Okay, here are the exam summary notes for Chapter 8: The Data Link Layer.

# The Data Link Layer (Layer 2) Introduction

- **Function**: To facilitate data communication between two nodes that are directly connected. This connection can be via shared copper cable, radio signals, or any other medium that allows direct communication without routing through intermediate nodes.
- **Core Responsibilities**:
    1. **Media Access Control (MAC)**, also known as contention control.
    2. **Data delineation** (framing).
    3. **(Transmission) error control**.

---

# Media Access Control (MAC)

MAC addresses the question of which node is allowed to transmit on the shared medium.

## Basic MAC Approaches:

1. **Master/Slave Protocols**:
    - A controlling node (master) manages access for slave nodes. The master polls slaves to see if they have data or selects a slave to send data to.
    - Can be point-to-point (one master, one slave) or multipoint (one master, multiple slaves).
    - **Pros**: Simple to implement, especially with less intelligent slave devices.
    - **Cons**: Inefficient due to polling overhead even when slaves have no data, potential for latency as slaves must wait to be polled, and a single point of failure (the master).
    - **Example**: SDLC (Synchronous Data Link Control) can operate in this mode.
2. **Token Passing Protocols**:
    - A special frame (token) circulates among nodes. A node can only transmit if it possesses the token. After transmitting (or if it has no data), it passes the token to the next node.
    - Operates on a logical ring, which can be a physical ring or bus topology.
    - **Token Reservation**: Allows for priority by letting nodes reserve the token. The node with the highest priority reservation gets the token next.
    - **Challenges & Solutions**:
        - **Node Disappearance**: On physical rings, wiring hubs can bypass offline nodes.
        - **Lost Token**: An "active monitor" node detects a missing token and generates a new one.
        - **Active Monitor Failure**: If the active monitor fails, a new one is elected using an algorithm (e.g., the bully algorithm where the node with the

highest MAC address wins).

- **Slotted Ring**: On large rings, multiple "empty slot" tokens can circulate to improve efficiency.
- **Examples**: IEEE 802.5 (Token Ring), IEEE 802.4 (Token Bus), FDDI (Fibre Distributed Data Interface).

3. **Multiple Access (MA) Protocols**:
    - Allows any node to transmit data when it wants to.
    - **Collisions**: Occur if two or more nodes transmit simultaneously, corrupting data.
    - **Aloha Protocol**: A "pure" MA protocol where nodes transmit at will.
    - **CSMA (Carrier Sense Multiple Access)**: Nodes "sense" the medium; if busy, they defer transmission.
        - **Hidden Node Problem**: CSMA is not foolproof. If node A can't hear C, but both can reach B, A might transmit while C is transmitting to B, causing a collision at B.
    - **Slotted Aloha**: Divides time into slots; transmissions must fit within a slot, reducing collision probability.
    - **CSMA Variations**:
        - **Persistent CSMA**: If busy, waits until idle, then transmits. High collision risk if many are waiting.
        - **Non-persistent CSMA**: If busy, waits a random time, then senses again. Reduces collisions but can waste idle time.
        - **p-persistent CSMA**: If busy, waits until idle, then transmits with probability 'p'. Balances between persistent and non-persistent.
        - **CSMA/CD (Collision Detection)**: Nodes listen while transmitting. If a collision is detected, transmission is aborted, and a jamming signal is sent. Nodes then wait a random time before retrying (binary exponential backoff). **Example**: Ethernet (IEEE 802.3).
        - **CSMA/CA (Collision Avoidance)**: Used when CD is not feasible (e.g., wireless).
            - **MACA (Multiple Access with Collision Avoidance)**: Uses RTS (Request To Send) and CTS (Clear To Send) frames. Nodes hearing RTS or CTS defer transmission for the specified duration.
            - **MACAW (MACA for Wireless)**: Adds a DS (Data Sending) frame after CTS to confirm the exchange, improving efficiency if CTS is lost. **Example**: WiFi (IEEE 802.11).
    - **Exposed Node Problem**: Node C hears B transmitting to A and defers sending to D, even though C's transmission to D would not interfere with A.

