CN Theory Assignment - 3

1.Station A needs to send a message consisting of 8 data frames to Station B using a sliding window (Widow size 3) and Go-Back-N error control strategy. All data frames are ready and immediately available for transmission. If the 4th frame that A transmit gets lost (but no ACKs from B ever get lost), then what is the number of frames that A will transmit for sending the message to B.

In a Go-Back-N protocol with a sliding window, when a frame is lost, all subsequent frames in the window need to be retransmitted. Here, the window size is 3, and the 4th frame is lost. This means that after the loss is detected, Station A will need to retransmit the 4th frame and all the frames following it within the window.

So, Station A will transmit a total of 6 frames to successfully send the message to Station B:

- Original transmission of frames 1, 2, 3, 4 (lost), 5, 6, 7, 8
- Retransmission of frames 4, 5, 6, 7, 8

2.Briefly explain different versions of CSMA protocol.

1. **CSMA/CD (Carrier Sense Multiple Access with Collision Detection):**
    - **Use:** In wired networks like Ethernet.
    - **Operation:** Nodes sense the channel, transmit if clear, and handle collisions by stopping and initiating a backoff.
2. **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance):**
    - **Use:** In wireless networks like Wi-Fi.
    - **Operation:** Nodes sense the channel, wait if busy, and use RTS/CTS to reserve the channel, avoiding collisions.
3. **CSMA/CR (Carrier Sense Multiple Access with Collision Resolution):**
    - **Use:** In networks where collision resolution is preferred.
    - **Operation:** Nodes continue transmitting after collisions, adjusting power levels to resolve collisions more efficiently than CSMA/CD.

3.State the difference between thick and thin Ethernet.

Thick Ethernet (10BASE5):

- Cable: Thick and rigid coaxial cable (0.4 inches).
- Segment Length: Up to 500 meters.
- Attachment: Uses vampire taps.
- Topology: Bus topology.
- Cost and Installation: More expensive and challenging to install.

Thin Ethernet (10BASE2):

- Cable: Thin and flexible coaxial cable (0.2 inches).
- Segment Length: Up to 185 meters.
- Attachment: Uses T-connectors.
- Topology: Bus topology.
- Cost and Installation: More cost-effective and easier to install.

Both technologies are early forms of coaxial cable-based Ethernet, with Thick Ethernet suitable for larger networks, while Thin Ethernet is more adaptable and cost-effective for smaller setups.

Modern networks predominantly use twisted-pair cables and fiber optics.

4.Classify hub and switch. Briefly explain the functioning of switched Ethernet

Hub:

- **Classification:** Hub is a Layer 1 (physical layer) networking device.
- **Functionality:** Operates at the OSI model's physical layer, where it simply repeats incoming electrical signals to all connected devices in the network, regardless of the destination. Hubs do not have the capability to intelligently manage or filter traffic.

Switch:

- **Classification:** Switch is a Layer 2 (data link layer) networking device.
- **Functionality:** Operates at the OSI model's data link layer, making forwarding decisions based on MAC addresses. Unlike hubs, switches are more intelligent and can selectively send data only to the device it is intended for, improving network efficiency and reducing collisions.

Switched Ethernet Functioning: Switches in Ethernet networks operate at the data link layer, using MAC address tables for efficient frame forwarding. Key points include:

1. **MAC Address Learning:** Switches build tables mapping MAC addresses to specific ports by observing incoming frames.
2. **Frame Forwarding:** Frames are selectively forwarded only to the port where the destination device is connected, reducing unnecessary traffic.
3. **Reduced Collision Domain:** Each device connected to a switch has a separate collision domain, preventing collisions and improving network performance.
4. **Filtering and Efficiency:** Switches filter traffic at the data link layer, enhancing network efficiency by minimizing broadcast and unnecessary transmissions.
5. **Full-Duplex Operation:** Switched Ethernet supports full-duplex communication, enabling simultaneous data transmission and reception for connected devices.

5.Briefly elaborate the infrastructure based and ad hoc structure of Wireless LAN 802.11 architecture.

