Computer Networks Assignment-2

M.kiran raj

AIML-D

2023PECML350

Q1: Compare and contrast the features of HDLC and Frame Relay in networking.

HDLC (High-Level Data Link Control):

1. **Protocol Type**: HDLC is a bit-oriented protocol that operates at the data link layer (Layer 2) of the OSI model.
2. **Connection**: Primarily designed for point-to-point and point-to-multipoint configurations.
3. **Error Handling**: Includes robust error detection and correction mechanisms, such as automatic retransmissions in case of errors.
4. **Efficiency**: Less efficient in high-speed networks due to overhead from extensive error control.
5. **Flow Control**: Implements flow control to manage data flow between sender and receiver.
6. **Usage**: Commonly used in WANs and older systems due to its reliability.

Frame Relay:

1. **Protocol Type**: Frame Relay is a packet-switched protocol also operating at Layer 2 of the OSI model.
2. **Connection**: Designed for high-speed networks and supports both Permanent Virtual Circuits (PVCs) and Switched Virtual Circuits (SVCs).
3. **Error Handling**: Provides error detection but relies on upper-layer protocols for error correction.
4. **Efficiency**: Optimized for high-speed data transmission with minimal overhead.
5. **Flow Control**: Assumes a reliable underlying network and does not include flow control mechanisms.
6. **Usage**: Popular for connecting geographically distant LANs and supporting modern WAN implementations.

Q2: What is PPP? Discuss its authentication and security mechanisms.

Point-to-Point Protocol (PPP): PPP is a versatile protocol used for establishing direct communication between two nodes. It operates at the data link layer and supports multiple network-layer protocols such as IPv4, IPv6, and IPX.

Features:

1. **Multiprotocol Support**: Handles diverse network protocols.
2. **Error Detection**: Uses Cyclic Redundancy Check (CRC) to identify transmission errors.
3. **Authentication**: Offers mechanisms for validating users.
4. **Compression**: Reduces data size for faster transmission.

5. **Link Management**: Establishes, configures, and terminates connections using the Link Control Protocol (LCP).

Authentication Mechanisms:

1. **Password Authentication Protocol (PAP):**
    - Simple two-way handshake method.
    - Transmits credentials in plaintext, making it vulnerable to interception.
2. **Challenge Handshake Authentication Protocol (CHAP):**
    - Secure three-way handshake.
    - Encrypts credentials using a hashed value, enhancing security against eavesdropping and replay attacks.

Security Mechanisms:

1. **Encryption**: Supports encryption protocols like ECP for securing data.
2. **Error Handling**: Ensures reliable communication by detecting and managing transmission errors.
3. **IPSec Integration**: Provides additional encryption for secure communication when used with protocols like IP.

Q3: Explain various controlled access methods in MAC.

Controlled Access Methods:

1. **Polling:**
    - A central controller (primary device) queries devices (secondary devices) sequentially to determine if they need to transmit data.
    - **Advantages**:
        - Collision-free as only one device transmits at a time.
        - Fair allocation of bandwidth.
    - **Disadvantages**:
        - High overhead and delays due to sequential polling.
        - Single point of failure if the primary device malfunctions.
2. **Token Passing:**
    - A special frame, called a token, is passed between devices. A device must possess the token to transmit data.
    - **Advantages**:
        - Completely eliminates collisions.

        - Guarantees transmission opportunity for all devices.
    - **Disadvantages**:
        - Complex implementation and token management.
        - Network can become idle if no device has data to transmit.

3. **Reservation:**
    - Devices reserve the medium for transmission during a control phase.
    - **Advantages**:
        - Efficient for scheduled and time-sensitive transmissions.
        - Prevents collisions during the data phase.
    - **Disadvantages**:
        - Reservation phase consumes bandwidth.
        - Inefficient if few devices have data to send.

Q4: Procedure for Calculating the Checksum of a Message.

Steps:

1. **Divide the Message**: Split the message into fixed-size blocks (e.g., 16 bits).
2. **Add the Blocks**: Perform binary addition on all blocks. If there's an overflow, add the carry back to the sum.
3. **Compute the Complement**: Take the one's complement of the final sum to generate the checksum.
4. **Verify**: Add the checksum to the original data. The result should be all 1s if the checksum is correct.

Example (M(X) = [7, 11, 12, 0, 6]):

1. Binary Representation: Convert values (7 = 0111, 11 = 1011, etc.).
2. Addition: Add blocks with binary arithmetic and handle overflow.
    - 0111 + 1011 = 10010 (carry: 1, result: 0010).
    - 0010 + 1100 = 1110.
    - 1110 + 0000 = 1110.
    - 1110 + 0110 = 10100 (carry: 1, result: 0100).
3. Complement: Take one's complement (0100 → 1011).
4. Verification: Add checksum (1011) to sum (0100): 0100 + 1011 = 1111 (all 1s). **Checksum**: 1011 (binary) or 11 (decimal).

