UNIT II PHYSICAL AND DATA LINK LAYERS 9

Wired and wireless media – Functions of physical layer – Modems – Transmission errors – Error detection and correction – Framing - Flow control – Sublayers of DLL – Broadcast networks – Collision Domain - Ethernet – CSMA/CD – Token Ring – VLAN – LAN Analyzer – IEEE 802.11 - WLAN – CSMA/CA – Bluetooth – Ad hoc networks.

**Unit II: Physical and Data Link Layers** with a focus on **Wired and Wireless Media**, **Physical Layer**, and **Data Link Layer (DLL)**:

## Wired and Wireless Media:

- **Wired Media**:
  - Physical cables (e.g., **twisted pair**, **coaxial cable**, **fiber optics**) used for data transmission.
  - **Advantages**: Higher speed, lower interference.
  - **Disadvantages**: Limited mobility, installation cost.
- **Wireless Media**:
  - Uses electromagnetic waves (e.g., **radio waves**, **microwaves**) for communication.
  - **Advantages**: Mobility, easy to install.
  - **Disadvantages**: More prone to interference and security issues, lower bandwidth.

## Functions of the Physical Layer:

- Responsible for the **transmission of raw bits** over a communication medium.
- Converts digital data into signals (electrical, optical, or radio) for transmission.
- Ensures that signals are correctly encoded, modulated, and transmitted.
- Handles hardware elements like cables, connectors, and signal synchronization.

## Modems:

- **Modulator-Demodulator**: Converts **digital data** from a computer into **analog signals** for transmission over analog communication lines (like phone lines) and vice versa.

- **Role**: Enables computers to communicate over long distances using telephone infrastructure.

## Transmission Errors:

- **Transmission errors** occur when data is corrupted during transmission due to factors like noise, attenuation, or interference.
- **Bit errors** may occur when a ‘1’ is mistaken for a ‘0’ or vice versa.

## Error Detection and Correction:

- **Error Detection**: Methods to detect errors in transmitted data, ensuring data integrity.
  - Techniques: **Parity Check**, **Checksum**, **Cyclic Redundancy Check (CRC)**.
- **Error Correction**: Methods to not only detect but also correct errors in transmission.
  - Techniques: **Hamming Code**, **Reed-Solomon Codes**.

## Framing (Data Link Layer):

- **Framing** refers to dividing the stream of bits into smaller, manageable units called **frames**.
- Allows for synchronization between sender and receiver, and error detection can be applied on individual frames.

## Flow Control:

- Mechanism to ensure that a sender doesn’t overwhelm a receiver by sending data too fast.
  - Examples: **Stop-and-Wait Protocol**, **Sliding Window Protocol**.

## Sublayers of Data Link Layer (DLL):

1. **Logical Link Control (LLC)**: Provides error checking, flow control, and manages data exchange between devices.
2. **Media Access Control (MAC)**: Controls how devices on a network gain access to the medium and permission to transmit data. It uses physical addressing (MAC addresses).

## Broadcast Networks:

- Networks where data sent by one device can be received by all other devices in the network (e.g., Ethernet LAN).
- Broadcast networks rely on protocols like CSMA/CD to manage multiple devices transmitting on the same network medium.

## Collision Domain:

- A network segment where **data packets can collide** when multiple devices transmit simultaneously.
- **Hubs** increase the size of a collision domain, while **switches** segment it, reducing collisions and improving efficiency.

## Ethernet:

- A widely used **wired LAN technology** that uses twisted pair cables or fiber optics.
- Operates primarily at the data link layer and the physical layer.

## CSMA/CD (Carrier Sense Multiple Access with Collision Detection):

- A protocol used in Ethernet networks to manage access to the shared medium.
- **CSMA**: Devices sense the carrier (the medium) to see if it's free before transmitting.
- **CD**: If two devices transmit simultaneously and a collision occurs, they stop, wait a random amount of time, and retransmit.

## Ethernet and Related Concepts:

- **Ethernet**: A widely used wired LAN technology based on the CSMA/CD protocol.
- **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)**: A protocol for managing data collisions in wired networks. Devices listen to the network before transmitting and detect collisions to retransmit the data.
- **Token Ring**: A LAN protocol where a token circulates in the network, and only the device holding the token can transmit data, preventing collisions.
- **VLAN (Virtual Local Area Network)**: Logical segmentation of a LAN into multiple, isolated broadcast domains, improving security and reducing broadcast traffic.
- **LAN Analyzer**: A tool used to monitor, analyze, and troubleshoot LAN traffic.

