is $x^4 + x + 1$ what would be the transmitted frame.

May 05, Dec. 09, 5 Marks, May 11, 10 Marks

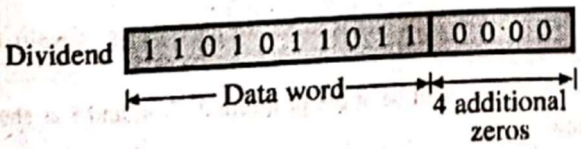
Soln. :

Given : Data word : 1 1 0 1 0 1 1 0 1 1

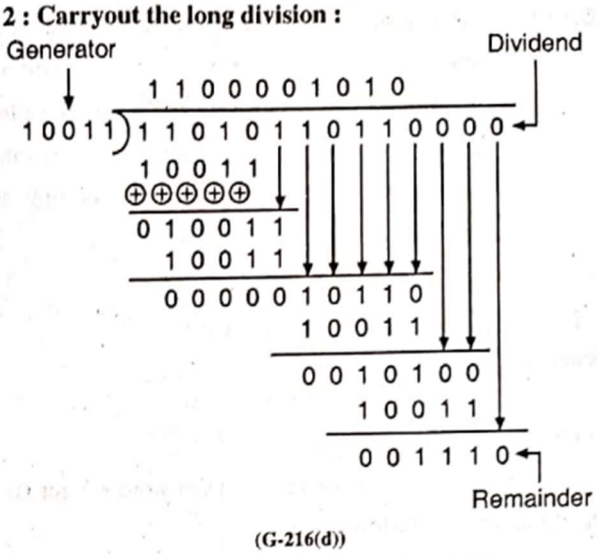
Generator : $x^4 + x + 1 = x^4 + 0x^3 + 0x^2 + x + 1 = 10011 = n$

Step 1 : Add four zeros at the end of the data word :

Add four zeros (n – 1) at the end of data word to get the dividend as follows :



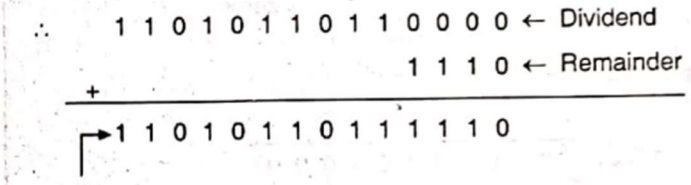
Step 2 : Carryout the long division :



(G-216(d))

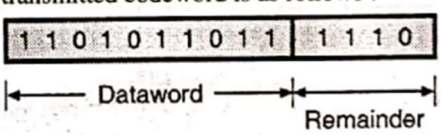
Step 3 : Write the transmitted frame :

The transmitted frame is obtained by writing the data word followed by the remainder.



(G-1967)

∴ The transmitted codeword is as follows :



- **Advantages**: Highly effective for detecting multiple-bit errors.
- **Disadvantages**: Can detect but not correct errors.

3. Hamming Code (Error Correction)

Hamming code is an error **detection and correction** technique. It adds **parity bits** at specific positions in the data to not only detect but also correct single-bit errors.

- **Example**:
  - Data: 1010
  - Hamming code (7-bit): 1011010
    If a single-bit error occurs, the receiver can use the parity bits to both **detect and correct** the error.
- **Advantages**: Can both detect and correct single-bit errors.
- **Disadvantages**: Not effective for detecting or correcting multiple-bit errors.

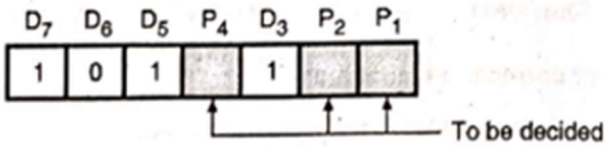
Hamming code numerical example:

Ex. 3.6.6 : A bit word 1 0 1 1 is to be transmitted. Construct the even parity seven-bit Hamming code for this data.

Soln. :

Step 1 : The codeword format :

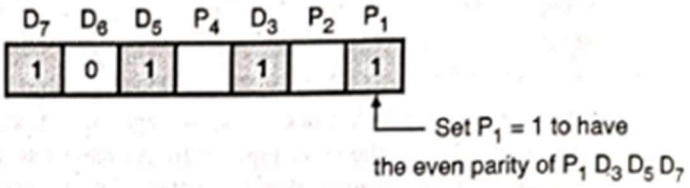
The seven bit Hamming code format is shown in Fig. P. 3.6.6 : Given bit word = 1 0 1 1



(G-1948) **Fig. P. 3.6.6**

Step 2 : Decide P_1 :

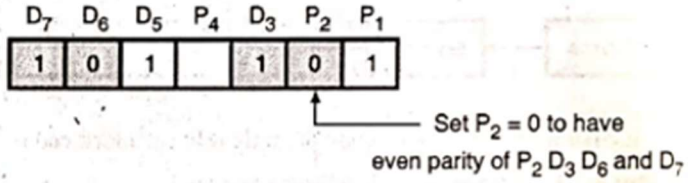
P_1 sets the parity of bits P_1, D_3, D_5 and D_7. As D_7, D_5, D_3 = 1 1 1 we have to set P_1 = 1 in order to have the even parity.



(G-1949)

Step 3 : Decide P_2 :

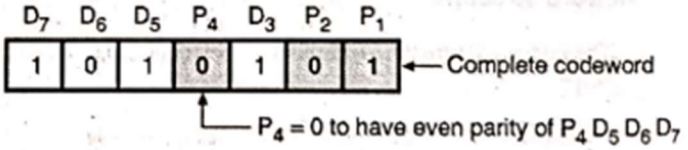
P_2 is set to have the even parity of P_2 D_3 D_6 and D_7. But D_3 D_6 D_7 = 1 0 1 hence set P_2 = 0.



(G-1950)

Step 4 : Decide P_4 :

P_4 is set to have the even parity of P_4 D_5 D_6 and D_7. But D_5 D_6 D_7 = 1 0 1, hence set P_4 = 0.



10. Numerical on CSMA/CD and ALOHA, Slotted ALOHA:

i. Consider building a CSMA/CD network running at 1Gbps over a 1 km cable with no repeaters. The signal speed of the cable is 200,000 km/sec. What is the minimum frame size?

Soln. :

Propagation speed = 200000 km/sec.

Length of cable = 1 km

Propagation Time = $\frac{1}{200000} = 5 \times 10^{-6}$ s $= 5\ \mu$ sec

Transmission speed = 1 Gbps.

Number of bits in cable :

Number of bits sender can transmit from time it sends 1st bit to the time that bit reaches end of cable.

$$1 \times 10^9 \times \frac{1}{20000} = 0.5 \times 10^5 = 5 \times 10^4 \text{ bits.}$$

Frame size = $5 \times 10^4 \times 2$

= 10,000 bits

Total round time = $5 \times 2 = 10\ \mu$ sec.

For collision detection frame should take at least 10 µS to send.

Data rate = 1000 bit per µS.

Thus 10,000 bits could be sent in 10 µS. Thus frame size should be at least 10,000 bits.

ii. What is the throughput of the system both in Pure ALOHA and Slotted ALOHA, if the network transmits 200 bits frames on a shared channel of 200 Kbps and the system produces:

a) 1000 frames per second
b) 500 frames per second

Given: Network transmission rate = 200 bits
Bandwidth = 200 Kbps
∴ Frame transmission rate = 200/200 = 1 ms

Formulae:
Throughput of Pure ALOHA = $G \times e^{-2G}$
Throughput of Slotted ALOHA = $G \times e^{-G}$

a) When system produces 1000 frames per second:
∴ In 1 ms, frames = $1000 \times 10^{-3} = 1 = G$
For Pure ALOHA, $S = G \times e^{-2G}$
$\therefore S = 1 \times e^{-2\times1}$
$\therefore S = 0.135$
∴ Throughput of system = $0.135 \times 1000 = 135$ fps

For Slotted ALOHA, $S = G \times e^{-G}$
$\therefore S = 1 \times e^{-1}$
$\therefore S = 0.368$
∴ Throughput of system = $0.368 \times 1000 = 368$ fps

b) When system produces 500 frames per second,
In 1 ms, frames = $500 \times 10^{-3} = 1/2 = G$
For Pure ALOHA, $S = 1/2 \times e^{-2\times1/2} = 0.184$
∴ Throughput of system = $0.184 \times 500 = 92$ fps

For Slotted ALOHA, $S = 1/2 \times e^{-1/2} = 0.3032$
∴ Throughput of system = $0.3032 \times 500 = 151.6$ fps

Ans

Frames produced (in fps)	Throughput of System	
	Pure ALOHA (in fps)	Slotted ALOHA (in fps)
1000	135	368
500	92	151.6

iii. A network with CSMA/CD has 10 Mbps bandwidth and 25.6 ms maximum propagation delay. What is the minimum frame size?

