Unit-05

The Link Layer and LAN

5.1. Introduction to the Link Layer

The **Link Layer** is the second layer in the OSI (Open Systems Interconnection) model and plays a critical role in the transmission of data across physical network links. It is responsible for the communication between adjacent network nodes, ensuring that data frames are properly formatted, transmitted, and received over the physical medium.

5.1.1 The Services Provided by the Link Layer

The Link Layer provides several essential services that enable reliable data transmission between directly connected devices:

1. **Framing**:
   - The Link Layer encapsulates the network layer's datagrams (packets) into frames for transmission. This involves adding a header and sometimes a trailer to the data to create a frame, which is the basic unit of communication at this layer.
2. **Error Detection and Correction**:
   - The Link Layer includes mechanisms to detect and sometimes correct errors that may occur during the transmission of frames. Techniques like checksums, CRC (Cyclic Redundancy Check), or parity bits are used to identify errors.
3. **Flow Control**:
   - The Link Layer manages the pace at which data is sent to ensure that the sender does not overwhelm the receiver. This is particularly important when there is a significant difference in processing speeds or buffer sizes between the sender and receiver.
4. **Medium Access Control (MAC)**:
   - The Link Layer controls access to the physical transmission medium, especially in shared networks like Ethernet or Wi-Fi. The MAC sublayer ensures that devices on the same network do not interfere with each other's transmissions, using protocols like CSMA/CD (Carrier Sense Multiple Access with Collision Detection) or CSMA/CA (Collision Avoidance).
5. **Addressing**:
   - The Link Layer uses physical (MAC) addresses to identify devices on the same network. These unique addresses are used to deliver frames to the correct recipient on a local network.

6. **Reliable Delivery (optional)**:
    - In some networks, the Link Layer provides reliable delivery by ensuring that frames are acknowledged and retransmitted if necessary. However, this service is not always provided, as reliability can also be handled by higher layers like the Transport Layer.

5.2. Error-Detection and -Correction Techniques

Error-Detection and Correction Techniques are essential in ensuring data integrity during transmission across a network. These techniques help identify and correct errors that may occur due to noise, interference, or other issues during data transfer. Here are the main techniques used at the data Link Layer:

5.2.1 Parity checks

1. Single-Bit Parity:

- Adds a single parity bit to a block of data to make the number of 1s either even (even parity) or odd (odd parity).
- **Example**: For even parity, if the data is `1010101`, the parity bit added would be `0` (making the total number of 1s even). If the data was `1010111`, the parity bit would be `1`.
- **Detection Capability**: Single-bit parity can detect single-bit errors but cannot correct them or detect errors involving an even number of bit flips.

2. Two-Dimensional Parity:

- Extends the single-bit parity check by organizing data into a grid and adding parity bits for each row and column.
- This allows for the detection and correction of single-bit errors and the detection (but not correction) of multiple-bit errors.

5.2.2 Check Sum Methods

Checksum Methods are error-detection techniques used to verify the integrity of data transmitted over a network or stored in memory. The checksum is a value calculated from the data, and it is transmitted along with the data. The receiver recalculates the checksum from the received data and compares it with the transmitted checksum. If the two checksums match, the data is considered intact; if not, an error is detected.

5.2.3 Cyclic Redundancy Check (CRC)

Cyclic Redundancy Check (CRC) is an error-detection technique used to detect changes to raw data in digital networks and storage devices. CRC is widely used because of its efficiency in detecting common errors caused by noise or other transmission issues.

5.3. Multiple Access Links and Protocols

Multiple access protocols are used to manage how data is shared over a common communication medium to avoid collisions and ensure efficient use of the channel.

5.3.1 Channel Partitioning Protocols

- These protocols divide the channel into separate parts, either by time, frequency, or code.
- Examples include Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA), and Code Division Multiple Access (CDMA).
- Each user gets a specific time slot, frequency band, or code to transmit, which reduces collisions.

5.3.2 Random Access Protocols

- In these protocols, users can transmit data whenever they have data to send, leading to possible collisions.
- When collisions occur, a mechanism is used to detect them and resolve the conflict.
- Examples include ALOHA, Slotted ALOHA, and Carrier Sense Multiple Access with Collision Detection (CSMA/CD), used in Ethernet.

