Computer Network

Unit 2 Questions:

Q1. What are the design issue in Data link Layer?

Ans. The design issues in the Data Link Layer include the following:

1. **Framing**: Determining how to break the data stream into manageable units or frames, including defining frame boundaries.
2. **Error Detection and Correction**: Implementing mechanisms to detect and correct errors that may occur during data transmission. This includes techniques like checksums, CRC, and Hamming codes.
3. **Flow Control**: Managing the rate of data transmission between sender and receiver to prevent the sender from overwhelming the receiver. Common methods include stop-and-wait and sliding window protocols.
4. **Access Control**: Regulating how multiple devices access the shared medium, especially in networks with multiple nodes. Protocols like CSMA/CD and token ring help manage this.
5. **Link Layer Protocols**: Defining the specific protocols used for communication at the Data Link Layer, such as Ethernet, PPP (Point-to-Point Protocol), and HDLC (High-Level Data Link Control).
6. **Physical Addressing**: Including the use of MAC addresses to identify devices on the network for proper data delivery.
7. **Link Management**: Establishing, maintaining, and terminating connections between devices, ensuring reliable communication.

Q2. What are Data Link Control and Protocols? Explain in detail.

Ans. Data Link Control refers to the protocols and mechanisms used in the Data Link Layer of the OSI model to manage data transmission between directly connected network nodes. It ensures that data frames are transmitted reliably and efficiently over the physical medium. The primary functions of Data Link Control include framing, addressing, error detection and correction, flow control, and medium access control. Here's a detailed overview:

1. **Framing**: This process involves encapsulating network layer packets into frames with defined headers and trailers. The header typically includes source and destination MAC addresses, while the trailer may include error-checking information. Various methods can be used for framing, including byte stuffing, bit stuffing, and fixed-size frames.
2. **Addressing**: Data Link Layer protocols use physical addressing to identify devices on a local network. Each network interface card (NIC) has a unique MAC address, which is used to ensure that frames reach the correct destination.
3. **Error Detection and Correction**: Protocols implement mechanisms to identify and correct errors that occur during data transmission. Common techniques include:
    - **Checksums**: A simple method that sums the data in a frame and appends the result.

    - **Cyclic Redundancy Check (CRC)**: A more robust method that treats data as polynomials and checks for errors using polynomial division.
    - **Hamming Code**: An error-correcting code that allows for the detection and correction of single-bit errors.
4. **Flow Control**: This ensures that a sender does not overwhelm a receiver by sending data too quickly. Common flow control methods include:
    - **Stop-and-Wait ARQ**: The sender transmits one frame and waits for an acknowledgment (ACK) from the receiver before sending the next frame.
    - **Sliding Window Protocol**: This allows multiple frames to be in transit before requiring an ACK, increasing efficiency and throughput.
5. **Medium Access Control (MAC)**: In networks where multiple devices share the same communication medium, MAC protocols manage how devices gain access to the medium. Various methods include:
    - **Carrier Sense Multiple Access (CSMA)**: Devices listen to the medium before transmitting.
    - **Token Ring**: A token circulates around the network, and only the device holding the token can transmit.
    - **Time Division Multiple Access (TDMA)**: Time slots are assigned to devices for transmission.
6. **Link Layer Protocols**: Several specific protocols operate at the Data Link Layer, including:
    - **Ethernet**: The most widely used LAN technology, utilizing CSMA/CD for collision detection.
    - **PPP (Point-to-Point Protocol)**: Commonly used for direct connections between two nodes, providing authentication and compression.
    - **HDLC (High-Level Data Link Control)**: A bit-oriented protocol used for point-to-point and multipoint connections, providing framing, error control, and flow control.

In summary, Data Link Control and its associated protocols play a crucial role in ensuring that data is transmitted reliably, efficiently, and securely across the physical network. They manage the complexities of data communication, allowing higher layers of the OSI model to focus on processing and interpreting the data rather than the details of transmission.

Q3. What is Flow and Error Control, Stop-and-wait ARQ? Explain in detail.