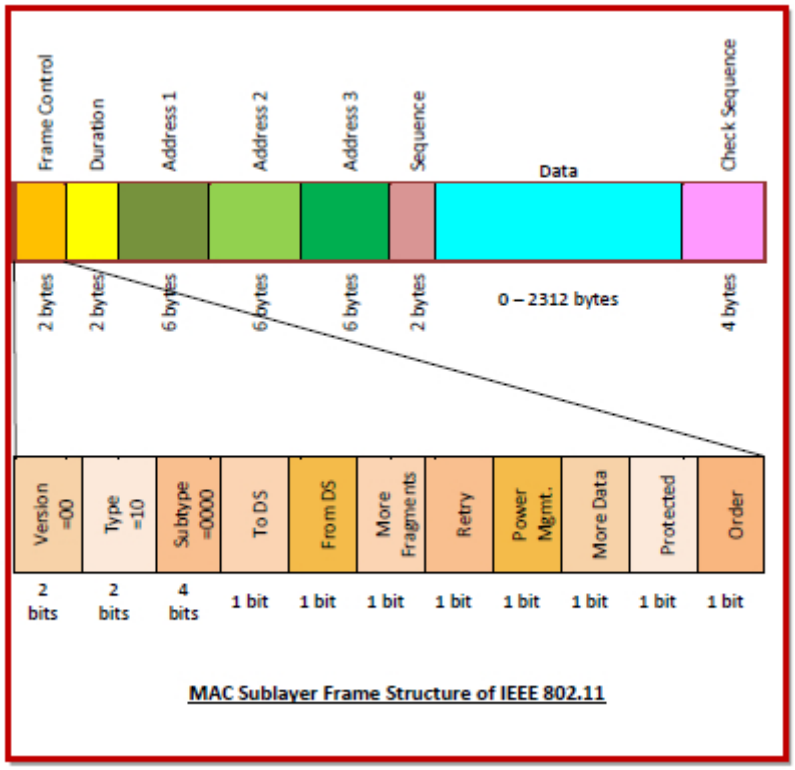
Infrastructure Mode (Infrastructure-Based):

- Centralized network with an Access Point (AP) managing communication.
- Ideal for business and home networks requiring centralized control.

Ad Hoc Mode (Peer-to-Peer):

- Devices communicate directly without an access point.
- Suitable for temporary or spontaneous setups without a centralized infrastructure.

6.With neat diagram describe the 802.11 frame structure.



The 802.11 frame structure typically consists of the following fields:

1. **Frame Control:** Contains information about the type and control of the frame, including protocol version, frame type, and subtype.
2. **Duration/ID:** Specifies the duration the medium will be reserved for the frame transmission and may also include an association ID.
3. **Address Fields:**
    - **Receiver Address (RA):** MAC address of the recipient.
    - **Transmitter Address (TA):** MAC address of the sender.
    - **BSSID (Basic Service Set Identifier):** MAC address representing the basic service set (BSS).
4. **Sequence Control:** Manages the order of frame transmission and reception.
5. **Frame Body:** Contains the actual data payload or information being transmitted.
6. **Frame Check Sequence (FCS):** CRC (Cyclic Redundancy Check) for error detection.
7. **Frame Control (optional):** Certain frames may have a second Frame Control field for additional control information.

7.Compare the implementation of connection less and connection-oriented service by network layer.

Connectionless Service:

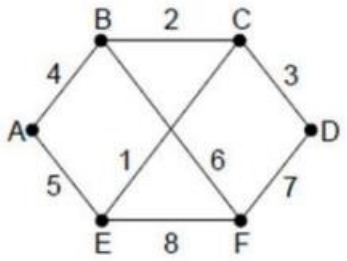
- **Protocol:** IP (Internet Protocol)
- **Handling:** Packets treated independently, stateless, efficient for bursty communication.
- **Example:** UDP (User Datagram Protocol)

Connection-Oriented Service:

- **Protocol:** TCP (Transmission Control Protocol)
- **Establishment:** Three-way handshake for connection setup, stateful communication.
- **Reliability:** Ensures reliable, ordered delivery, with overhead for connection setup.
- **Example:** TCP for reliable and ordered data delivery.