Given:

- Bandwidth = 10 Mbps (which is 10×10^6 bits per second)
- Maximum propagation delay = 25.6 ms (which is 25.6×10^{-3} seconds)

Step 1: Calculate RTT

$$\text{RTT} = 2 \times 25.6 \text{ ms} = 51.2 \text{ ms} = 51.2 \times 10^{-3} \text{ seconds}$$

Step 2: Calculate the minimum frame size

$$\text{Minimum Frame Size} = \text{Bandwidth} \times \text{RTT}$$

$$\text{Minimum Frame Size} = (10 \times 10^6 \text{ bits/sec}) \times (51.2 \times 10^{-3} \text{ sec})$$

$$\text{Minimum Frame Size} = 512,000 \text{ bits} = 64,000 \text{ bytes}$$

Thus, the minimum frame size is **512 bits**, or **64 bytes**.

iv. A 5 km long broadcast LAN uses CSMA has 10^7 bps bandwidth and uses CSMA/CD. The signal travels along the wire at 5×10^8 m/s. What is the minimum packet size that can be used on this network?

Given: Distance = 5 km
Bandwidth = 10^7 bps
Speed = 5×10^8 m/s

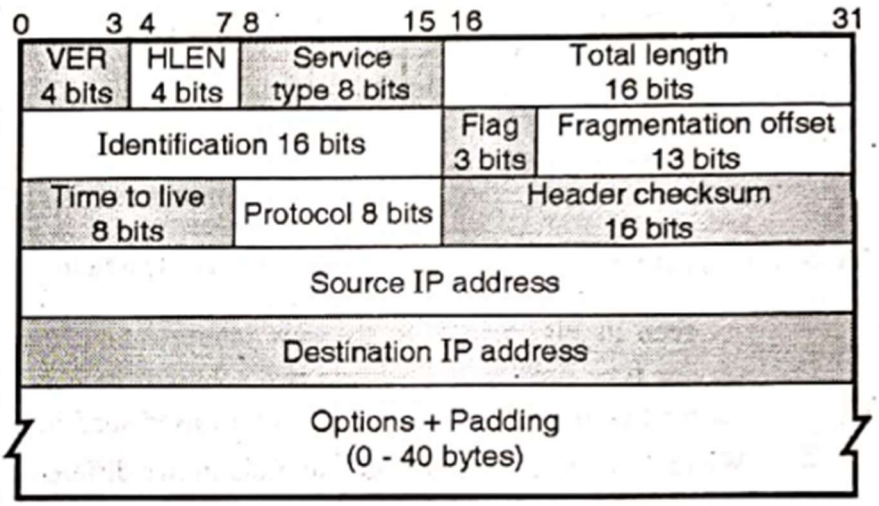
Calculating propogation delay:
T_p = Distance / Propogation speed
= $5 / (5 \times 10^8)$ ($\because$ 5 km = 5×10^3 m)
T_p = 10^{-5} m/s

Calculating Minimum Frame Size:
Minimum frame size = 2 × Propogation delay × bandwidth
= $2 \times 10^{-5} \times 10^7$
= 200 bits or 25 bytes

Minimum frame size should be 200 bits or 25 bytes

4. Network Layer (45-75 marks)

1. Explain IPv4 header format in detail.



(G-2082) **Fig. 5.13.3 : IPv4 header format**

I) Version: This Field defines the version of IP. It is Static 4-bit value.

II) Header Length: This Field defines the length of the datagram header. It is 4-bit value.

III) Type of Service: It is 8-bit value. It is used tell the network how to treat the IP packet. These bits are generally used to indicate the Quality of Service (QoS) for the IP Packet.

IV) Packet Length: 16-bit value indicating the size of the IP Packet in terms of bytes. This gives a maximum packet size of 65536 bytes.

V) Identification: 16-bit field used for reassembling the packet at the destination.

VI) Flags: It is 3 bits value. It indicates if the IP packet can be further fragmented or not and if the packet is the last fragment or not of a larger transfer.

VII) Fragment offset: 13-bit value used in the reassembly process at the destination.

VIII) Time to Live: 8-bit value telling the network how long an IP packet can exist in a network before it is destroyed.

IX) Protocol: 8-bit value used to indicate the type of protocol being used (TCP, UDP etc.).

X) Header checksum: It is 16-bit value. It is used to indicate errors in the header only. Every node in the network has to check and re-insert a new checksum as the header changes at every node.

XI) Source address: 32-bit value representing the IP address of the sender of the IP packet.

XII) Destination address: 32-bit value representing the IP address of the packet's final destination.

XIII) Options: Options are not required for every datagram. They are used for network testing and debugging.

XIV) Padding: Variable size bit field. These bits are used to ensure a 32 bit boundary for the header is achieved.

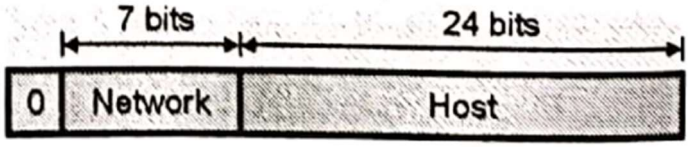
2. Explain classful and classless IPv4 addressing .

❖ Classful addressing:

- The first addressing system to be implemented as part of the internet protocol was Classful addressing.
- The value of any segment(byte) is between 0 and 255.
- There are zeroes preceding the value in any segment (054 is wrong, 54 is correct).
- Each of these classes has a valid range of IP addresses.
- The order of bits in the first octet determines the classes of IP address.
- IPv4 is divided into two parts: Network ID & Host ID.

Class A :

- IP address belonging to class A are assigned to the networks that contain many hosts.
- The network ID is 8 bits long.
- The host ID is 24 bits long.
- The higher order bit of the first octet in class A is always set to 0. The remaining 7 bits in first octet are used to determine network ID.

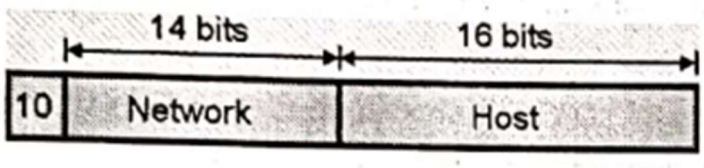


(G-531) **Fig. 5.9.2(a) : Class A IPv4 address formats**

- The 24 bits of host ID are used to determine the host in any network. The default subnet mask for class A is 255.0.0.0.
- IP addresses belonging to class A ranges from 1.x.x.x - 126.x.x.x

Class B :

- IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.
- The network ID is 16 bits long.
- The host ID is 16 bits long.
- The higher order bits of the first octet of IP addresses of class B are always set to 10.
- The remaining 14 bits are used to determine network ID. The 16 bits of host ID is used to determine the host in any network.



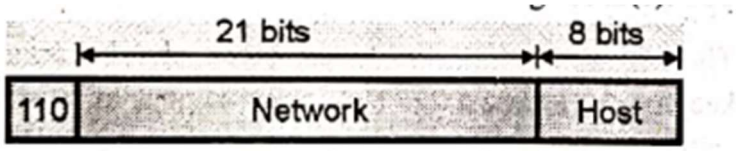
(G-532) **Fig. 5.9.2(b) : Class B format**

- The default sub-net mask for class B is 255.255.0.0
- IP addresses belonging to class B ranges from 128.0.x.x – 191.255.x.x.

Class C :

- IP address belonging to class C are assigned to small sized networks.
- The network ID is 24 bits long.
- The host ID is 8 bits long.

- The higher order bits of the first octet of IP addresses of class C are always set to 110.
- The remaining 21 bits are used to determine network ID. The 8 bits of host ID is used to determine the host in any network.



- (G-533) **Fig. 5.9.2(c) : Class C format**
- The default sub-net mask for class C is 255.255.255.0.

Classes D & E are reserved for multicast and experimental purposes respectively.

❖ Classless Addressing

Classless Inter-Domain Routing (CIDR) is another name for classless addressing. This addressing type aids in the more efficient allocation of IP addresses.

- This technique assigns a block of IP addresses based on specified conditions when the user demands a specific amount of IP addresses.
- This block is known as a "CIDR block", and it contains the necessary number of IP addresses.
- When allocating a block, classless addressing is concerned with the following three rules.
  - Rule 1 – The CIDR block's IP addresses must all be contiguous.
  - Rule 2 – The block size must be a power of two to be attractive. Furthermore, the block's size is equal to the number of IP addresses in the block.
  - Rule 3 – The block's first IP address must be divisible by the block size.

Example:

- Assume the classless address is 192.168.1.35/27.
- The network component has a bit count of 27, whereas the host portion has a bit count of 5. (32-27)
- The binary representation of the address is: (00100011 . 11000000 . 10101000 . 00000001).
- (11000000.10101000.00000001.00100000) is the first IP address (assigns 0 to all host bits), that is, 192.168.1.32
- (11000000.10101000.00000001.00111111) is the most recent IP address (assigns 1 to all host bits), that is, 192.168.1.63
- The IP address range is 192.168.1.32 to 192.168.1.63.

3. What is subnetting? Compare subnetting and super netting. What are the default subnet masks? Explain the need for subnet mask in subnetting.

Subnetting is the process of dividing a large IP network into smaller, more manageable segments called subnets. This improves the efficiency of IP address allocation and enhances network security and performance. Each subnet can function as its own small network, with its own range of IP addresses, while still being part of a larger network.