Ans. Flow and error control are essential functions of the Data Link Layer, ensuring reliable communication between devices in a network. Here's a detailed explanation:

Flow Control

Flow control is a technique used to manage the pace at which data is sent from a sender to a receiver, ensuring that the receiver is not overwhelmed by too much data at once. It helps prevent buffer overflow at the receiver, which can lead to data loss. The main methods of flow control include:

1. **Stop-and-Wait Protocol**:

- In this protocol, the sender transmits a single frame and waits for an acknowledgment (ACK) from the receiver before sending the next frame.
- This method is simple and easy to implement, but it can be inefficient, especially in high-latency networks, as the sender remains idle while waiting for the ACK.

2. **Sliding Window Protocol**:
    - This method allows multiple frames to be sent before requiring an ACK for the first frame.
    - The sender maintains a "window" of frames that can be sent without waiting for acknowledgment, increasing the throughput and efficiency of the communication.
    - The size of the window can be adjusted based on network conditions, allowing for more flexibility.

Error Control

Error control involves techniques used to detect and correct errors that may occur during data transmission. The primary methods for error control include:

1. **Error Detection**:
    - Mechanisms that identify errors in transmitted frames. Common techniques include:
        - **Checksums**: A simple error detection method where a checksum value is calculated from the data and sent along with the frame. The receiver calculates the checksum again to check for discrepancies.
        - **Cyclic Redundancy Check (CRC)**: A more robust method that treats data as polynomials and checks for errors using polynomial division. It provides better error detection capabilities than checksums.
2. **Error Correction**:
    - Mechanisms that not only detect errors but also correct them. Common techniques include:
        - **Hamming Code**: A method that adds redundant bits to the data, allowing the detection and correction of single-bit errors.
        - **Reed-Solomon Code**: A more advanced error-correcting code that can correct multiple errors, widely used in data storage and transmission.

Stop-and-Wait ARQ

Stop-and-Wait Automatic Repeat reQuest (ARQ) is a specific protocol used in flow and error control. It combines the concepts of flow control with error detection and correction. Here’s how it works:

1. **Transmission Process**:
    - The sender transmits a data frame to the receiver.
    - After sending the frame, the sender waits for an acknowledgment (ACK) from the receiver before sending the next frame.
2. **Acknowledgment**:
    - The receiver checks the received frame for errors using a detection method (e.g., CRC).

- If the frame is received correctly, the receiver sends an ACK back to the sender.
- If an error is detected, the receiver sends a negative acknowledgment (NACK) or does not respond, prompting the sender to retransmit the same frame.

3. **Efficiency**:
    - While the Stop-and-Wait ARQ is simple and easy to implement, it can be inefficient in high-latency environments due to the idle time spent waiting for ACKs.
    - The protocol is best suited for low-speed networks or situations where reliability is crucial.

In summary, flow and error control are critical for ensuring reliable communication in data networks. The Stop-and-Wait ARQ method effectively manages data transmission by combining flow control with error detection and correction, although it may not be the most efficient approach in high-latency environments.

Q4. Explain Sliding Window Protocol in detail?

Ans. The Sliding Window Protocol is an efficient flow control method used in the Data Link Layer of network communication. It allows for the transmission of multiple frames before requiring an acknowledgment (ACK) for the first frame, optimizing the use of available bandwidth and reducing idle time. Here's a detailed explanation of how the Sliding Window Protocol works:

Key Concepts

1. **Window Size**:
    - The window size determines how many frames can be sent before receiving an acknowledgment. This size can be fixed or variable, depending on the implementation.
    - A sender can transmit a specified number of frames (the window size) without needing to wait for an acknowledgment for the first transmitted frame.
2. **Frames and Sequence Numbers**:
    - Each frame is assigned a unique sequence number to keep track of the order in which frames are sent and received.
    - The sequence numbers help manage retransmissions in case of errors.
3. **Sender and Receiver Windows**:
    - **Sender Window**: Represents the range of sequence numbers that the sender is allowed to transmit without waiting for an acknowledgment. The sender can send frames within this window.
    - **Receiver Window**: Indicates the range of sequence numbers that the receiver is expecting to receive in order. This helps the receiver identify out-of-order frames.