5.3.3 Taking-Turns Protocols

- These protocols allow users to take turns accessing the channel.
- Common methods include polling (a central controller invites nodes to transmit) and token passing (a token is passed around the nodes, and only the holder of the token can transmit).
- This approach minimizes collisions and ensures fair access.

5.3.4 DOCSIS: The Link-Layer Protocol for Cable Internet Access

- DOCSIS (Data Over Cable Service Interface Specification) is a standard used for high-speed data transfer over cable TV systems.
- It defines the protocols for data exchange over cable networks, including both downstream and upstream data flows.
- DOCSIS uses a combination of channel partitioning and random access techniques to manage data transmissions between the cable modem and the cable modem termination system (CMTS).

5.4. Switched Local Area Networks

Switched LANs are networks that use switches to connect devices, allowing efficient and direct communication within a local network.

5.4.1 Link-Layer Addressing and ARP

- **Link-Layer Addressing**: Each device on a network has a unique MAC address, used to identify devices on the same local network.
- **Address Resolution Protocol (ARP)**: ARP is used to map IP addresses to MAC addresses within a local network. When a device wants to communicate with another device, it uses ARP to find the MAC address corresponding to the IP address.

5.4.2 Ethernet

- **Ethernet**: It is the most common technology for wired local area networks. Ethernet uses cables and switches to connect devices within a LAN, providing high-speed communication.
- **Frame Structure**: Ethernet frames include source and destination MAC addresses, type, data, and error-checking information (CRC).

5.4.3 Link-Layer Switches

- **Link-Layer Switches**: These switches operate at the data link layer (Layer 2) and use MAC addresses to forward data to the correct destination within a LAN.

- **Switch Functionality**: Switches learn the MAC addresses of devices connected to each port, allowing them to efficiently direct frames only to the intended recipient, reducing unnecessary traffic.

5.4.4 Virtual Local Area Networks (VLANs)

- **VLANs**: VLANs are used to segment a physical network into multiple logical networks. This helps organize devices into different groups, improving security and performance.
- **Functionality**: VLANs allow devices on separate VLANs to communicate as if they are on different physical networks, even if they share the same physical infrastructure. VLAN tagging is used to identify which VLAN a frame belongs to.

5.5. A Day in the Life of a Web Page Request

When we request a web page, several protocols work together to deliver the content from the server to our browser.

5.5.1 DHCP, UDP, IP, and Ethernet

- **DHCP (Dynamic Host Configuration Protocol)**: Your device uses DHCP to obtain an IP address, subnet mask, default gateway, and DNS server information automatically. DHCP messages are sent over UDP, a connectionless protocol, using IP addresses to communicate.
- **UDP (User Datagram Protocol)**: UDP is used for sending messages that don't require acknowledgment, like DHCP requests.
- **IP (Internet Protocol)**: IP handles addressing and routing packets between devices, ensuring data reaches its destination.
- **Ethernet**: Ethernet is the link-layer protocol used for wired connections in local networks, managing the actual transmission of data frames.

5.5.2 DNS and ARP

- **DNS (Domain Name System)**: When you enter a web address, your device uses DNS to translate the domain name into an IP address. This involves querying DNS servers to resolve the human-readable address into a machine-readable IP address.
- **ARP (Address Resolution Protocol)**: ARP is used to map IP addresses to MAC addresses on a local network. Before sending data to the destination IP, your device uses ARP to find the corresponding MAC address of the next hop on the path to the destination.

5.5.3 Intra-Domain Routing to the DNS Server

Intra-Domain Routing: Within a local network or an organization's network, routing protocols (like OSPF or RIP) direct packets to the DNS server. These protocols ensure that your request for DNS resolution reaches the correct server within the network.

5.5.4 Web Client-Server Interaction: TCP and HTTP

- **TCP (Transmission Control Protocol)**: TCP establishes a reliable connection between your device (client) and the web server. It ensures that data packets are delivered in order and without errors.
- **HTTP (Hypertext Transfer Protocol)**: Once the TCP connection is established, HTTP is used to request and receive the web page data. The browser sends an HTTP request to the server, and the server responds with the requested web page content.