

SIT 202 – COMPUTER NETWORKS AND COMMUNICATION:

DATA LINK LAYER

SUMMARY

MODULE LEARNING OBJECTIVES:

- ***Understand the principles behind the data-link layer services***
- ***Explain different error detection and correction techniques used***
- ***Analyse and explain medium access control, link layer addressing, and local area networks***

The Data Link Layer is the second layer of the OSI (Open Systems Interconnection) model. Its primary role is to facilitate reliable communication between directly connected nodes on a network. We can think of it as a set of rules and processes that ensure our data is transmitted accurately.

Key Functions:

1. ****Framing****: We package raw bits into frames, making it easier to manage and understand the data we are sending.
2. ****Error Detection and Correction****: We include mechanisms to identify and correct any errors that might occur during transmission, ensuring our data arrives intact.
3. ****Flow Control****: We manage the rate of data transmission so that the receiver is not overwhelmed, allowing for smooth communication.
4. ****Medium Access Control (MAC)****: We determine how multiple devices can share the same physical medium, like deciding who gets to speak when in a conversation.

Real-Life Example:

Imagine we are sending a letter to a friend. Before we send it, we:

1. ****Write the Letter****: This represents the creation of our data.
2. ****Put it in an Envelope****: This is like framing; the envelope protects our letter and makes it easier to handle.
3. ****Address the Envelope****: Just as each data frame has a MAC address, our envelope has our friend's address to ensure it reaches the right destination.
4. ****Drop it in the Mail****: This step is similar to sending the frame over the physical layer, whether through wires or wireless signals.

When our friend receives the envelope, they check if it's intact (error detection). If it's torn or damaged, they know something went wrong during transmission and might ask us to send a new letter.

We use the Data Link Layer for several key reasons:

1. Reliable Communication

It ensures accurate data transmission through error detection and correction.

2. Framing

It organizes raw data into frames, making it easier to manage.

3. Addressing

It uses MAC addresses to identify devices on a local network.

4. Flow Control

It regulates data transmission speed to prevent overloading.

5. Medium Access Control

It manages access to shared communication mediums, preventing collisions.

Example

In an office with a shared printer, the Data Link Layer ensures that documents are sent correctly, prevents jams from simultaneous printing, and organizes communication efficiently, enhancing productivity.

SERVICES PROVIDED BY DATA LINK LAYER :

FLOW CONTROL : pacing between adjacent sending and receiving nodes.

ERROR DETECTION : errors caused by signal attenuation, noise .

Receiver detects errors , signals , retransmission , or drops frame

ERROR CORRECTION : receiver identifies and corrects bit errors without retransmission .

HALF DUPLEX FULL DUPLEX :

With half duplex , nodes at both ends of link can transmit but not at same time.

ERROR DETECTION AND CORRECTION

Two of the main services provided by the link layer are error detection and error correction. The link layer is responsible for detecting and correcting errors in link-layer frames that are sent by the physically connected (via wired or wireless medium) neighbouring nodes.

Three techniques used for the error detections and corrections are:

- **Parity check:** simple form (discussed in the above video)
- **Internet checksum:** we have discussed this in Module 3 and Module 4. You can watch the following video to review checksum calculations
- **Cyclic Redundancy Check (CRC):** This is the third technique that is widely used in link layer for error detections and corrections. Let's see how CRC is calculated.

The link layer in networking plays a crucial role in ensuring that data transmitted between neighboring nodes is accurate and reliable. This is achieved through two primary services: error detection and error correction.

Error Detection: Error detection involves identifying errors that may have occurred during the transmission of data frames. Common techniques include:

- **Checksums:** A value calculated from the data and sent along with it. The receiver calculates the checksum again and compares it with the received checksum to check for discrepancies.
- **Cyclic Redundancy Check (CRC):** A more robust method that uses polynomial division to detect changes to raw data.

Error Correction: Error correction goes a step further by not just identifying errors but also correcting them. Techniques include:

- **Hamming Code:** This method adds extra bits to the data to allow for the detection and correction of errors. It can fix single-bit errors and detect two-bit errors.
- **Reed-Solomon Codes:** Often used in CDs and DVDs, this method can correct multiple errors in a block of data.

Real-Life Example: Sending a Package

Imagine sending a package through a postal service:

1. **Preparing the Package (Creating Frames):** You carefully pack items in a box (data frame) and include a note with the total weight (checksum).
2. **Sending the Package (Transmission):** The package is sent via a delivery truck (network medium) to your friend. During transit, the package might get jostled, and the contents could shift.
3. **Package Arrival (Receiving Frames):** When your friend receives the package, they check the note to see if the weight matches what they expect. If it doesn't (error detection), they might find that something inside has broken or shifted (indicating a problem).
4. **Resolving Issues (Error Correction):** If your friend finds that the package is damaged, they could either:
 - Contact the postal service to report the issue (request a retransmission).
 - Use some tools they have to fix the broken item (error correction), if possible.