Q5: Bluetooth Technology and Its Advantages in Healthcare.

Working Principle:

1. Operates in the unlicensed 2.4 GHz ISM band.
2. Employs Frequency Hopping Spread Spectrum (FHSS) to minimize interference.
3. Devices undergo a pairing process using protocols like Secure Simple Pairing (SSP).
4. Supports a master-slave architecture with piconets, allowing up to 8 devices to communicate.
5. Low Energy (BLE) mode optimizes power usage for battery-operated devices.

Advantages in Healthcare:

1. **Wireless Connectivity**: Eliminates the need for physical cables, enhancing mobility and comfort for patients.
2. **Energy Efficiency**: BLE allows long battery life, crucial for continuous monitoring devices.
3. **Interoperability**: Ensures compatibility with various devices like smartphones, tablets, and health monitors.
4. **Cost-Effectiveness**: Affordable modules reduce costs in healthcare applications.
5. **Real-Time Monitoring**: Enables immediate data transfer for critical patient monitoring systems.
6. **Data Security**: Includes encryption protocols like AES-128 to protect sensitive medical data.

Q6: Categorize Ethernet 802.3 Frame Formats.

Frame Types:

1. **Ethernet II (DIX)**: Commonly used in modern networks. Utilizes the Type field to identify higher-layer protocols.
2. **IEEE 802.3**: Older standard that uses the Length field to indicate data payload size.
3. **SNAP**: Extends the 802.3 frame with a Subnetwork Access Protocol (SNAP) header for additional protocol support.
4. **Novell Raw**: Proprietary frame type used in legacy Novell networks.

Fields in Ethernet Frame:

1. **Preamble**: 7 bytes for synchronization.
2. **Start Frame Delimiter (SFD)**: 1 byte marking frame start.
3. **Destination Address**: 6-byte MAC address of the recipient.
4. **Source Address**: 6-byte MAC address of the sender.

5. **Type/Length**: Indicates payload type or size.
6. **Data and Pad**: Contains payload (up to 1500 bytes).
7. **Frame Check Sequence (FCS)**: 4-byte CRC for error detection.

Q7: Architecture of 802.11 Wireless LAN.

Components:

1. **Basic Service Set (BSS):** A single access point (AP) and its associated stations (devices).
2. **Extended Service Set (ESS):** Two or more BSSs interconnected via a distribution system (DS), often a wired backbone.

Physical Layer Technologies:

1. **FHSS (Frequency Hopping Spread Spectrum):** Splits the 2.4 GHz band into sub-channels and hops frequencies to avoid interference.
2. **DSSS (Direct Sequence Spread Spectrum):** Spreads data over a wide frequency band using a unique code.
3. **OFDM (Orthogonal Frequency Division Multiplexing):** Utilizes multiple subcarriers for high-speed data transmission in the 5 GHz band.

Management Frames: Used for device association, authentication, and synchronization within the WLAN.

Q8: Differences Between IEEE 802.3 (Wired) and IEEE 802.11 (Wireless):

1. **Transmission Medium**: IEEE 802.3 uses physical cables like Ethernet; IEEE 802.11 employs wireless signals such as radio waves.
2. **Mobility**: Wired LANs limit mobility due to physical connections; wireless LANs offer mobility within the AP's range.
3. **Installation**: Wired networks require extensive cabling; wireless networks are simpler and cost-effective to deploy.
4. **Interference**: Wired LANs are immune to electromagnetic interference; wireless LANs are prone to interference from other devices.

Q9: CSMA/CD Protocol and Efficiency.

Working:

1. **Carrier Sensing**: A device checks if the channel is idle before transmitting.
2. **Collision Detection**: If a collision occurs, devices stop transmitting and send a jam signal to notify others.

3. **Backoff Mechanism**: Devices wait a random amount of time before retransmitting, reducing chances of repeated collisions.

Efficiency:

1. Performs well in low-traffic networks with minimal collisions.
2. Efficiency decreases with high traffic due to increased collisions and retransmissions.
3. Modern networks use switches to segment collision domains and improve performance.

Q10: ALOHA and CSMA/CA.

ALOHA:

1. **Pure ALOHA**:
   - Devices transmit data anytime without sensing the channel.
   - Collisions are detected, and data is retransmitted after a random delay.
2. **Slotted ALOHA**:
   - Divides time into slots; devices can transmit only at the beginning of a slot, reducing collisions.

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance):

1. Devices sense the channel before transmitting.
2. If the channel is busy, devices wait for a random backoff time.
3. Once the channel is idle, the device transmits data and waits for an acknowledgment.
4. Used in wireless networks like IEEE 802.11 to prevent collisions.