8.Explain the importance of routing algorithm as one of the design issues. Consider the below shown network, where the weights on the lines indicates the distance. Determine the shortest route from A to D using Dijkstra algorithm.

Routing algorithms are foundational to the design and operation of computer networks, impacting efficiency, reliability, fault tolerance, security, and overall network performance. Careful consideration and selection of appropriate routing strategies are essential for building robust and effective communication infrastructures.



With the provided weights on the network edges, we can use Dijkstra's algorithm to find the shortest path from A to D.
The shortest path from A to D is A -> B -> C -> D with a total distance of 9.

9.Briefly explain how flooding algorithm works to find the route between a pair of routers.

In flooding, a router forwards a packet to all neighboring routers, which, in turn, forward it to their neighbors. The process continues until the packet reaches the destination. While simple, it may cause network congestion and redundant transmissions. Loop prevention mechanisms, like sequence numbers, are often employed.

10.Discuss the significance of each field in IP header.

The IP header contains several fields, each serving a specific purpose in the delivery of data across networks. Here's the significance of some key fields:

1. **Version (4 bits):**
    - Identifies the version of the IP protocol (IPv4 or IPv6).
2. **Header Length (4 bits):**
    - Indicates the length of the IP header in 32-bit words.
3. **Type of Service (8 bits):**
    - Specifies the quality of service for packet prioritization, handling, and delivery.
4. **Total Length (16 bits):**
    - Represents the total size of the IP packet (header + data).

5. **Identification (16 bits):**
    - A unique identifier assigned to fragmented IP packets for reassembly at the destination.
6. **Flags (3 bits) and Fragment Offset (13 bits):**
    - Flags control fragmentation. Fragment Offset indicates the position of the fragment in the original unfragmented packet.
7. **Time-to-Live (TTL - 8 bits):**
    - Limits the lifespan of a packet, preventing it from circulating indefinitely in the network.
8. **Protocol (8 bits):**
    - Identifies the higher-layer protocol that will receive the packet from the IP layer (e.g., TCP, UDP).
9. **Header Checksum (16 bits):**
    - Provides error-checking for the IP header to ensure data integrity during transmission.
10. **Source Address (32 bits) and Destination Address (32 bits):**
    - Source Address: The IP address of the sender.
    - Destination Address: The IP address of the intended recipient.
11. **Options (variable length):**
    - Optional fields providing additional information or control options. Rarely used due to efficiency concerns.
12. **Padding (variable length):**
    - Fills the header to ensure proper alignment.

11.Classify the IP V4 addressing on the basis of host and network. Determine the class of the following addresses: (i) 227.13.14.88 (ii) 25.34.12.56

IPv4 addresses are classified into different classes based on the number of network and host bits. The common classes are A, B, C, D, and E. The class of an IPv4 address is determined by the value of its first octet. Here's the classification:

1. **Class A (1.0.0.0 to 126.255.255.255):**
    - First octet: 1 to 126
    - Example: 25.34.12.56 is in Class A.
2. **Class B (128.0.0.0 to 191.255.255.255):**
    - First octet: 128 to 191
    - Example: 227.13.14.88 is in Class B.
3. **Class C (192.0.0.0 to 223.255.255.255):**
    - First octet: 192 to 223
4. **Class D (Multicast addresses - 224.0.0.0 to 239.255.255.255):**
    - First octet: 224 to 239
5. **Class E (Reserved for experimental use - 240.0.0.0 to 255.255.255.255):**
    - First octet: 240 to 255

Now, determining the class of the provided addresses:

(i) **227.13.14.88:**

- First octet: 227
- Class: Class D (Multicast)

(ii) **25.34.12.56:**

- First octet: 25
- Class: Class A

So, the classification is:

- (i) 227.13.14.88 is in Class D (Multicast).
- (ii) 25.34.12.56 is in Class A.

12.State the difference between IPV6 and IPV4 addressing.

IPv4:

- 32-bit addresses (4.3 billion).
- Dotted-decimal notation.
- Manual or DHCP configuration.
- Unicast, broadcast, and multicast.
- NAT commonly used due to address scarcity.
- More complex header with checksum.