Multiple access control protocol

Multiple access control protocols are essential for managing how multiple devices communicate over a shared network channel without interfering with each other. These protocols ensure that data transmission is organized and efficient, preventing collisions and ensuring fair access for all nodes.

Types of Multiple Access Control Protocols:

1. Time Division Multiple Access (TDMA): Divides the channel into time slots, allowing each device to transmit in its designated slot.
2. Frequency Division Multiple Access (FDMA): Assigns different frequency bands to each device for simultaneous communication.
3. Carrier Sense Multiple Access (CSMA): Devices listen to the channel before transmitting. If the channel is clear, they send their data. Variants include:
 - o CSMA/CD (Collision Detection): Used in wired networks (like Ethernet), where devices detect collisions and take action to retransmit.
 - o CSMA/CA (Collision Avoidance): Used in wireless networks (like WiFi), where devices avoid collisions by sending a signal indicating they intend to transmit.

Real-Life Example:

Imagine a Busy Intersection:

- Scenario: Cars at a traffic light intersection represent nodes trying to use the same road (shared channel).
- TDMA: Each car is allowed to go at a specific time. For example, cars from the north can go every 30 seconds, then those from the south.
- FDMA: Different lanes are designated for each direction. Northbound cars use one lane (frequency), while southbound cars use another.
- CSMA: Before a car enters the intersection, it checks if the road is clear. If it sees another car already moving, it waits. If the road is clear, it goes ahead. In CSMA/CD, if two cars enter the intersection simultaneously, they stop and wait before trying again.
- CSMA/CA: Before proceeding, a car signals its intention to move. This way, other cars can avoid entering the intersection at the same time.

Multiple access control protocols can be mainly categorised into three groups. They are:

1. Channel partitioning
2. Random access
3. Taking turns protocols

CHANNEL PARTITIONING PROTOCOLS:

Channel partitioning protocols are techniques used to divide a shared communication channel among multiple users or devices, allowing them to transmit data without interference. These protocols ensure that each user has a designated portion of the channel, thus minimizing collisions and maximizing efficiency.

Types of Channel Partitioning Protocols:

1. **Time Division Multiple Access (TDMA)**: The channel is divided into time slots, and each user is assigned a specific time slot for transmission.
2. **Frequency Division Multiple Access (FDMA)**: The channel is divided into different frequency bands, with each user assigned a specific frequency for communication.
3. **Code Division Multiple Access (CDMA)**: Each user is assigned a unique code that allows them to transmit simultaneously over the same frequency band, with the codes helping to differentiate between the users' signals.

Real-Life Example:

Imagine a Radio Station:

- **Scenario**: A radio station that wants to broadcast multiple shows at different times and frequencies.
 1. **TDMA**:
 - The station schedules different shows at specific time slots throughout the day. For instance, a news program airs from 8:00 to 9:00 AM, while a music show takes over from 9:00 to 10:00 AM. Each show has its own time to broadcast without overlap.
 2. **FDMA**:
 - The station uses different frequencies for each show. For example, the news show might be broadcast on 101.5 FM, while a talk show

airs on 102.5 FM. Each program has its own frequency, allowing them to transmit simultaneously without interference.

3. CDMA:

- Imagine that instead of different frequencies, the station broadcasts multiple programs on the same frequency but uses distinct codes. Each listener's radio can decode their chosen program by recognizing its unique code, allowing multiple shows to be transmitted simultaneously without overlap.

RANDOM ACCESS PROTOCOLS :

Random access protocols are communication protocols that allow multiple users or devices to access a shared communication channel without predetermined scheduling. These protocols enable users to transmit data whenever they have data to send, making them efficient for bursty traffic. However, since multiple users may attempt to transmit simultaneously, random access protocols include mechanisms to manage collisions.

Types of Random Access Protocols:

1. ALOHA Protocol:

- Users transmit whenever they have data. If a collision occurs (two users transmit simultaneously), they wait a random amount of time before attempting to retransmit.

2. Carrier Sense Multiple Access (CSMA):

- Before transmitting, a device listens to the channel (carrier sensing) to check if it's free. If the channel is busy, it waits until it's clear. Variants include:
 - **CSMA/CD (Collision Detection):** Used in wired networks, where devices can detect collisions and back off for a random time before retransmitting.
 - **CSMA/CA (Collision Avoidance):** Used in wireless networks, where devices avoid collisions by waiting for a clear channel and using acknowledgments.