Aspect	Subnetting	Supernetting
Definition	Divides a larger network into smaller subnets.	Combines smaller networks into a larger one.
Purpose	Efficient IP address use, better network management.	Simplifies routing by reducing the size of routing tables.
Address Range	Reduces available address range.	Expands address range by aggregation.
Prefix Length	Increases prefix length (e.g., /24 → /28).	Decreases prefix length (e.g., /24 → /22).
Use Case	Used within organizations to manage internal networks.	Used by ISPs for routing optimization.
Efficiency	Reduces IP wastage within a network.	Improves routing efficiency by consolidating routes.

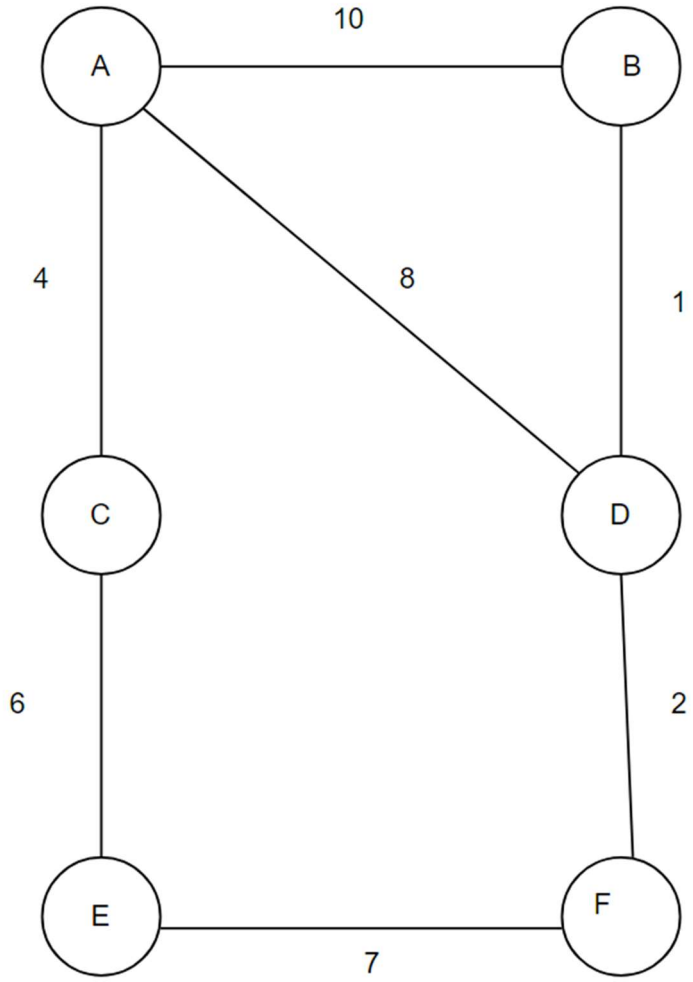
Default Subnet Masks:

- **Class A**: 255.0.0.0 (or /8)
- **Class B**: 255.255.0.0 (or /16)
- **Class C**: 255.255.255.0 (or /24)

Need for Subnet Mask in Subnetting:
A subnet mask is used in subnetting to determine which part of an IP address is the network ID and which part is the host ID. It tells devices how to separate the IP address into network and host components, ensuring that the devices know whether another IP address belongs to the same subnet or is part of a different one.
Without a subnet mask, devices would not be able to distinguish between the network portion and the host portion, leading to routing confusion and potential security risks. Subnet masks are essential for defining and maintaining the boundaries of subnets.

4. Explain Link State Routing with suitable example.

Link State Routing is a dynamic routing algorithm used in network routing. It ensures that every router has a complete map of the network topology. Each router independently calculates the shortest path to every other router using Dijkstra's algorithm. The process involves sharing information about the state (status and cost) of each link in the network.



Step-by-Step Process Using Link State Routing:

1. **Initialization**:
    - Each router creates a Link State Packet (LSP) containing:
        - Its directly connected neighbours.
        - The cost to each neighbour.
    - For example, Router A's LSP:
      A: B(10), C(4), D(8)
2. **Exchange of LSPs**:

- All routers flood their LSPs to every other router in the network.
- Each router stores the LSPs it receives from others, building a complete network topology map.
- Every router now has the same information about the network.

3. **Running Dijkstra's Algorithm**:

- Each router independently computes the shortest path to all other routers using Dijkstra's algorithm.
- Let's see how Router A calculates the shortest path:

Step 1: Start at Router A

- Distance to itself d(A)=0
- Distance to neighbours:
    - d(B)=10
    - d(C)=4
    - d(D)=8
- Other routers set to infinity (∞):
    - d(E)=∞
    - d(F)=∞

Step 2: Select the router with the shortest distance (not visited)

- Choose C (d(C)=4)
- Update distances using C's connections:
    - From C to E: d(E)=d(C)+c(C,E) =4+6= 10

Step 3: Repeat selection and update

- Next, select D (d(D)=8)
    - From D to F: d(F)=d(D)+c(D,F) =8+2 =10
- E and F both have a distance of 10, so select (e.g., B).
    - No further updates from B's neighbours.

Final Shortest Path Tree from Router A:

A → C (4) → E (6) → F (7) or D (8)

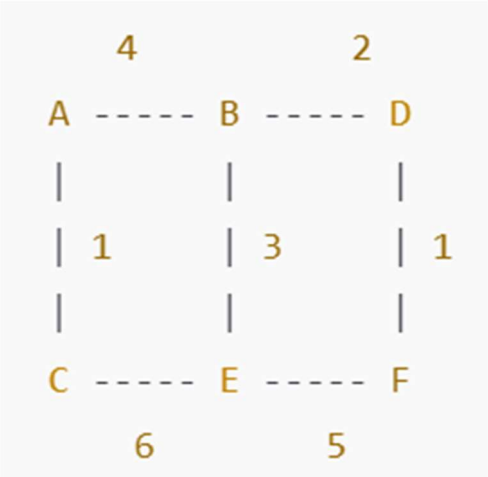
Shortest paths:

- To B: A→B with cost 10
- To C: A→C with cost 4
- To D: A→D with cost 8
- To E: A→C→E with cost 10
- To F: A→D→F with cost 10

5. Explain Distance vector routing protocol.

Distance Vector Routing is a dynamic routing protocol used in computer networks where each router maintains a routing table that stores the best-known distance (cost) to every other router in the network. Routers exchange information with their directly connected neighbours to update their routing tables. This algorithm is based on the **Bellman-Ford** algorithm.

Example:



Step by Step solution:

Step 1: Initial Routing Tables

Router	To A	To B	To C	To D	To E	To F
A	0	4	1	∞	∞	∞
B	4	0	∞	2	3	∞
C	1	∞	0	∞	6	∞
D	∞	2	∞	0	∞	1
E	∞	3	6	∞	0	5
F	∞	∞	∞	1	5	0

- Initially, each router knows the distance to its directly connected neighbors.

Step 2: Exchange Information with Neighbours

Let's say **Router A** receives information from its neighbours B and C.

- **From Router B**:
  - d(A,D)d(A, D)d(A,D) through B=d(A,B)+d(B,D) =4+2 =6
  - d(A,E)d(A, E)d(A,E) through B=d(A,B)+d(B,E) =4+3 =7
- **From Router C**:
  - d(A,E)d(A, E)d(A,E) through C=d(A,C)+d(C,E) =1+6 =7

Updated Routing Table for Router A:

To	A	B	C	D	E	F
A	0	4	1	6	7	∞

Step 3: Further Propagation

Routers continue to exchange their updated tables with neighbours:

- **Router E** will update its table with information from F.
- **Router B** updates the route to F as d(B,F)=d(B,D)+d(D,F)=2+1=3

Final Routing Table for Router B:

To	A	B	C	D	E	F
B	4	0	5	2	3	3

What is count to infinity problem. How to overcome it?

The **Count to Infinity Problem** is a major limitation of the **Distance Vector Routing (DVR)** protocol used in computer networks. It occurs when routers take a long time to converge on the correct path after a network change, such as a link failure, causing delays and routing inefficiencies.

Problem:

- If a link between two routers fails (e.g., between routers A and B), B sets its distance to A as infinite (unreachable).
- However, other routers that are still unaware of the link failure may continue to advertise outdated routes to A through B, causing B to gradually increase the distance to A in small increments.
- This results in a loop where routers keep updating the distance to a failed destination with progressively higher costs, taking a long time to realize that the destination is truly unreachable.

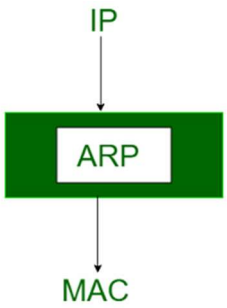
One of the most common ways **of overcoming this problem** is Split Horizon:

Split Horizon : A router does not advertise a route back to the neighbour from which it learned that route.

- **How it Works**:
    - If router **A** learns about a route to **C** from router **B**, **A** will not send information about **C** back to **B**.
- **Benefit**: Prevents routing loops by stopping routers from sending misleading information back and forth.