IPv6:

- 128-bit addresses (vastly more).
- Hexadecimal notation.
- Stateless autoconfiguration, DHCPv6, or manual config.
- Primarily unicast, multicast, and anycast.
- No NAT due to a vast address space.
- Simplified header with fewer fields.

13.Briefly elaborate the difference between TCP and UDP.

TCP (Transmission Control Protocol):

- **Connection-oriented:** Establishes a reliable and ordered connection before data transfer.
- **Reliability:** Provides error checking, retransmission of lost packets, and in-order delivery.
- **Flow Control:** Uses sliding window mechanism to manage data flow.
- **Acknowledgments:** Requires acknowledgments for each transmitted segment.
- **Usage:** Suitable for applications requiring reliable, error-free, and ordered data delivery, such as web browsing, email, file transfer (FTP).

UDP (User Datagram Protocol):

- **Connectionless:** Does not establish a connection before data transfer.
- **Reliability:** Best-effort delivery with no error checking or retransmission.
- **Flow Control:** No inherent flow control mechanism.
- **Acknowledgments:** No acknowledgments for sent packets.
- **Usage:** Suitable for applications where speed and low latency are crucial, such as real-time video streaming, online gaming, DNS.

14.Explain, the importance of DNS name space. Also enumerate, how DNS helps to get the IP address against a domain name.

Importance of DNS Name Space:

- **Human-Readable Naming:** Provides a readable and universal naming system for internet resources.
- **Universal Identification:** Allows users worldwide to access resources using consistent and memorable names.
- **Centralized Management:** Facilitates centralized control of domain names for organizations.
- **Scalability:** Accommodates the dynamic nature of the internet with a scalable and distributed database.
- **Redundancy and Load Distribution:** Implements redundancy and load distribution for reliability.

How DNS Resolves IP Addresses:

1. **User Input:** Enters domain name.
2. **Local DNS Cache Check:** Checks local cache for the IP address.
3. **Recursive Query:** Initiates recursive query to root DNS server.
4. **Root and TLD Servers:** Receives referrals from root and TLD servers.
5. **Authoritative Server:** Queries authoritative server for the specific domain.
6. **Local Cache Update:** Updates local cache with the IP address.
7. **IP Address Return:** Returns the IP address to the user for connection establishment.

15.Imagine you are the Cryptography team lead and the organisation is under a digital attack, explain the steps that should be adopted to handle the situation.

Cryptography Team Lead's Response to a Digital Attack:

1. **Identification:**
    - Swiftly identify and understand the digital attack's type and scope.
2. **Isolation:**
    - Isolate affected systems to contain the attack.
3. **Notification:**
    - Notify stakeholders and establish communication protocols.
4. **Engage Response Team:**
    - Activate the cybersecurity response team for analysis and strategy.
5. **Evidence Preservation:**
    - Preserve digital evidence for forensic analysis.
6. **Coordinate with Law Enforcement:**
    - Collaborate with law enforcement, providing evidence.
7. **Mitigation Measures:**

- Implement immediate measures to neutralize the attack.

8. **Cryptographic Key Management:**
   - Assess and rotate compromised cryptographic keys if needed.
9. **Security Awareness:**
   - Conduct security awareness programs for employees.
10. **Root Cause Analysis:**
    - Investigate and identify vulnerabilities comprehensively.
11. **Security Enhancements:**
    - Implement enhancements based on root cause analysis.
12. **Post-Incident Review:**
    - Evaluate response effectiveness and document lessons.
13. **Legal Compliance:**
    - Ensure compliance with legal and regulatory requirements.
14. **Public Relations:**
    - Manage public relations to protect the organization's reputation.
15. **Continuous Monitoring:**
    - Implement continuous monitoring and adapt security measures.
16. **Documentation:**
    - Document incident response details and provide reports.
17. **Employee Assistance:**
    - Offer support to affected employees and reinforce cybersecurity awareness.
18. **Tabletop Exercises:**
    - Conduct regular exercises to test the incident response plan.