## Wireless Networking Concepts:

- **IEEE 802.11 WLAN**: The standard for wireless LANs, commonly known as Wi-Fi. It provides wireless connectivity between devices using access points.
- **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)**: A protocol for wireless networks where devices avoid collisions by waiting for a clear channel before transmitting.
- **Bluetooth**: A short-range wireless technology used for connecting devices like phones, laptops, and peripherals.
- **Ad Hoc Networks**: Decentralized wireless networks where devices communicate directly without relying on a fixed infrastructure (e.g., Wi-Fi Direct, Bluetooth).

**************************************Wired Media

Wired media refers to physical cables that transmit data using electrical or optical signals. They are typically used for local area networks (LANs), data centers, and various telecommunications applications.

### *Types of Wired Media:*

1. **Twisted Pair Cable**:
    a. **Description**: Consists of pairs of insulated copper wires twisted together to reduce electromagnetic interference.
    b. **Categories**:
        i. **Cat 5e**: Supports speeds up to 1 Gbps for short distances.
        ii. **Cat 6/6a**: Supports speeds up to 10 Gbps for distances up to 55 meters (Cat 6) and up to 100 meters (Cat 6a).
    c. **Applications**: Commonly used in Ethernet networks.
2. **Coaxial Cable**:
    a. **Description**: Composed of a central conductor, insulating layer, metallic shield, and outer cover.
    b. **Bandwidth**: Higher bandwidth capacity than twisted pair cables.
    c. **Applications**: Used in cable television, internet connections, and some LANs.
3. **Fiber Optic Cable**:
    a. **Description**: Composed of thin strands of glass or plastic (optical fibers) that transmit data as light signals.
    b. **Types**:

        i. **Single-mode Fiber**: Suitable for long-distance communication (up to 40 km or more) with higher bandwidth.
        ii. **Multi-mode Fiber**: Suitable for shorter distances (up to 2 km) and lower bandwidth applications.
    c. **Applications**: High-speed internet connections, data centers, backbone networks.

### *Advantages of Wired Media:*

- **Higher Speeds**: Generally provide faster data transfer rates compared to wireless media.
- **Lower Latency**: Less prone to delays in transmission.
- **Security**: More secure than wireless as physical access to cables is required to intercept data.
- **Reliability**: Less susceptible to interference from external factors like electromagnetic interference (EMI).

### *Disadvantages of Wired Media:*

- **Mobility**: Limited mobility; devices must be physically connected to the network.
- **Installation Costs**: Can be more expensive to install due to the need for cabling and infrastructure.
- **Physical Limitations**: Limited by distance; signal quality can degrade over long distances.

## Wireless Media

Wireless media refers to data transmission methods that use electromagnetic waves to transmit data without physical cables. Wireless networks are widely used for mobile communication, internet access, and local networking.

### *Types of Wireless Media:*

1. **Radio Waves**:
    a. **Description**: Use radio frequency (RF) signals to transmit data over the air.
    b. **Applications**: Wi-Fi networks, Bluetooth devices, and cellular networks.
2. **Microwaves**:

    a. **Description**: Higher frequency than radio waves; used for point-to-point communication.
    b. **Applications**: Satellite communications, microwave relay links.
3. **Infrared**:
    a. **Description**: Uses infrared light for short-range communication.
    b. **Applications**: Remote controls, some wireless peripherals (e.g., wireless mice).
4. **Li-Fi**:
    a. **Description**: Uses visible light for data transmission.
    b. **Applications**: Emerging technology for high-speed wireless communication in environments where RF communication is not feasible.

### *Advantages of Wireless Media:*

- **Mobility**: Allows devices to connect to the network without being physically tethered.
- **Easy Installation**: Generally easier and quicker to deploy since no cabling is required.
- **Flexibility**: Supports a range of devices, including mobile phones, tablets, and laptops.

### *Disadvantages of Wireless Media:*

- **Speed Limitations**: Generally slower than wired media due to factors like signal degradation and interference.
- **Interference**: Susceptible to interference from other devices, obstacles, and environmental factors.
- **Security Risks**: More vulnerable to eavesdropping and unauthorized access if not properly secured.