Working Mechanism

1. **Initialization**:
    - The sender initializes the window with a specified size (N), allowing N frames to be sent before requiring an acknowledgment.
    - The sender keeps track of the sequence numbers of the frames being sent and the next expected ACK.

2. **Frame Transmission**:
    - The sender can transmit all frames within the current window. Once the sender transmits a frame, it slides the window forward by one frame as it receives ACKs.
    - The sender maintains a buffer of frames that have been sent but not yet acknowledged.
3. **Acknowledgment**:
    - The receiver sends an ACK for the highest-sequence-numbered frame received in order. If all frames up to a certain number have been received, the receiver sends an ACK for that number.
    - If the receiver detects an error in a frame, it may send a negative acknowledgment (NACK) for that specific frame, prompting the sender to retransmit it.
4. **Sliding the Window**:
    - When the sender receives an ACK, it slides the window forward to allow the transmission of new frames. For example, if the sender's window size is 4 and it has transmitted frames 0, 1, 2, and 3, once it receives an ACK for frame 0, it can slide the window to transmit frame 4.
    - If the receiver sends a NACK or does not send an ACK for an expected frame, the sender does not slide the window and retransmits the missing frame.

Advantages

- **Increased Throughput**: By allowing multiple frames to be sent before requiring an acknowledgment, the Sliding Window Protocol effectively utilizes the available bandwidth and reduces idle time.
- **Flow Control**: The protocol manages the flow of frames based on the receiver's capacity, preventing buffer overflow.
- **Error Handling**: The use of sequence numbers and acknowledgments allows for effective error detection and retransmission.

Types of Sliding Window Protocols

1. **Go-Back-N ARQ**:
    - The sender can send multiple frames (up to the window size), but if an error occurs, all subsequent frames must be retransmitted, even if they were received correctly.
2. **Selective Repeat ARQ**:
    - Similar to Go-Back-N, but the sender only retransmits the specific frames that were detected as erroneous, allowing for more efficient use of bandwidth.

Summary

The Sliding Window Protocol is a robust and efficient method for managing data transmission in computer networks. By allowing multiple frames to be in transit at once and utilizing sequence numbers for error detection and acknowledgment, it enhances the reliability and efficiency of communication between devices. The protocol is widely used in various networking technologies, including TCP/IP, ensuring smooth data flow in both wired and wireless networks.

Q5. What is Go-Back-N ARQ?

Ans. Go-Back-N ARQ (Automatic Repeat reQuest) is an error control protocol used in data communication for reliable transmission. It is a type of sliding window protocol that allows a sender to send multiple frames before needing an acknowledgment for the first frame sent. Here's a concise explanation of its key features and functioning:

Key Features

1. **Window Size (N)**:
    - The sender can send up to N frames before waiting for an acknowledgment. The receiver can only receive frames in order.
2. **Sequence Numbers**:
    - Each frame is assigned a unique sequence number. The sequence numbers help in tracking the order of frames and managing retransmissions.
3. **Acknowledgment**:
    - The receiver sends an acknowledgment (ACK) for the highest-numbered frame that it has received in order. If a frame is missing or erroneous, the receiver does not acknowledge frames that follow the erroneous one.

Working Mechanism

1. **Frame Transmission**:
    - The sender transmits frames sequentially up to the window size. For example, if the window size is 4, frames 0, 1, 2, and 3 can be sent before requiring an ACK.
2. **Receiving ACK**:
    - When the receiver gets a frame correctly, it sends an ACK for the highest correctly received frame. For instance, if frames 0, 1, and 2 are received correctly, the receiver will send an ACK for frame 2.
3. **Handling Errors**:
    - If the receiver detects an error in a frame (e.g., frame 3 is lost or corrupted), it will not acknowledge frame 3 or any subsequent frames. Instead, the sender must go back and retransmit frame 3 and all subsequent frames (frames 4 and onwards) even if they were received correctly.
4. **Sliding the Window**:
    - Upon receiving an ACK, the sender slides the window forward, allowing it to send new frames. For example, if the sender receives an ACK for frame 2, it can send frame 4 next, keeping the window size intact.