Real-Life Example:

Imagine a Busy Coffee Shop:

- **Scenario:** Customers (users) want to order coffee (send data) at a counter (shared channel).

1. ALOHA:

- Customers approach the counter when they are ready to order. If two customers start ordering at the same time, they both might get confused and have to step back (collision). After a random time, they each try again to place their order.

2. CSMA:

- Customers first check if the counter is free (carrier sensing). If they see that no one is at the counter, they step up to place their order. If they see someone ordering, they wait until the counter is clear before they attempt to place their order.

3. CSMA/CD:

- If two customers step up simultaneously and a misunderstanding occurs (collision), they both notice it and step back to wait a moment before trying again, each selecting a random time to re-approach the counter.

4. CSMA/CA:

- Before a customer approaches the counter, they listen to the environment. If they see that the counter is busy, they will wait, and when it clears, they will step up cautiously. They might also raise a hand to signal their intent before stepping up, reducing the chance of simultaneous orders.

LOCAL AREA NETWORK

The data-link layer is responsible for transferring data packets, known as datagrams, between nodes that are physically close to each other within a local area network (LAN). A LAN is essentially a group of devices connected in a specific physical location, which can range in size from a small home network to larger setups like those in schools or offices.

To enable the transfer of datagrams between neighboring nodes in a LAN, unique addresses are required. In the data-link layer, these addresses are known as MAC addresses (Media Access Control addresses), which are also referred to as physical or Ethernet addresses.

Real-Life Example

Consider a small office where multiple computers, printers, and other devices are connected to the same network. Each device has a unique MAC address that serves as its identifier on the network. When one computer wants to send

a document to a networked printer, it uses the printer's MAC address to ensure the data is delivered to the correct device.

For instance, if Computer A, with a MAC address of `00:1A:2B:3C:4D:5E`, wants to print a document, it will package the data into a datagram and include the printer's MAC address, say `00:1A:2B:3C:4D:6F`, in the packet header. This way, the network knows exactly where to send the data, ensuring efficient communication within the office LAN.

By using MAC addresses, the data-link layer facilitates reliable data transfer between devices in a localized network, helping streamline everyday tasks like printing and file sharing.

Address Resolution Protocol (ARP)

The Address Resolution Protocol (ARP) is a network protocol used to map an IP address to a MAC address within a local area network (LAN). When a device wants to communicate with another device using its IP address, it needs to know the corresponding MAC address to ensure that the data packets are correctly delivered over the physical network.

How ARP Works

1. **Request**: When a device (let's call it Device A) wants to send data to another device (Device B), it first checks its ARP cache to see if it already knows the MAC address associated with Device B's IP address. If it doesn't find the address, Device A broadcasts an ARP request to all devices in the LAN. This request essentially says, "Who has the IP address X.X.X.X? Please send me your MAC address."

2. **Response**: All devices on the network receive this ARP request, but only Device B (the one with the matching IP address) responds. Device B sends back an ARP reply, which includes its MAC address.

3. **Update Cache**: Device A receives the ARP reply and updates its ARP cache with the new MAC address, allowing it to communicate directly with Device B in the future without needing to send another ARP request.

Real-Life Example

Imagine a scenario in an office setting:

1. **Devices**: You have a laptop (Device A) and a printer (Device B) on the same local network.
2. **Action**: You want to print a document from your laptop to the printer. Your laptop knows the printer's IP address (e.g., `192.168.1.10`) but doesn't know its MAC address.
3. **ARP Request**: Your laptop broadcasts an ARP request: "Who has the IP address 192.168.1.10? Please send me your MAC address."
4. **ARP Response**: The printer, which has the IP address `192.168.1.10`, sees the request and responds with its MAC address (e.g., `00:1A:2B:3C:4D:5E`).
5. **Printing**: Now that the laptop has the printer's MAC address, it can send the print job directly to the printer over the network.

ETHERNET :

Ethernet: An Overview

Ethernet is a widely used networking technology that defines how data is transmitted over local area networks (LANs). It operates primarily at the data-link layer of the OSI model and is known for its reliability and speed. Ethernet uses a protocol to format data into packets and provides mechanisms for error checking, addressing, and managing access to the physical network medium.