---

# Data Delineation (Framing)

Methods to define the start and end of a frame:

1. **Mark Start and End**:

   - **Transparency Problem**: The chosen start/end markers must not appear naturally within the data, or a mechanism is needed to differentiate data markers from control markers.
   - **Using Special Characters (Byte Stuffing)**:
      - **Example**: Bisync (BSC) uses control characters like SOH (Start of Header), STX (Start of Text), ETX (End of Text).
      - To send control characters as data or handle problematic data bytes, DLE (Data Link Escape) is used. E.g., binary data framed by DLE-STX and DLE-ETX. A DLE character in the data is sent as DLE-DLE.
   - **Using Special Bit Patterns (Bit Stuffing)**:
      - **Example**: SDLC uses the flag 01111110 to mark start and end.
      - To prevent the flag appearing in data, the sender inserts a 0 bit after any five consecutive 1s in the data. The receiver removes this stuffed 0.
   - **Using Non-Bit Patterns (Code Violations)**:
      - Uses physical layer code violations (e.g., high-high or low-low voltage levels in Manchester coding, called J and K symbols) that cannot represent data bits. This inherently solves transparency.
      - **Example**: IEEE 802.5 Token Ring uses JK0JK000 as starting delimiter and JK1JK1xx as ending delimiter.

2. **Mark Start and Indicate Length / Fixed Length**:
   - The frame header contains a length field indicating the payload size, or the protocol uses fixed-length frames.
   - **Example: Ethernet (IEEE 802.3)**:
      - Preamble (7 octets: 1010...10) and Start of Frame Delimiter (1 octet: 10101011) mark the beginning.
      - Has fixed-position fields for addresses and a length field (or Ethertype).
      - The length field specifies data size (46-1500 octets). Transparency is not an issue.
      - **MTU (Maximum Transmission Unit)** is 1500 octets for standard Ethernet; "jumbo frames" can be larger (e.g., 9000 octets).
   - **Example: ATM (Asynchronous Transfer Mode)**:
      - Uses fixed-size 53-octet cells (5-octet header, 48-octet payload).
      - Delineation can be achieved by synchronizing on the HEC (Header Error Control – an 8-bit CRC for the header).

---

# Error Control

Mechanisms to detect and possibly correct errors in transmitted data.

## Error Detection:

- **Parity Check**:

    - An extra bit is added to a block of data (e.g., an octet) to make the total number of 1s either even (even parity) or odd (odd parity).
    - **Weakness**: Detects only an odd number of bit errors within the block. Fails if an even number of bits flip.
    - **Longitudinal Parity**: An extra octet (parity octet) is calculated, where each bit of the parity octet provides parity for the corresponding bit position across all data octets.
- **Checksums**:
    - Typically a sum of the data values (e.g., octets), calculated modulo some number (e.g., sum modulo 256 for 8-bit checksums).
    - **Weakness**: Relatively weak; can miss certain error patterns (e.g., if all data bits become zero).
- **Cyclic Redundancy Codes (CRCs)**:
    - Widely used and effective. Based on polynomial division in binary.
    - **Process**:
        1. A generator polynomial (e.g., x4+x+1→10011) is chosen.
        2. The data to be sent is padded with 'n' zeros at the end, where 'n' is the degree of the generator polynomial.
        3. This padded data is divided by the generator polynomial using binary polynomial arithmetic.
        4. The remainder of this division is the CRC.
        5. The CRC replaces the 'n' padded zeros and is transmitted with the data.
        6. The receiver divides the received data (including CRC) by the same generator polynomial. If the remainder is zero, no error is detected.

## Error Correction:

- **n-Modular Redundancy**:
    - The data is transmitted 'n' times. The receiver takes the majority vote as the correct data.
    - Example: Triple Modular Redundancy (TMR) sends data 3 times.
    - **Overhead**: High, (n−1)×message size.
- **Hamming Code**:
    - Can correct single-bit errors (the version discussed).
    - Parity bits are calculated for overlapping sets of data bits.
    - Parity bits are placed at positions that are powers of 2 (1, 2, 4, 8, ...). Data bits fill the remaining positions.
    - At the receiver, parity checks are recomputed. The pattern of incorrect parity bits (called the syndrome) directly indicates the position of the erroneous bit, which can then be flipped for correction.
- **Reed-Solomon Codes**: Mentioned as to be described later.