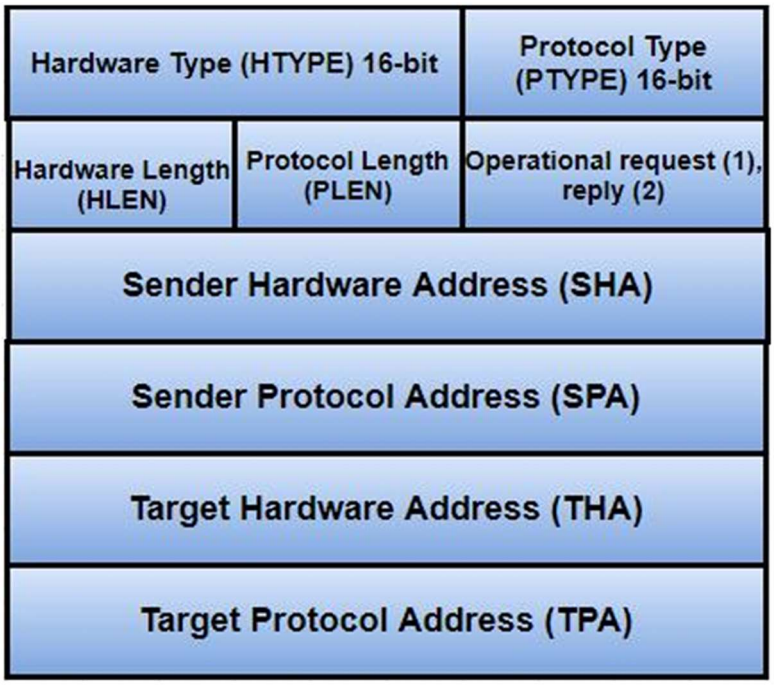
6. Explain ARP and RARP protocols in detail.

Address Resolution Protocol (ARP) is a communication protocol used to find the MAC (Media Access Control) address of a device from its IP address.
This protocol is used when a device wants to communicate with another device on a Local Area Network or Ethernet.



ARP Packet Format:

- The address resolution protocol (ARP) uses a basic message format that contains either address resolution request or address resolution response.
- The ARP message size depends on the address size of the link layer and the network layer.
- The message header describes the network type used at each layer and the address size of each layer. The message header is complete with the help of the operation code, which is 1 for request and 2 for the response



- **Hardware Type:** Specifies the type of hardware (e.g., Ethernet).
- **Protocol Type:** Specifies the protocol being used (e.g., IPv4).
- **Hardware Address Length:** Length of the MAC address.
- **Protocol Address Length:** Length of the IP address.
- **Operation Code:** Specifies if the message is an ARP Request (1) or ARP Reply (2).
- **Sender Hardware Address:** MAC address of the sender.
- **Sender Protocol Address**: IP address of the sender.
- **Target Hardware Address:** MAC address of the destination (initially unknown in an ARP Request).
- **Target Protocol Address:** IP address of the destination.

RARP

- RARP is short for Reverse Address Resolution Protocol which is a protocol based on computer networking which is employed by a client computer to request its IP address from a gateway server's Address Resolution Protocol table or cache.

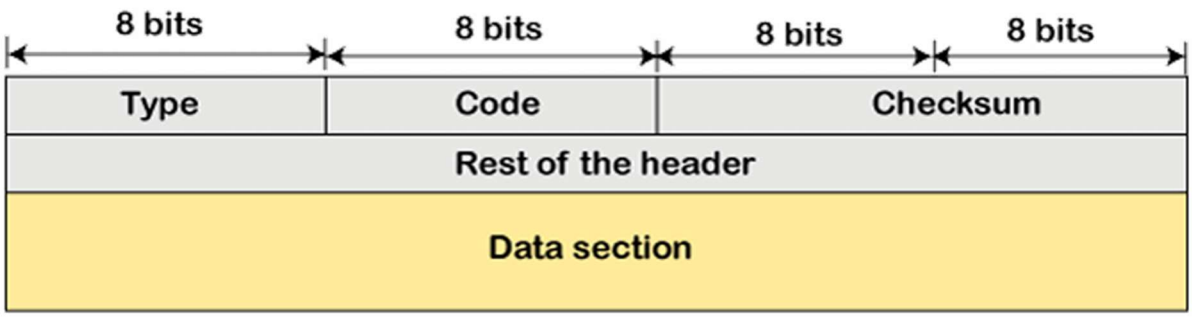
- The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address.
- The RARP is on the Network Access Layer and is employed to send data between two points in the very network. Each network participant has two unique addresses:- IP address (a logical address) and MAC address (the physical address).
- The IP address gets assigned by software and after that the MAC address is constructed into the hardware.
- The RARP server that responds to RARP requests, can even be any normal computer within the network.
- However, it must hold the data of all the MAC addresses with their assigned IP addresses.
- If a RARP request is received by the network, only these RARP servers can reply to it.

7. Write a short note on ICMP protocol.

ICMP (Internet Control Message Protocol) is a network layer protocol used for sending error messages and operational information, such as when a requested service is not available or when a router or host cannot be reached. ICMP is primarily used for diagnostic and network management purposes, but it does not facilitate the transmission of data between devices.

ICMP Message Format:

- The message format has two things; one is a category that tells us which type of message it is. If the message is of error type, the error message contains the type and the code.
- The type defines the type of message while the code defines the subtype of the message



Types of error reporting messages:

- Destination unreachable
- Source quench
- Time exceeded
- Parameter problems
- Redirection

8. What is Congestion control? Explain Open loop and closed loop congestion control.

Congestion control refers to the techniques used to control or prevent congestion. When congestion happens, it can lead to packet loss, delays, and reduced network performance. The primary goal of congestion control is to ensure efficient data transmission and maintain the quality of service in a network by regulating the amount of data entering the network and managing traffic flow effectively.

Congestion control techniques can be broadly classified into two categories:

❖ Open Loop Congestion Control

Open loop congestion control policies are applied to prevent congestion before it happens. The congestion control is handled either by the source or the destination. Key techniques include:

1. **Retransmission Policy:**
   - Manages packet retransmission if a sender thinks a packet is lost or corrupted.
   - Retransmissions can increase network congestion.
   - Effective timers are needed to optimize retransmissions and reduce congestion.
2. **Window Policy:**
   - The sender's window type affects congestion.
   - In **Go-Back-N**, multiple packets may be resent unnecessarily, increasing congestion.
   - Use **Selective Repeat** to resend only the specific lost packets.
3. **Discarding Policy:**
   - Routers can help prevent congestion by selectively discarding less important or corrupted packets.
   - For example, during audio transmission, routers can drop fewer sensitive packets to maintain overall audio quality.
4. **Acknowledgment Policy:**
   - Acknowledgments add to network load and can affect congestion.
   - The receiver should:
     - Acknowledge multiple packets (N packets) at once instead of one at a time.
     - Send an acknowledgment only when sending a packet or when a timer expires.

❖ Closed Loop Congestion Control

Closed loop congestion control techniques help manage congestion after it occurs. Key techniques include:

1. **Backpressure**:
   - A congested node stops receiving packets from upstream nodes.
   - This may cause upstream nodes to also become congested and stop receiving data.
   - It works in virtual circuits where each node knows about its upstream connections.
2. **Choke Packet Technique**:
   - Used in both virtual networks and datagram subnets.
   - A choke packet is sent from a router to the source to indicate congestion.
   - When resource use exceeds a set limit, the router sends this packet to tell the source to reduce traffic.
   - Intermediate nodes are not notified about the congestion.
3. **Implicit Signalling**:
   - There is no direct communication about congestion.
   - The source assumes congestion when it doesn’t receive acknowledgments for sent packets.

4. **Explicit Signalling**:
    - A node sends a message to the source or destination to inform them about congestion.
    - Unlike choke packets, the signal is included in regular data packets.
        - **Forward Signalling**: The signal goes towards the destination to warn about congestion.
        - **Backward Signalling**: The signal goes back to the source, telling it to slow down.

9. What is traffic shaping? Explain leaky bucket algorithm and compare it with token bucket algorithm

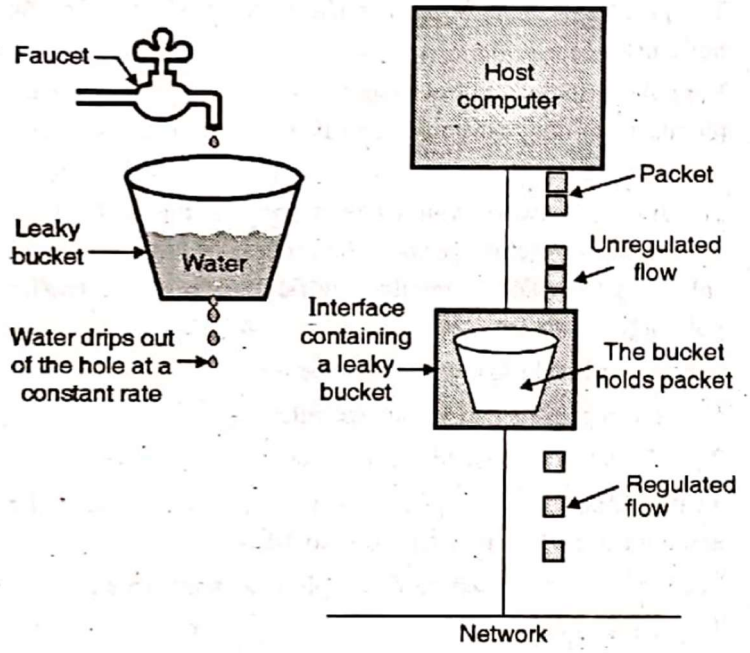
Traffic Shaping is a mechanism to control the amount and the rate of traffic sent to the network. Approach of congestion management is called Traffic shaping. Traffic shaping helps to regulate the rate of data transmission and reduces congestion.