Key Features of Ethernet

1. **Frame Structure**: Ethernet encapsulates data in frames that contain source and destination MAC addresses, type/length fields, and a checksum for error detection.
2. **Media**: It can operate over various types of cabling, including twisted pair (commonly used in homes and offices), coaxial cables, and fiber optics.
3. **Speed**: Ethernet standards have evolved to support various speeds, from the original 10 Mbps to 1 Gbps and beyond (10 Gbps, 100 Gbps, etc.).
4. **Broadcast Domain**: All devices on the same Ethernet network share a broadcast domain, meaning that broadcast packets are sent to all devices in that segment.

Real-Life Example

Imagine an office environment where multiple employees are using desktop computers connected to a network.

1. **Setup**: Each computer is connected to an Ethernet switch via twisted-pair cables. The switch acts as a central hub, managing traffic between the devices.
2. **Communication**: When Employee A wants to send a file to Employee B's computer, the following happens:
 - Employee A's computer formats the file into an Ethernet frame, including its own MAC address and Employee B's MAC address.
 - The frame is sent over the Ethernet network to the switch.

3. **Switch Functionality**: The switch receives the frame and checks the destination MAC address. It then forwards the frame only to the port connected to Employee B's computer, rather than broadcasting it to all devices.
3. **Reception**: Employee B's computer receives the Ethernet frame, extracts the file, and processes it accordingly.

Each field in the Ethernet frame has a purpose.

- Preamble: this field is used to wake up the adapter if they are out of sync and to synchronise the receiver's clock before transferring the data.
- Destination address: The MAC address of the destination adapter is notified by this field.
- Source address: The Ethernet frame is transmitted to LAN by an adapter with this MAC address.
- Type: This field is used to notify the network layer protocol used (remember we have similar fields in network layer datagram and transport layer segments to notify the upper layer protocol used)
- Data: IP datagram is carried in this field and size of this field can vary from 46 Bytes to 1500 Bytes. You can see that if the IP datagram is longer than 1500 Bytes, then that IP datagram has to be fragmented to fit into the data field of the Ethernet frame.
- CRC: We know that the cyclic redundancy check (CRC) is used to detect errors.

Virtual LAN (VLAN): An Overview

A Virtual Local Area Network (VLAN) is a logical subdivision of a physical network that allows devices to communicate as if they are on the same local area network, even if they are physically located in different areas. VLANs enhance network management, security, and efficiency by grouping devices based on function rather than physical location.

Key Features of VLANs

1. **Logical Segmentation:** VLANs allow network administrators to segment networks logically, creating distinct broadcast domains without needing separate physical infrastructure.
2. **Enhanced Security:** By isolating sensitive data and devices, VLANs can improve security. Devices on one VLAN cannot directly communicate with those on another unless routed through a firewall.
3. **Improved Performance:** Reducing broadcast traffic by confining it to specific VLANs helps optimize network performance.
4. **Flexibility and Scalability:** VLANs can be easily reconfigured as organizational needs change, allowing for dynamic adjustment of network resources.

Real-Life Example

Consider a university campus with several departments, such as Computer Science, Mathematics, and Administration.

1. **Physical Network:** All departments share the same physical network infrastructure, with switches connecting computers in each department.
2. **VLAN Configuration:**
 - o The network administrator sets up separate VLANs for each department:
 - **VLAN 10** for Computer Science
 - **VLAN 20** for Mathematics
 - **VLAN 30** for Administration
3. **Benefits:**
 - o **Isolation:** Computers in the Computer Science department can communicate with each other without their traffic affecting the Mathematics or Administration departments.
 - o **Security:** Sensitive administrative data remains secure and isolated from students and faculty in other departments.
 - o **Resource Management:** If the Computer Science department needs more bandwidth, the administrator can adjust settings within VLAN 10 without impacting other departments.

REFLECTIONS :

Most Important Learning: The most significant takeaway from this module is understanding the critical functions of the Data Link Layer in ensuring reliable communication between directly connected nodes. It encapsulates data into frames, detects and corrects errors, manages flow control, and oversees

medium access. This foundational knowledge is essential for grasping how data moves across a network.

Relation to Prior Knowledge: This content builds upon my existing understanding of networking fundamentals, particularly the OSI model. Previously, I had a basic grasp of how data is transmitted but lacked insight into the specific mechanisms that ensure data integrity and efficient communication. The concepts of MAC addressing and error management are now clearer, linking theory to practical applications.

Purpose of Learning: The course team likely emphasizes this module because a solid grasp of the Data Link Layer is crucial for anyone pursuing a career in networking or IT. Understanding how data is framed, addressed, and managed lays the groundwork for more advanced topics, such as network design and troubleshooting. It's essential for ensuring efficient and secure data transmission in real-world scenarios.