## Summary

| Feature | Wired Media | Wireless Media |
|---|---|---|
| **Types** | Twisted pair, coaxial, fiber optic | Radio waves, microwaves, infrared, Li-Fi |
| **Speed** | Generally higher speeds | Generally lower speeds |
| **Latency** | Lower latency | Higher latency |

| | | |
|---|---|---|
| **Mobility** | Limited mobility | High mobility |
| **Installation** | More complex, higher cost | Easier, lower cost |
| **Reliability** | More reliable, less interference | Less reliable, more prone to interference |
| **Security** | More secure | More vulnerable to security threats |

Both wired and wireless media play crucial roles in modern networking. The choice between them depends on specific use cases, performance requirements, and environmental considerations.

*********************************************************************8

## Transmission Errors in Data Communication

Transmission errors occur when data is corrupted during the transmission process from a sender to a receiver. These errors can result from various factors, including:

- **Noise**: Interference from electrical devices, environmental conditions, or physical obstructions.
- **Signal Degradation**: Loss of signal strength over long distances, especially in wired communications.
- **Interference**: External electromagnetic interference from other devices or networks.
- **Packet Loss**: Loss of data packets due to network congestion or faulty hardware.

To ensure the integrity of transmitted data, error detection and correction mechanisms are employed.

## Error Detection

### *1. Parity Check*

- **Example**:
  - Let's say we have a 4-bit data sequence: `1011`.
  - **Even Parity**: The number of 1's in `1011` is 3 (odd). To make it even, we add a parity bit of `1`. The transmitted data becomes `10111`.

- **Receiver's Check**: The receiver gets `10111`, counts the number of 1's (which is now 4), and determines that the parity is even, so it assumes there is no error.
- If the received sequence is `10011` (where one bit has changed), the number of 1's is 3 (odd). The receiver detects a discrepancy in parity, indicating an error.

### *2. Checksum*

- **Example**:
  - Consider a data packet consisting of two 8-bit bytes: `11010101` (213 in decimal) and `01100010` (98 in decimal).
  - **Checksum Calculation**:
    - Add the two bytes:

`11010101`

- 01100010

1 00110111 (Carry bit is ignored, resulting in 01101111)

```
markdown
Copy code
- The checksum is the one's complement of the sum:
- One’s complement of `01101111` is `10010000` (144 in decimal).
```

- **Transmitted Data**: The packet sent would be `11010101`, `01100010`, and `10010000`.
- **Receiver's Check**:
  - The receiver adds the two data bytes and the received checksum:

`11010101`

- 01100010
- 10010000

1 00110111 (Again, ignoring the carry bit)

```
- If the result is `11111111` (all bits 1), the data is considered valid. If it’s anything else, an error is detected.
```

### *3. Cyclic Redundancy Check (CRC)*

- **Example**:
  - Suppose we want to send the data `1101` using a divisor polynomial `1011`.
  - **Data**: `1101`
  - **Append Zeros**: Append `n-1` zeros (where n is the degree of the divisor) to the data. Thus, `1101000`.
  - **Division**:
    - Perform binary division of `1101000` by `1011`.
    - The remainder is calculated as `0010`.
  - **Transmitted Data**: The transmitted message is `11010010` (original data + CRC).
  - **Receiver's Check**:
    - The receiver performs the same division with the received data. If the remainder is `0`, the data is assumed to be correct; if not, an error is detected.

## Error Correction

### *1. Hamming Code*

- **Example**:
  - Consider a 4-bit data sequence: `1011`.
  - **Step 1**: Determine the number of redundant bits. For 4 data bits, you need 3 redundant bits (`r` bits satisfy *2r≥m+r+12^r \geq m + r + 1*2r≥m+r+1 where `m` is data bits).
  - **Step 2**: Place redundant bits at positions 1, 2, and 4 (1-indexed):

```
Position:   1  2  3  4  5  6  7
Bits:       r1 r2 1 r3  0  1 1
```

  - **Step 3**: Calculate redundant bits:
    - **r1** covers positions 1, 3, 5, 7: `r1 ⊕ 1 ⊕ 0 ⊕ 1 = 0` (thus, r1 = 0).
    - **r2** covers positions 2, 3, 6, 7: `r2 ⊕ 1 ⊕ 1 ⊕ 1 = 0` (thus, r2 = 1).
    - **r3** covers positions 4, 5, 6, 7: `r3 ⊕ 0 ⊕ 1 ⊕ 1 = 0` (thus, r3 = 0).
  - **Final Code**: The transmitted code is `0111011`.
- **Step 4**: Suppose the receiver receives `0111001` (the last bit is erroneous).
  - Calculate parity:

- For r1: `0 ⊕ 1 ⊕ 0 ⊕ 1 = 0` (ok).
- For r2: `1 ⊕ 1 ⊕ 0 ⊕ 1 = 1` (error detected).
- For r3: `0 ⊕ 0 ⊕ 1 ⊕ 1 = 0` (ok).