Advantages

- **Simplicity**: Go-Back-N is straightforward to implement and understand.
- **Error Recovery**: It efficiently manages errors by allowing for quick retransmissions of lost frames.

Disadvantages

- **Inefficiency with High Loss Rates**: If the error rate is high, a large number of frames may need to be retransmitted, which can lead to inefficiency.
- **Increased Latency**: Retransmitting all frames after an error can introduce delays, particularly in high-latency networks.

Summary

Go-Back-N ARQ is a reliable data transmission protocol that balances the need for speed and reliability. It is commonly used in various networking applications where maintaining the order and integrity of transmitted data is crucial, such as in TCP/IP networks.

Q6. Explain Selective Repeat ARQ?

Ans. Selective Repeat ARQ (Automatic Repeat reQuest) is an error control protocol used in data communication that allows a sender to retransmit only the frames that were lost or corrupted, rather than all frames following an error. This protocol enhances efficiency and reduces unnecessary retransmissions compared to the Go-Back-N ARQ protocol. Here's a detailed overview:

Key Features

1. **Window Size (N)**:
    - Like Go-Back-N, Selective Repeat uses a sliding window mechanism where the sender can send multiple frames before requiring an acknowledgment. The window size is defined by N, determining how many frames can be in transit without acknowledgment.
2. **Sequence Numbers**:
    - Each frame is assigned a unique sequence number. This allows both the sender and receiver to keep track of which frames have been transmitted and acknowledged.
3. **Acknowledgment**:
    - The receiver sends individual acknowledgments (ACKs) for each correctly received frame. If a frame is received with errors or is missing, the receiver will send a negative acknowledgment (NAK) for that specific frame.

Working Mechanism

1. **Frame Transmission**:
    - The sender transmits frames up to the window size. For instance, if the window size is 4, the sender can send frames 0, 1, 2, and 3.
2. **Receiving ACKs**:
    - The receiver acknowledges each correctly received frame. For example, if frames 0 and 1 are received correctly, the receiver sends ACKs for both frames.
3. **Handling Errors**:
    - If a frame is lost or corrupted (e.g., frame 2), the receiver sends a NAK for that specific frame. The sender only retransmits frame 2 instead of all subsequent frames.
4. **Sliding the Window**:

- Upon receiving ACKs, the sender can slide the window forward to send new frames. If frame 2 is retransmitted and received correctly, the sender can then proceed to send frames 4 and onwards.

Advantages

- **Efficiency**: Selective Repeat is more efficient than Go-Back-N because it reduces the number of retransmissions by only resending erroneous or lost frames.
- **Reduced Latency**: By avoiding unnecessary retransmissions, Selective Repeat can achieve lower latency, especially in networks with higher error rates.

Disadvantages

- **Complexity**: Selective Repeat is more complex to implement than Go-Back-N due to the need for maintaining multiple buffers for received frames and the management of individual ACKs and NAKs.
- **Buffering Requirements**: The receiver needs to have sufficient buffering to hold out-of-order frames until the missing frames are received.

Summary

Selective Repeat ARQ is a reliable data transmission protocol that optimizes the error recovery process by only retransmitting the affected frames, making it suitable for high-speed networks where minimizing delays and maximizing efficiency are essential. It is widely used in various communication systems, including wireless and data link layer protocols.

Q7. What is HDLC?

Ans. HDLC (High-Level Data Link Control) is a bit-oriented synchronous data link layer protocol used for transmitting data over point-to-point and multipoint links. It was developed by the International Organization for Standardization (ISO) and is widely used in various communication systems. Here's an overview of HDLC:

Key Features

1. **Framing**:
    - HDLC uses a specific frame structure to encapsulate data. Each frame begins and ends with a unique flag sequence (01111110), which allows the receiver to identify the start and end of the frame.
2. **Frame Types**:
    - HDLC defines three types of frames:
        - **Information Frame (I-frame)**: Carries user data and control information. It is used for the transfer of data between devices.
        - **Supervisory Frame (S-frame)**: Provides control information to manage the flow of data (e.g., acknowledgments, requests for retransmission).
        - **Unnumbered Frame (U-frame)**: Used for various control functions such as connection establishment and termination.
3. **Addressing**:

- Each HDLC frame can include an address field to identify the sender and receiver, allowing communication between multiple devices on the same link.