There are 2 types of traffic shaping algorithms:

1. Leaky Bucket
2. Token Bucket

Leaky Bucket algorithm :

The **Leaky Bucket algorithm** is a traffic shaping technique that regulates the flow of data into a network. It treats incoming data packets like water filling a bucket. The water (data packets) leaks out of the bucket at a constant rate, irrespective of the rate at which it enters. This creates a steady output rate. Leaky Bucket Algorithm mainly controls the total amount and the rate of the traffic sent to the network.



• Step 1 – Let us imagine a bucket with a small hole at the bottom where the rate at which water is poured into the bucket is not constant and can vary but it leaks from the bucket at a constant rate.

• Step 2 – So (up to water is present in the bucket), the rate at which the water leaks does not depend on the rate at which the water is input to the bucket.

• Step 3 – If the bucket is full, additional water that enters into the bucket that spills over the sides and is lost.

• Step 4 – Thus the same concept applied to packets in the network. Consider that data is coming from the source at variable speeds. Suppose that a source sends data at 10 Mbps for 4

seconds. Then there is no data for 3 seconds. The source again transmits data at a rate of 8 Mbps for 2 seconds. Thus, in a time span of 9 seconds, 68 Mb data has been transmitted.

If a leaky bucket algorithm is used, the data flow will be 8 Mbps for 9 seconds. Thus, constant flow is maintained.

Difference between Leaky bucket and token bucket algorithm:

Feature	Leaky Bucket	Token Bucket
Output Rate	Fixed constant rate	Variable rate depending on tokens
Handling Bursts	Does not accommodate bursts (drops packets)	Allows for bursts (accumulates tokens)
Implementation Complexity	Simpler to implement	Slightly more complex due to token management
Efficiency	Less efficient for bursty traffic	More efficient for bursty traffic
Capacity Management	Capacity limits input traffic directly	Manages output based on token availability

10. Numerical on subnetting:

1) An ISP is granted a block of addresses starting with 190.100.0.0/16 (65,536). The ISP needs to distribute these addresses to three groups of customers as follows:
    a) The first group has 64 customers; each needs 256 addresses
    b) The second group has 128 customers; each needs 128 addresses.
    c) The third group has 128 customers; each needs 64 addresses.

   Design the subblocks and find out how many addresses are still available after these allocations.

Group 1 :

Each customer in this group needs 256 addresses i.e. suffix length is 8 ($2^8 = 256$).

∴ Prefix length = 32 – 8 = 24. The addresses are as follows :

Customer	Starting address	Ending address
1.	190.100.0.0/24	190.100.0.255/24
2.	190.100.1.0/24	190.100.1.255/24
3.	190.100.2.0/24	190.100.2.255/24
.		
.		
..		
64	190.100.63.0/24	190.100.63.255/24

Total : 64 × 256 = 16384

Group 2 :

Each customer in this group needs 128 addresses i.e. suffix length is 7 ($2^7 = 128$).

∴ Prefix length = 32 – 7 = 25. The addresses are as follows :

Customer	Starting address	Ending address
1	190.100.64.0/25	190.100.64.127/25
2.	190.100.64.128/25	190.100.64.255/25
.		
.		
.		
128	190.100.127.128/25	190.100.127.255/25

Total : 128 × 128 = 16384

Group 3 :

Each customer in this group needs 64 addresses i.e. suffix length is 6. ($2^6 = 64$).

∴ Prefix length = 32 – 6 = 26. The addresses are as follows :

Customer	Starting address	Ending address
1	190.100.128.0/26	190.100.128.63/26
2.	190.100.128.64/26	190.100.128.127/26
.		
.		
.		
128	190.100.159.192/26	190.100.159.255/26

Total = 128 × 64 = 8192

Number of granted addresses to the ISP = 65536

Number of allocated addresses by the ISP = 40960

Number of available addresses = 65536 – 40960

= 24576

2) An organization has granted a block of addresses starting with 105.8.71.0/24, organization wanted to distribute this block to 11 subnets as follows:
   a) First Group has 3 medium size businesses, each need 16 addresses
   b) The second Group has 4 medium size businesses, each need 32 addresses.
   c) The third Group has 4 households, each need 4 addresses.

   Design the sub blocks and give slash notation for each subblock. Find how many addresses have been left after this allocation.

Step 1: Understanding the Given Address Block

- **Given Block**: 105.8.71.0/24
- **Total Addresses**: A `/24` network has $2^{32-24} = 2^8 = 256$ addresses (from 105.8.71.0 to 105.8.71.255).

Step 2: Subnet Requirements

1. **First Group**: 3 medium-sized businesses, each requiring 16 addresses.
2. **Second Group**: 4 medium-sized businesses, each requiring 32 addresses.
3. **Third Group**: 4 households, each requiring 4 addresses.

Step 3: Allocating Subnets

We'll allocate subnets using CIDR (Classless Inter-Domain Routing) notation to match the required number of addresses.

Group 1: 3 subnets, each with 16 addresses

- Each needs 16 addresses → Requires a `/28` subnet (i.e., $2^{32-28} = 16$ addresses).

Subnet	Network Address	Slash Notation	Address Range
Subnet 1	105.8.71.0	/28	105.8.71.0 to 105.8.71.15
Subnet 2	105.8.71.16	/28	105.8.71.16 to 105.8.71.31
Subnet 3	105.8.71.32	/28	105.8.71.32 to 105.8.71.47

- **Total addresses used for Group 1:** $16 \times 3 = 48$ addresses.

Group 2: 4 subnets, each with 32 addresses

- Each needs 32 addresses → Requires a `/27` subnet (i.e., $2^{32-27} = 32$ addresses).

Subnet	Network Address	Slash Notation	Address Range
Subnet 1	105.8.71.48	/27	105.8.71.48 to 105.8.71.79
Subnet 2	105.8.71.80	/27	105.8.71.80 to 105.8.71.111
Subnet 3	105.8.71.112	/27	105.8.71.112 to 105.8.71.143
Subnet 4	105.8.71.144	/27	105.8.71.144 to 105.8.71.175

- **Total addresses used for Group 2:** $32 \times 4 = 128$ addresses.

Group 3: 4 subnets, each with 4 addresses

- Each needs 4 addresses → Requires a `/30` subnet (i.e., $2^{32-30} = 4$ addresses).

Subnet	Network Address	Slash Notation	Address Range
Subnet 1	105.8.71.176	/30	105.8.71.176 to 105.8.71.179
Subnet 2	105.8.71.180	/30	105.8.71.180 to 105.8.71.183
Subnet 3	105.8.71.184	/30	105.8.71.184 to 105.8.71.187
Subnet 4	105.8.71.188	/30	105.8.71.188 to 105.8.71.191

- **Total addresses used for Group 3:** $4 \times 4 = 16$ addresses.

Step 4: Calculating Remaining Addresses

- **Total addresses in original block:** 256
- **Total addresses used:**
  - Group 1: 48 addresses
  - Group 2: 128 addresses
  - Group 3: 16 addresses
- **Total used addresses:** $48 + 128 + 16 = 192$ addresses
- **Addresses left:** $256 - 192 = 64$ addresses

3) A large number of consecutive IP address are available starting at 198.16.0.0. Suppose that four organizations, A, B, C, and D, request 4000, 2000, 4000, and 8000 addresses, respectively, and in that order. For each of these. give the first IP address assigned. the last IP address assigned, and the mask in the w.x.y.z/s notation.

Starting IP Address: 198.16.0.0

Step 1: Organization A (needs 4000 addresses)

- **Required addresses**: 4000
- **IP address range**: We need a subnet that provides 4000 IP addresses. 4000 addresses require subnet mask with a /20 prefix (2^12 = 4096, which is enough for 4000 addresses).
- **Subnet Mask**: /20 (255.255.240.0)
- **First IP Address**: 198.16.0.0
- **Last IP Address**: 198.16.15.255
- **Subnet**: 198.16.0.0/20

Step 2: Organization B (needs 2000 addresses)

- **Required addresses**: 2000
- **IP address range**: A subnet for 2000 addresses requires a /21 prefix (2^11 = 2048, which is enough for 2000 addresses).
- **Subnet Mask**: /21 (255.255.248.0)
- **First IP Address**: 198.16.16.0
- **Last IP Address**: 198.16.23.255
- **Subnet**: 198.16.16.0/21

Step 3: Organization C (needs 4000 addresses)

- **Required addresses**: 4000
- **IP address range**: Same as Organization A, a /20 subnet is required.
- **Subnet Mask**: /20 (255.255.240.0)
- **First IP Address**: 198.16.24.0
- **Last IP Address**: 198.16.39.255
- **Subnet**: 198.16.24.0/20

Step 4: Organization D (needs 8000 addresses)

- **Required addresses**: 8000
- **IP address range**: A subnet for 8000 addresses requires a /19 prefix (2^13 = 8192, which is enough for 8000 addresses).
- **Subnet Mask**: /19 (255.255.224.0)
- **First IP Address**: 198.16.40.0
- **Last IP Address**: 198.16.71.255
- **Subnet**: 198.16.40.0/19