*(Error control examples for Bisync, SDLC, Ethernet, IEEE 802.5 are noted as incomplete in the text)*.

# Other Layer 2 Functions

## Connection-Oriented Services:

Some Layer 2 protocols can establish, manage, and terminate connections.

- **SDLC/HDLC**:
  - Bit-oriented, uses flags (01111110) for framing.
  - **I-frames (Information frames)**: Carry data. Use sequence numbers N(S) (sent) and N(R) (next expected/acknowledging). Uses Go-Back-N ARQ. Max 7 unacknowledged frames with 3-bit sequence numbers.
  - **S-frames (Supervisory frames)**: For control, no data. Include N(R). Types:
    - **RR (Receiver Ready)**: Acknowledges frames up to N(R)-1, ready for N(R).
    - **RNR (Receiver Not Ready)**: Acknowledges, but tells sender to pause.
    - **REJ (Reject)**: Rejects frame N(R) and all subsequent frames (Go-Back-N).
    - HDLC adds **SREJ (Selective Reject)** for only N(R) (Selective Repeat ARQ).
  - **U-frames (Unnumbered frames)**: For commands like setting mode (e.g., SNRME to switch to extended 16-bit control fields for 7-bit N(S)/N(R)), RSET (reset connection), DISC (disconnect).
  - **P/F (Poll/Final) bit**: In master/slave, master sets P bit to poll. Slave sets F bit in final response. In peer-to-peer, marks the final frame in a sequence.
- **Bisync**:
  - Historical. Connection initiated with SYN SYN ENQ. Uses stop-and-wait flow control with alternating acknowledgements (ACK0, ACK1).
- **Token Ring (IEEE 802.5)**:
  - Connectionless, but header includes "Address Recognised" and "Frame Copied" bits for rudimentary acknowledgement.

## Flow Control:

- **SDLC/HDLC**: Uses RNR S-frame.
- **Bisync**: Uses WACK (Wait-before-transmit Acknowledgment).
- Many current Layer 2 protocols rely on Layer 4 (e.g., TCP) for robust flow control.

# The MAC and LLC Sublayers

Layer 2 is sometimes divided into two sublayers:

- **LLC (Logical Link Control) Sublayer**:
  - Upper sublayer, responsible for medium-independent aspects. Standardized by IEEE 802.2.
  - **LLC PDU Format**: DSAP (Destination Service Access Point), SSAP (Source Service

    Access Point), Control, and Information fields.
    - DSAP and SSAP identify the Layer 3 protocol being used.
    - Control field supports connection-oriented, connectionless, or acknowledged connectionless services.
- **MAC (Media Access Control) Sublayer**:
    - Lower sublayer, handles medium-dependent aspects.
    - Includes the specific MAC mechanism (e.g., CSMA/CD, token passing) and data delineation from the physical medium.

---

# Examples of Layer 2 Protocols

*(This section is a stub in the provided text, offering brief descriptions)*

- **Ethernet (IEEE 802.3)**:
    - CSMA/CD protocol.
    - **Ethernet II (DIX)** frames use an "Ethertype" field to identify the Layer 3 protocol.
    - **IEEE 802.3** frames use a "Length" field and typically carry an IEEE 802.2 LLC PDU as payload to identify Layer 3 protocol.
    - **Harmonization**: If the Ethertype/Length field value is ≤1500, it's a length (IEEE 802.3). If ≥1536, it's an Ethertype (Ethernet II). Ethernet II frames are most common.
    - Can include IEEE 802.1Q field for VLAN tagging.
- **IEEE 802.4 (Token Bus)**: Byte-oriented token passing on a bus topology.
- **IEEE 802.5 (IBM Token Ring)**: Byte-oriented token passing on a ring topology.
- **IEEE 802.11 (WiFi)**: Series of standards for wireless LANs (WLANs), based on IEEE 802.3 principles but adapted for wireless (e.g., uses CSMA/CA). Includes 802.11a, b, g, n, ac (WiFi 5), ax (WiFi 6), be (WiFi 7).
- **SDLC/HDLC**: Bit-oriented, for point-to-point or multipoint links. Often used in WANs.
- **Bisync**: Older, character-oriented protocol from IBM.