  - The error is in position 3 (binary 011 indicates bit 3 is incorrect), so flip the bit to correct it: `0111011`.

### *2. Reed-Solomon Code*

- **Example**:
  - Suppose we have a message block of 7 bytes: `ABCDEFG`.
  - **Encoding**:
    - The original message is encoded by adding redundant bytes to allow correction. Let's say 3 redundant bytes are added, resulting in a total of 10 bytes (7 data + 3 redundant).
  - **Transmission**: The encoded message `ABCDEFGXXX` is sent.
  - **Error Occurrence**: Due to noise, the received message might be `ABZDEFGXXX` (the third byte has been corrupted).
  - **Correction**: The receiver uses the redundant bytes to analyze and determine the nature of the error. If the error is within the correctable limits, the receiver can reconstruct the original data as `ABCDEFG`.

## Summary

- **Error Detection** techniques like parity checks, checksums, and CRC help identify if data has been corrupted during transmission.
- **Error Correction** techniques such as Hamming codes and Reed-Solomon codes allow for identifying and correcting errors without needing retransmission.

*******************************************************************************88

Sublayers of Data Link Layer (DLL):

***ChatGPT said:***

ChatGPT

The Data Link Layer (DLL) is the second layer of the OSI model and plays a critical role in facilitating communication between devices on a local area network (LAN) or within a wide area network (WAN). The DLL is divided into two sublayers, each serving distinct functions:

## 1. Logical Link Control (LLC) Sublayer

### *Functions:*

- **Framing**: The LLC sublayer is responsible for defining frame boundaries and managing frame synchronization. It encapsulates network layer packets into frames.
- **Flow Control**: LLC provides mechanisms to control the rate of data transmission between sender and receiver, ensuring that a fast sender does not overwhelm a slow receiver.
- **Error Detection and Handling**: It can provide basic error detection capabilities by checking frame integrity through methods such as checksums or CRC.
- **Multiplexing**: LLC allows multiple network layer protocols (e.g., IP, IPX) to coexist over the same physical medium by using service access points (SAPs) to distinguish between different protocols.

### *Example:*

- In Ethernet networks, the LLC sublayer handles the communication between the network layer (Layer 3) and the MAC (Media Access Control) sublayer by adding headers and trailers to the data received from the network layer.

## 2. Media Access Control (MAC) Sublayer

### *Functions:*

- **Access Control**: The MAC sublayer is responsible for controlling how devices on a shared medium access the network. It determines when a device can transmit data and manages potential collisions.
- **Framing**: Similar to the LLC, the MAC sublayer also frames the data, but its focus is more on the format and addressing of the data for transmission.
- **Addressing**: The MAC sublayer adds hardware addresses (MAC addresses) to frames, allowing devices to identify each other on the local network.
- **Error Detection**: It can also incorporate error detection mechanisms, such as CRC, to ensure the integrity of the frames transmitted over the medium.

***Example:***

- In Ethernet networks, the MAC sublayer determines how frames are sent over the network using the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol. It also adds source and destination MAC addresses to the Ethernet frames.

## Summary of Data Link Layer Sublayers

| Sublayer | Functions | Responsibilities |
|---|---|---|
| **LLC** | - Framing<br>- Flow Control<br>- Error Detection<br>- Multiplexing | Manages communication between the network layer and the MAC sublayer, ensuring proper data encapsulation and control mechanisms. |
| **MAC** | - Access Control<br>- Framing<br>- Addressing<br>- Error Detection | Controls how devices access the physical medium, formats frames for transmission, and adds addressing information. |