11. Compare the network layer protocols IPv4 and IPv6.

Feature	IPv4	IPv6
Address Size	32-bit (4 bytes)	128-bit (16 bytes)
Address Format	Dotted decimal (e.g., 192.168.1.1)	Hexadecimal, colon-separated (e.g., 2001:0db8:85a3::8a2e:0370:7334)
Address Space	4.3 billion addresses	340 undecillion (vastly larger)
Header Complexity	More complex with 12 fields	Simplified with 8 fields for faster processing
Fragmentation	Routers and sending hosts can fragment	Only sending hosts can fragment
Security Features	Security is optional (IPSec is not mandatory)	IPSec is mandatory, providing stronger security support
Broadcast Support	Supports broadcasting	No broadcast; uses multicast and anycast instead
Routing Table Size	Larger, due to more complex routing	Smaller, optimized for more efficient routing
Configuration	Manual (DHCP) or automatic configuration	Supports both stateless (SLAAC) and stateful (DHCPv6) auto-configuration
Checksum	Includes checksum in the header	No checksum (error checking is handled by other layers)
Mobility and Multihoming	Limited support	Better support for mobility and multiple addresses
NAT (Network Address Translation)	Commonly used due to address shortage	Not required because of the large address space

12. Write a short note on Network Address Translation(NAT).

Network Address Translation (NAT) is a technique used in networking to translate the private (internal) IP addresses of devices within a local network to a single public (external) IP address. NAT is commonly implemented in routers and serves several key functions.

The idea of NAT is to allow multiple devices to access the Internet through a single public address. Also, it does the translation of port numbers i.e., masks the port number of the host with another port number, in the packet that will be routed to the destination.
It then makes the corresponding entries of IP address and port number in the NAT table.

Advantages of NAT

1. NAT conserves legally registered IP addresses.
2. It provides privacy as the device's IP address, sending and receiving the traffic, will be hidden.
3. Eliminates address renumbering when a network evolves.

Disadvantage of NAT

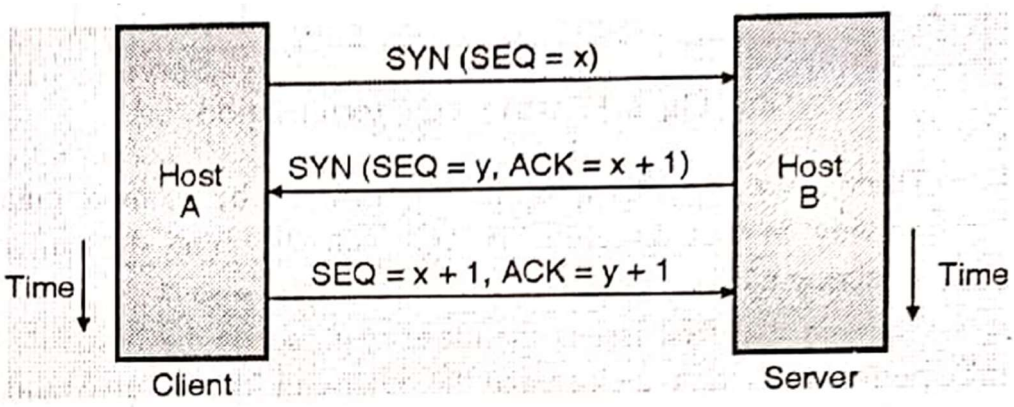
1. Translation results in switching path delays.
2. Certain applications will not function while NAT is enabled.

5. Transport layer (10-25 marks)

1. Explain the TCP connection establishment (Three-Way Handshake technique) .

TCP Connection Establishment (Three-Way Handshake)

- Handshake refers to the process to establish connection between the client and server. Handshake is simply defined as the process to establish a communication link.
- The reliable communication in TCP is termed as PAR (Positive Acknowledgement Retransmission).
- The process of establishing a connection in TCP involves a three-way handshake, which ensures a reliable connection is set up between a client and a server. The steps are as follows:



(G-613) **Fig. 6.17.1(a) : TCP connection establishment (Three-way handshake)**

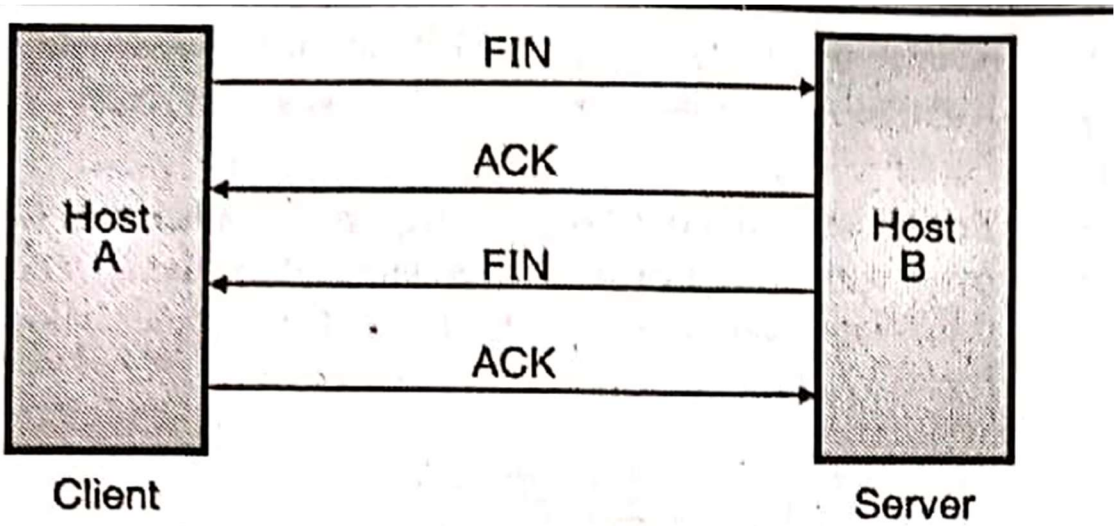
- **Step 1: SYN (Synchronize)**
  - SYN is a segment sent by the client to the server.
  - It acts as a connection requests between the client and server.
  - The client sends a TCP segment with the SYN (synchronize) flag set to 1. This indicates the client wants to establish a connection, and it sends a sequence number (SEQ) to the server.
- **Step 2: SYN-ACK (Synchronize-Acknowledgement)**
  - It is an SYN-ACK segment or an SYN + ACK segment sent by the server.
  - The server responds with a segment where both the SYN and ACK (acknowledge) flags are set to 1.
  - The SYN is used to synchronize the connection, and the ACK is an acknowledgment that the server received the client's SYN.
  - The server also sends its sequence number and acknowledges the client's sequence number by setting (ACK) as the client's sequence number + 1.
- **Step 3: ACK (Acknowledgement)**
  - ACK (Acknowledgment) is the last step before establishing a successful TCP connection between the client and server.
  - The ACK segment is sent by the client as the response of the received ACK and SYN from the server. It results in the establishment of a reliable data connection.
  - After these three steps, the client and server are ready for the data communication process.

2. Explain TCP Connection release

TCP Connection Release (Four-Way Handshake)

To release a TCP connection, a four-step process is used, where both the client and server agree to terminate the connection. The steps are as follows:

- **Step 1: FIN** (Finish)
  - The client sends a FIN segment to indicate it has finished sending data and wants to close the connection.
- **Step 2: ACK**
  - The server acknowledges the FIN by sending an ACK, but the server may still need to send data, so the connection is not fully closed yet.
- **Step 3: FIN**
  - The server sends a FIN segment when it has finished sending all its data.
- **Step 4: ACK**
  - The client sends a final ACK to confirm that it received the server's FIN, and the connection is fully closed.



(G-614) Fig. 6.17.1(b) : TCP termination

3. Differentiate between TCP and UDP.

Parameters	TCP	UDP
Connection type	Connection-oriented	Connectionless
Reliability	Reliable, ensures data delivery.	Unreliable, doesn't guarantee delivery of packets.
Header size	20 bits	8 bits
Speed	Slower than UDP.	Fast
Flow control	Provides flow control	Doesn't provide flow control.
Retransmission	Retransmission of lost data is possible.	Retransmission of lost data is not possible.
Error control	Provided.	Only checksum.
Used in	HTTP, SMTP, FTP.	Multimedia applications, DNS, DHCP

4. Write a shot note on TCP Timers.

TCP uses several timers to ensure that excessive delays are not encountered during communications. Several of these timers are elegant, handling problems that are not immediately obvious at first analysis.

Each of the timers used by TCP is examined in the following sections, which reveal its role in ensuring data is properly sent from one connection to another.

TCP has four timers:

1. **Keep-alive timer:**
    - This timer is used to check the integrity and validity of a connection.
    - When keep-alive time expires, the host sends a probe to check if the connection still exists.
2. **Retransmission timer:**
    - This timer maintains stateful session of data sent.
    - If the acknowledgement of sent data does not receive within the Retransmission time, the data segment is sent again.
3. **Persist timer:**
    - TCP session can be paused by either host by sending Window Size 0.
    - When the Persist timer expires, the host re-sends its window size to let the other end know.
    - Persist Timer helps avoid deadlocks in communication.
4. **Timed-Wait:**
    - After releasing a connection, either of the hosts waits for a Timed-Wait timer to terminate the connection completely.