4. **Error Control**:
    - HDLC employs mechanisms for error detection using a Frame Check Sequence (FCS), typically based on a cyclic redundancy check (CRC). If an error is detected, the receiver can request retransmission of the affected frame.
5. **Flow Control**:
    - HDLC supports flow control to manage data transmission rates between sender and receiver, ensuring that the sender does not overwhelm the receiver with too much data.

Operation

- **Synchronous Transmission**: HDLC operates synchronously, meaning both the sender and receiver are synchronized to a common clock.
- **Bit-Oriented**: It is a bit-oriented protocol, meaning it processes data as a stream of bits rather than bytes, allowing it to manage various data sizes efficiently.

Applications

- HDLC is commonly used in telecommunications, including point-to-point links, leased lines, and satellite communication. It serves as a foundation for several higher-level protocols, such as Frame Relay and X.25.

Summary

HDLC is a robust and versatile data link layer protocol designed for reliable communication over various network types. Its features, including framing, error control, and flow control, make it suitable for both point-to-point and multipoint configurations in diverse communication environments.

Q8. Elaborate Point-to-Point Access: PPP Point –to–Point Protocol, PPP Stack.

Ans. Point-to-Point Protocol (PPP) is a widely used data link layer protocol that facilitates direct communication between two network nodes, typically over serial links. It is commonly used for establishing internet connections via dial-up modems, DSL, and other types of point-to-point communications. Here's an elaboration on PPP and its stack:

Key Features of PPP

1. **Encapsulation**:
    - PPP encapsulates network layer packets (such as IP packets) within its frames, allowing different types of protocols to be transmitted over the same physical link.
2. **Link Quality Monitoring**:
    - PPP includes mechanisms for monitoring the quality of the link, allowing it to detect issues like link failures and initiate recovery processes.
3. **Authentication**:

- PPP supports multiple authentication methods, including Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP), to verify the identity of the connecting device.

4. **Multilink Support**:
    - PPP can aggregate multiple physical connections into a single logical connection using Multilink PPP (MLPPP), enhancing bandwidth and redundancy.
5. **Network Layer Protocol Support**:
    - PPP can carry multiple network layer protocols by using a Protocol field in its frame header, allowing interoperability with various networking technologies.

PPP Frame Structure

A typical PPP frame consists of the following fields:

- **Flag**: A single byte marking the start and end of the frame (0x7E).
- **Address**: Usually set to a broadcast address (0xFF) in point-to-point links.
- **Control**: Generally set to 0x03, indicating unnumbered information frames.
- **Protocol**: Specifies the encapsulated protocol (e.g., 0x0021 for IP).
- **Information**: Contains the encapsulated data payload.
- **FCS (Frame Check Sequence)**: A sequence used for error detection, typically a CRC.

PPP Stack

PPP operates on a layered architecture, allowing it to interact with various network protocols. The key components of the PPP stack include:

1. **Physical Layer**:
    - The physical medium over which the PPP frames are transmitted (e.g., serial links, ISDN, etc.).
2. **Data Link Layer (PPP)**:
    - Implements the PPP protocol itself, handling framing, error detection, link quality monitoring, and authentication.
3. **Network Layer**:
    - Carries the actual network layer protocols, such as IP, IPv6, IPX, and AppleTalk, encapsulated within PPP frames. PPP provides a flexible mechanism to support various protocols without changing its core functionality.
4. **Control Protocols**:
    - PPP uses several control protocols to negotiate the link parameters and establish the connection:
        - **LCP (Link Control Protocol)**: Used for establishing, configuring, and testing the data link connection.
        - **NCP (Network Control Protocol)**: Used for establishing and configuring the network layer protocols. Different NCPs exist for different protocols, such as IPCP (Internet Protocol Control Protocol) for IP.

Conclusion

PPP is a versatile and robust protocol for point-to-point communications, offering encapsulation, authentication, and link quality monitoring. Its layered architecture and support for multiple network layer protocols make it suitable for various networking applications, providing reliable connections for both dial-up and dedicated links.