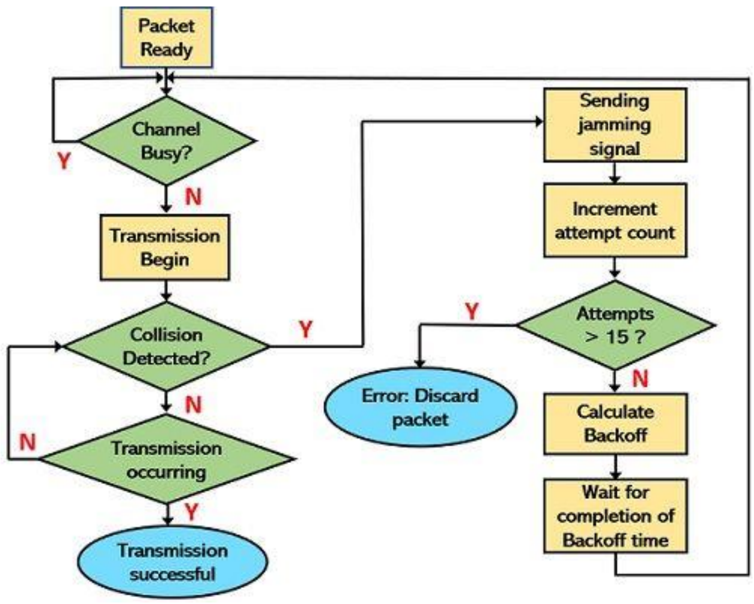
The separation of the Data Link Layer into these two sublayers allows for a more modular approach to network communication, providing flexibility and efficiency in managing data transmission and access control on local networks.

*****************************************************************************8

## CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

**CSMA/CD** is a network protocol used in Ethernet networks to manage how devices share a communication medium. It is designed to reduce the chances of collisions when multiple devices attempt to send data over the same medium. Here's an overview of how CSMA/CD works, its functioning, advantages, and disadvantages.

## How CSMA/CD Works




1. **Carrier Sense**:
   a. Before a device sends data, it listens to the network (the communication medium) to check if another device is currently transmitting. This is known as "carrier sensing."
   b. If the channel is clear (no other transmissions detected), the device can proceed to transmit its data.
2. **Data Transmission**:
   a. Once the medium is clear, the device begins to transmit its data.
3. **Collision Detection**:
   a. While transmitting, the device continues to monitor the network for any collisions. A collision occurs when two devices transmit data simultaneously.
   b. If the device detects that the signals are garbled (due to a collision), it stops transmitting immediately.
4. **Jamming Signal**:
   a. Upon detecting a collision, the device sends a jamming signal to inform all other devices on the network that a collision has occurred. This helps ensure that all devices are aware of the collision and can stop their transmissions.
5. **Backoff Algorithm**:
   a. After the collision is detected and the jamming signal is sent, each device involved in the collision waits for a random amount of time before attempting

to retransmit. This waiting period is calculated using the exponential backoff algorithm, which increases the wait time after each subsequent collision.

b. Once the backoff period has elapsed, the device returns to the carrier sense phase and checks the medium again before retransmitting.

## Advantages of CSMA/CD

1. **Efficient Use of Bandwidth**:
    a. CSMA/CD helps optimize bandwidth usage by allowing multiple devices to share the medium without requiring a fixed time slot for each device.
2. **Simplicity**:
    a. The protocol is relatively simple to implement, making it suitable for basic Ethernet networks.
3. **Cost-Effective**:
    a. CSMA/CD can reduce the costs associated with more complex network access methods that require dedicated controllers or time-slotting mechanisms.

## Disadvantages of CSMA/CD

1. **Collision Inefficiency**:
    a. As the number of devices on the network increases, the likelihood of collisions also increases, which can lead to network inefficiency and delays in data transmission.
2. **Performance Degradation**:
    a. In high-traffic networks, the performance can degrade significantly due to increased collisions and retransmissions, leading to a bottleneck effect.
3. **Limited Scalability**:
    a. CSMA/CD is not well-suited for large networks or networks with high data traffic, making it less effective as network demands grow.

## Applications of CSMA/CD

CSMA/CD is primarily used in wired Ethernet networks (IEEE 802.3). While it was widely employed in traditional bus and shared media Ethernet configurations, its use has diminished with the advent of switched Ethernet networks, which have largely eliminated collisions by providing dedicated bandwidth to each device.

## Summary

CSMA/CD is a protocol designed to manage how multiple devices share a communication medium by listening for traffic before transmitting and detecting collisions during transmission. While it offers several advantages in terms of efficiency and simplicity, it is limited in scalability and performance in high-traffic situations. The evolution of network technologies, particularly the shift to full-duplex communication and switched networks, has led to a decline in the use of CSMA/CD in modern networking.