- This is in order to make sure that the other end has received the acknowledgement of its connection termination request.

5. Explain Slow-Start algorithm for TCP's congestion handling policy.

Slow Start Phase

Initially, sender sets congestion window size = Maximum Segment Size (1 MSS).

After receiving each acknowledgment, sender increases the congestion window size by 1 MSS.

In this phase, the size of congestion window increases exponentially.

Congestion window size =

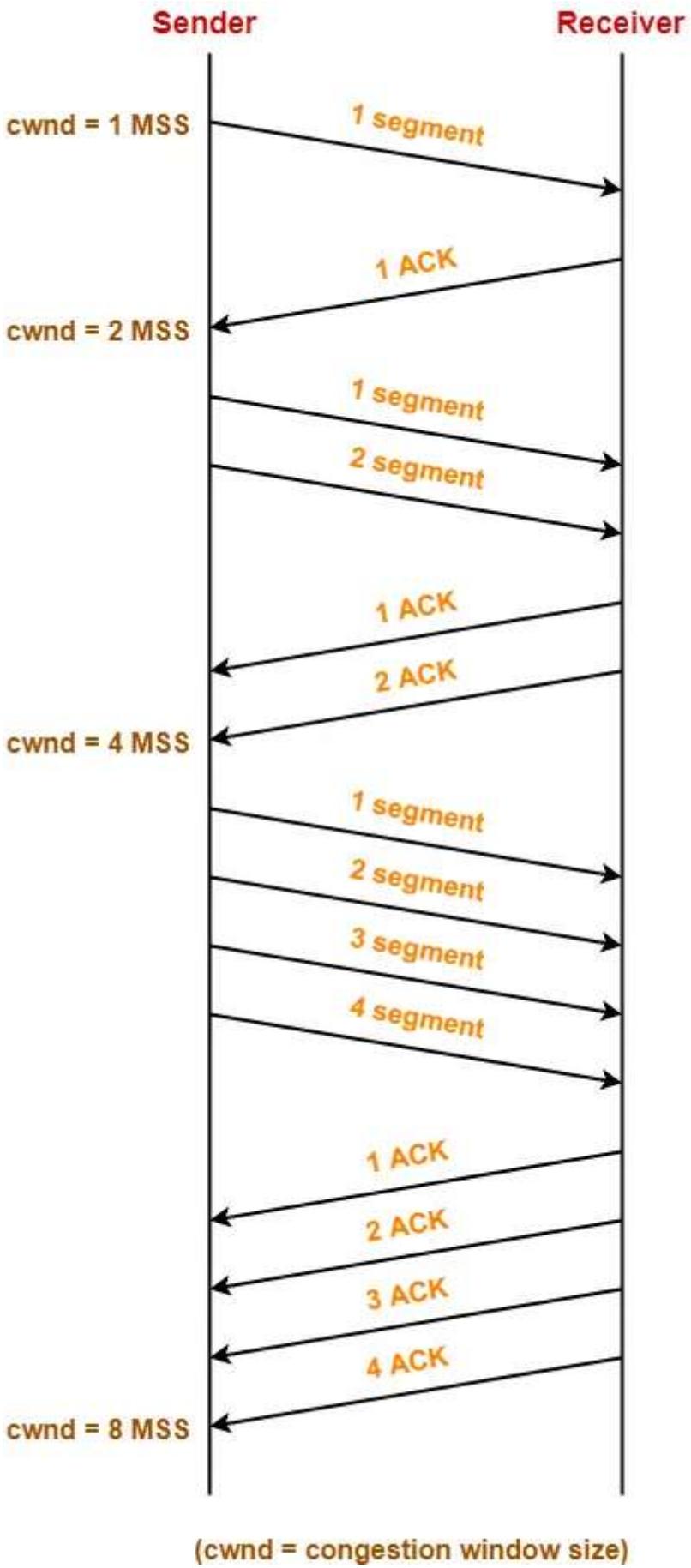
Congestion window size + Maximum segment size

- After 1 round trip time, congestion window size = $(2)^1$ = 2 MSS
- After 2 round trip time, congestion window size = $(2)^2$ = 4 MSS
- After 3 round trip time, congestion window size = $(2)^3$ = 8 MSS and so on.

This phase continues until the congestion window size reaches the slow start threshold.

Threshold = Maximum number of TCP segments that receiver window can accommodate / 2

∴ Threshold = (Receiver window size / Maximum Segment Size) / 2



6. Explain TCP flow control.

TCP Flow Control ensures that a sender does not overwhelm the receiver with more data than it can handle. This is achieved using the **sliding window mechanism**, where the receiver informs the sender about the amount of available buffer space it has for incoming data.

- **Receiver Window Size (rwnd)**: The receiver tells the sender how much data it can accept by specifying the window size in the TCP header. This is the amount of unacknowledged data the sender can send.
- **Sliding Window**: The sender can send data up to the size of the receiver's specified window. As the receiver processes data, it moves the window forward, allowing the sender to send more.
- **Zero Window**: If the receiver's buffer is full, it specifies a window size of 0, instructing the sender to stop sending data until more space is available.
- **Window Scaling**: For high-speed networks, TCP can use window scaling to allow a larger window size (more than 65,535 bytes) to improve performance.

In short, TCP flow control prevents the sender from sending more data than the receiver can process, ensuring smooth data transfer.

6. Application layer (10-20 marks)

1. What is need of DNS and explain how DNS works? Explain DNS namespace.

Need for DNS (Domain Name System):
DNS is essential for translating human-readable domain names (like example.com) into IP addresses (such as 192.0.2.1) that computers use to identify each other on a network, particularly the Internet. Since humans find it easier to remember domain names rather than numerical IP addresses, DNS enables seamless communication between devices by handling the translation between the two.

Without DNS, users would need to remember the IP addresses of websites and services, which would be impractical as networks grow.

How DNS Works(or DNS functioning)

1. **User Request (DNS Query)**:
    - When a user types a URL like www.example.com into a browser, the browser checks if the IP address corresponding to the domain is stored locally (in its cache).
    - If not found, it initiates a DNS query to resolve the domain name into an IP address.
2. **Recursive Resolver**:
    - The query is sent to a DNS resolver, which acts as a middleman between the user and the DNS system. The resolver starts by checking its local cache, and if the domain is not cached, it proceeds with further steps.
3. **Root Server**:
    - If the recursive resolver doesn't have the IP address, it contacts a root DNS server, which is the first step in DNS hierarchy. The root server responds with the IP address of a **Top-Level Domain (TLD)** server (like .com, .net).
4. **TLD Server**:
    - The resolver then queries the TLD server (e.g., .com TLD for example.com), which responds with the IP address of the authoritative DNS server for the requested domain.
5. **Authoritative DNS Server**:
    - The resolver sends the query to the authoritative DNS server for example.com. This server contains the DNS records (like A, AAAA records) that map the domain to its corresponding IP address.
6. **Response to the User**:
    - The authoritative DNS server responds with the IP address of the domain. The resolver caches the result and returns it to the browser, allowing the browser to connect to the server at that IP address.

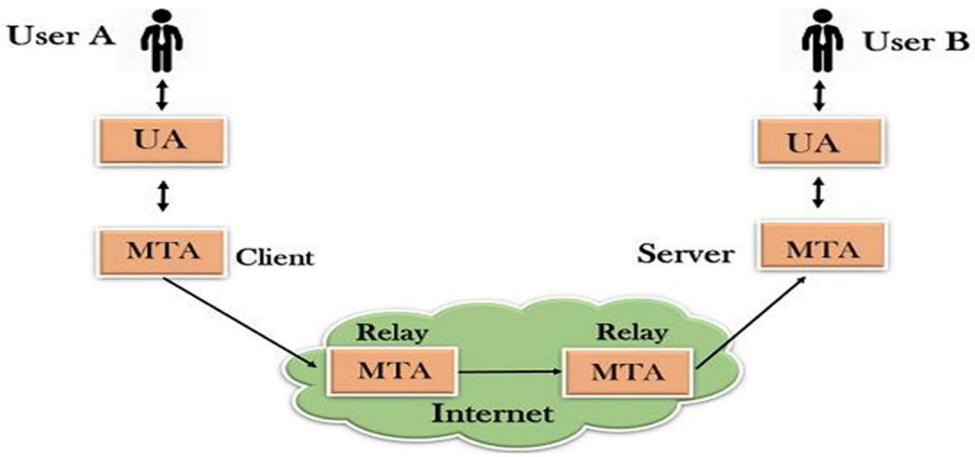
DNS Namespace

The DNS namespace is hierarchical and divided into multiple levels, each representing a different part of a domain name:

1. **Root Level**:
    - Represented by a single dot (.) and is at the top of the hierarchy. The root level contains root servers responsible for directing queries to the appropriate TLD servers.
2. **Top-Level Domains (TLDs)**:
    - Located directly under the root. These include common domains like .com, .org, .net, country-code TLDs like .uk, and newer generic TLDs like .xyz.
3. **Second-Level Domains**:
    - These are domains registered under a TLD, like example in example.com. They are managed by the domain owner.
4. **Subdomains**:
    - Subdomains are optional and can exist under a second-level domain, like blog.example.com.