Q9. Explain the function and requirements of DLL protocols.

Ans. **Explain the function and requirements of DLL protocols.**
Ans. Data Link Layer (DLL) protocols ensure reliable and error-free communication between two directly connected nodes in a network. Their main functions include:

1. **Framing**: Dividing data into manageable frames for transmission.
2. **Error Control**: Detecting and correcting errors in the frames.
3. **Flow Control**: Ensuring the sender doesn't overwhelm the receiver with too much data.
4. **Addressing**: Identifying source and destination MAC addresses.
5. **Synchronization**: Ensuring both devices are ready for data transmission.

Requirements include reliable error detection, acknowledgment mechanisms, and efficient data transmission without loss or duplication.\

Q10. **In sliding window protocol, can the sender receive an ACK for a packet that falls outside its current window? If yes, specify the scenario under which this occurs as well.**

Yes, in the sliding window protocol, the sender can receive an ACK for a packet that falls outside its current window. This happens when the receiver sends a cumulative acknowledgment, acknowledging all packets up to a certain point. If the sender has moved its window forward after receiving earlier ACKs, it may receive an ACK for a packet that is no longer in its current window. The scenario occurs when the window slides, and the ACK refers to a previously transmitted packet that was within the window before it shifted.

Q11. **In stop and wait ARQ, what happens if a negative acknowledgement is lost in transit?**

In stop-and-wait ARQ, if a negative acknowledgment (NAK) is lost, the sender will not receive it and will continue waiting for an acknowledgment. The sender has a timeout mechanism that triggers retransmission if no ACK or NAK is received within a certain time frame. If the NAK is lost, the sender will eventually time out and resend the packet, ensuring reliable data transmission even if the negative acknowledgment fails to reach the sender.

Q12. **What is CSMA? How is p-persistent CSMA different from non-persistent?**

CSMA (Carrier Sense Multiple Access) is a network protocol where a device checks the network to determine whether the communication channel is clear before attempting to transmit data. CSMA helps reduce collisions by ensuring that devices only transmit when the channel is idle.

- **p-persistent CSMA**: In this method, when a device senses that the channel is idle, it transmits with a probability ppp. If it does not transmit, it waits for the next time slot and tries again with the same probability. This approach allows for better control of collision probability.

- **Non-persistent CSMA**: In non-persistent CSMA, when a device finds the channel busy, it waits for a random amount of time before checking the channel again. If the channel is free, it transmits immediately. This reduces collisions, but can lead to longer delays compared to p-persistent CSMA.

Q13. **How is selective repeat better than Go-Back-N?**

Selective Repeat is better than Go-Back-N in several ways, particularly in terms of efficiency. In Go-Back-N, if an error occurs in one frame, the sender must retransmit all frames starting from the erroneous frame, even if subsequent frames were received correctly. This can lead to a lot of unnecessary retransmissions.

In contrast, **Selective Repeat** only retransmits the specific frames that were lost or erroneous. The receiver keeps track of each frame individually and can acknowledge non-erroneous frames even if they arrive out of order. This reduces the number of retransmissions, improving bandwidth utilization and overall throughput. However, Selective Repeat requires more buffer space and more complex logic compared to Go-Back-N.

Q14. **Compare the throughput of a pure ALOHA network with a slotted ALOHA network.**

- **Pure ALOHA**: In pure ALOHA, stations can transmit data whenever they have data to send, without waiting for a specific time slot. However, if two stations transmit at the same time, their packets collide, leading to a loss of both packets. The maximum throughput of pure ALOHA is **18.4%** of the total available bandwidth. This low efficiency is due to the high likelihood of collisions, as packets can be sent at any time.
- **Slotted ALOHA**: In slotted ALOHA, time is divided into discrete slots, and stations are only allowed to send data at the beginning of these time slots. This reduces the chances of collisions since stations are synchronized to transmit at specific intervals. The maximum throughput of slotted ALOHA is **36.8%**, which is significantly better than pure ALOHA due to the reduction in collision probability.

The higher efficiency of slotted ALOHA comes from the fact that it organizes transmissions into slots, minimizing the chances that two stations will collide by starting transmission simultaneously.