2. Write a short note on SMTP.

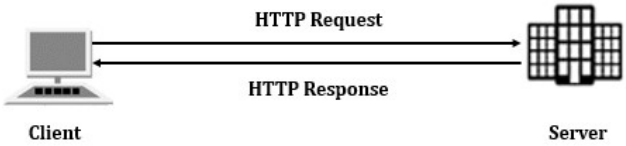
- SMTP stands for Simple Mail Transfer Protocol.
- SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called Simple Mail Transfer Protocol.
- It is a program used for sending messages to other computer users based on e-mail addresses.
- It provides a mail exchange between users on the same or different computers, and it also supports:
    - It can send a single message to one or more recipients.
    - Sending message can include text, voice, video or graphics.
    - It can also send the messages on networks outside the internet.



SMTP server can be broken down into two components such as user agent (UA) and mail transfer agent (MTA). The user agent (UA) prepares the message, creates the envelope and then puts the message in the envelope. The mail transfer agent (MTA) transfers this mail across the internet.

3. Explain HTTP. Draw and summarize the structure of HTTP request and response.

Hyper Text Transfer Protocol (HTTP) is a stateless protocol used for transmitting hypertext across the web. It functions as the foundation for any data exchange on the Web and facilitates communication between clients (browsers) and servers. HTTP uses methods like GET, POST, PUT, DELETE, etc., for different types of operations. It operates over TCP, typically using port 80. The protocol follows a request-response pattern where the client initiates a request, and the server sends a corresponding response.



HTTP Request:

The HTTP request is sent from the client to the server. It includes the request line, headers, and an optional message body.

1. **Request Line**: Specifies the HTTP method, the resource being requested, and the HTTP version.
    - Example: GET /index.html HTTP/1.1
2. **Headers**: Provide metadata about the request (e.g., browser type, content type, and accepted languages).
    - Example headers:
        - Host: www.example.com
        - User-Agent: Mozilla/5.0
        - Accept: text/html
3. **Body**: (Optional) Contains data sent to the server (mainly for POST and PUT requests).
    - Example: Form data or JSON payload.

HTTP Request Example:

GET /index.html HTTP/1.1 ----------Request line

Host: www.example.com ----------Header

User-Agent: Mozilla/5.0

Accept: text/html

----------Blank line separating header & body

Book ID=12345 ----------Request message body

HTTP Response:

The HTTP response is sent from the server to the client after processing the request. It consists of the status line, headers, and the message body.

1. **Status Line**: Contains the HTTP version, status code, and reason phrase.
    - Example: HTTP/1.1 200 OK
2. **Headers**: Provide metadata about the response (e.g., content type, length, server details).
    - Example headers:
        - Content-Type: text/html
        - Content-Length: 348
3. **Body**: (Optional) Contains the content requested by the client (e.g., HTML, JSON, images).
    - Example: <html>...</html>

HTTP Response Example:

HTTP/1.1 200 OK ----------Status line

Content-Type: text/html ----------Header

Content-Length: 137

----------Blank line separating header & body

<html> ----------Response message body

<body>

<h1>Hello, World!</h1>

</body>

</html>

4. Explain working(or operation) of DHCP protocol.

The **Dynamic Host Configuration Protocol (DHCP)** is used to automatically assign IP addresses and other network configuration details (such as subnet mask, gateway, and DNS servers) to devices on a network. This removes the need for manual IP address assignment and simplifies network administration, especially in large networks.

Key Components in DHCP

1. **DHCP Server**: A network device (usually a router or a dedicated server) that holds the pool of IP addresses and manages the assignment of these addresses.
2. **DHCP Client**: A device (computer, smartphone, IoT device) that requests an IP address from the DHCP server when it connects to the network.
3. **IP Address Pool**: A range of IP addresses that the DHCP server can assign to clients.
4. **Lease Time**: The duration for which an IP address is assigned to a client. After the lease expires, the client must renew the IP address, or it will be released for other clients to use.

How DHCP Works (The DORA Process)

DHCP works using a four-step process known as **DORA**:

1. **Discovery**
2. **Offer**
3. **Request**
4. **Acknowledge**

1. DHCP Discovery (DHCPDISCOVER)

- When a DHCP client (e.g., a computer) joins the network and needs an IP address, it broadcasts a **DHCPDISCOVER** message to the network.

2. DHCP Offer (DHCPOFFER)

- A DHCP server that receives the **DHCPDISCOVER** message checks its available IP address pool and reserves an IP address for the client.

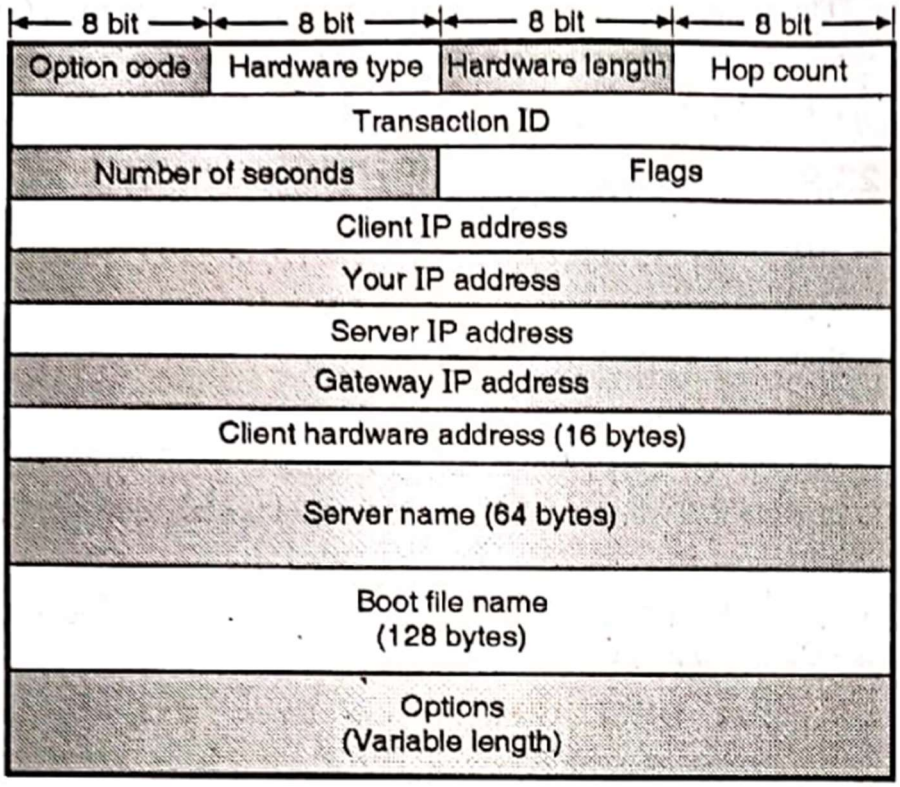
3. DHCP Request (DHCPREQUEST)

- The client receives one or more **DHCPOFFER** messages from DHCP servers (if multiple DHCP servers exist on the network). It selects one of the offers, usually the first received, and responds with a **DHCPREQUEST** message to the selected DHCP server.

4. DHCP Acknowledgment (DHCPACK)

- Upon receiving the **DHCPREQUEST**, the chosen DHCP server finalizes the process by sending a **DHCPACK** (acknowledgment) message.

5. Explain DHCP message format in detail.



DHCP Message Format (Fields):

1. **Operation Code (op)**:
   - 1 byte.
   - Indicates whether the message is a request (1) from the client or a reply (2) from the server.
2. **Hardware Type (htype)**:
   - 1 byte.
   - Specifies the type of hardware address (e.g., 1 for Ethernet).
3. **Hardware Address Length (hlen)**:
   - 1 byte.
   - Length of the hardware (MAC) address.
4. **Hops**:
   - 1 byte.
   - Used by relay agents to forward DHCP messages across networks.
5. **Transaction ID (xid)**:
   - 4 bytes.
   - A random number generated by the client to identify the DHCP transaction and match requests with responses.

6. **Seconds (secs)**:
    - 2 bytes.
    - The number of seconds elapsed since the client started the DHCP request process.
7. **Flags**:
    - 2 bytes.
    - Includes a broadcast flag, which indicates whether the client can receive unicast or broadcast replies.
8. **Client IP Address (ciaddr)**:
    - 4 bytes.
    - The client's IP address (if it already has one; otherwise, it is set to 0).
9. **Your IP Address (yiaddr)**:
    - 4 bytes.
    - The IP address being assigned to the client by the server.
10. **Server IP Address (siaddr)**:
    - 4 bytes.
    - IP address of the DHCP server providing the IP lease.
11. **Gateway IP Address (giaddr)**:
    - 4 bytes.
    - Used by relay agents when forwarding DHCP messages between networks.
12. **Client Hardware Address (chaddr)**:
    - 16 bytes.
    - The MAC address of the client requesting an IP address.
13. **Server Host Name (sname)**:
    - 64 bytes (optional).
    - The server’s host name, if applicable.
14. **Boot File Name (file)**:
    - 128 bytes (optional).
    - The name of a boot file to be used by diskless clients.
15. **Options**:
    - Variable length.
    - This field is used to carry additional options like the subnet mask, DNS server, default gateway, lease time, etc.