CNS QUESTION BANK ANSWERS

Unit 1: Introduction to computer networks

Definition, Types of Networks: Local area networks (LAN), Metropolitan area networks (MAN), Wide area networks (WAN), Wireless networks, Networks Software, Protocol, Design issues for the Network layers. Network Models: The OSI Reference Model, TCP/IP Model, Network Topologies, Types of Transmission Medium. Network Architectures: Client-Server, Peer To Peer, Hybrid. Network Devices: Bridge, Switch, Router, Gateway, Access Point. Line Coding Schemes: Manchester and Differential Manchester Encodings, Frequency Hopping (FHSS) and Direct Sequence Spread Spectrum (DSSS).

Unit 2: Datalink Layer

Introduction, functions. Design Issues: Services to Network Layer, Framing. ARQ strategies: Error Detection and correction, Parity Bits, Hamming Codes (11/12-bits) and CRC. Flow Control Protocols: Unrestricted Simplex, Stop and Wait, Sliding Window Protocol. WAN Connectivity: PPP and HDLC. MAC Sub layer: Multiple Access Protocols: Pure and Slotted ALOHA, CSMA, WDMA, CSMA/CD, CSMA/CA, Binary Exponential Back-off algorithm, Introduction to Ethernet IEEE 802.3, IEEE 802.11 a/b/g/n, IEEE 802.15 and IEEE 802.16 Standards.

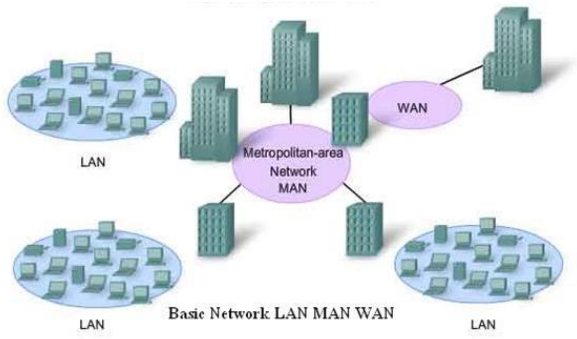
QUESTIONS:

[1] Explain LAN, MAN, WAN. [6]

LAN (Local Area Network), MAN (Metropolitan Area Network), and WAN (Wide Area Network) are three types of networks classified based on their geographic scope and the area they cover.

1. **LAN (Local Area Network):**
    - A LAN covers a small geographical area, typically within a single building or a campus.
    - It connects computers and devices within this limited area, enabling high-speed data transfer.
    - Common in homes, offices, schools, and small businesses.
    - Example: The network in a home that connects all the devices (like computers, printers, and smartphones) to the internet.
2. **MAN (Metropolitan Area Network):**
    - A MAN covers a larger geographical area than a LAN, usually a city or a large campus.
    - It connects multiple LANs within a specific metropolitan area, providing efficient data communication.
    - It is typically owned by a single organization or a group of organizations.
    - Example: A network that connects various branches of a company within a city.
3. **WAN (Wide Area Network):**
    - A WAN covers a vast geographical area, potentially connecting networks across cities, countries, or even continents.
    - It connects multiple LANs and MANs, facilitating communication over long distances.
    - The internet is the most prominent example of a WAN.
    - Example: A global corporation's network that connects its offices in different countries.

Each type of network is designed to serve different scales and purposes, with LAN being the smallest and WAN being the largest.



Basic Network LAN MAN WAN

[2] What are design issues of layers? Explain it. [5]

The design issues of layers in a network model, such as the OSI (Open Systems Interconnection) or TCP/IP models, refer to the challenges and considerations involved in designing and implementing the layers that make up these models. Each layer in a network model has specific functions and responsibilities, and the design issues typically revolve around ensuring that these functions are carried out efficiently and effectively. Here are the main design issues for network layers:

1. Service Definition

- **Issue**: Each layer must clearly define the services it provides to the layer above it. This involves specifying what functions the layer performs without dictating how they should be implemented.
- **Consideration**: The service definition should be broad enough to accommodate different technologies and implementations but precise enough to ensure compatibility and interoperability.

2. Interface Design

- **Issue**: The interfaces between adjacent layers must be well-defined to allow smooth communication. This includes specifying how data is passed between layers and how layers interact with each other.
- **Consideration**: Interfaces should be simple, consistent, and efficient, minimizing the overhead of communication between layers while ensuring that layers are decoupled (i.e., changes in one layer do not affect others).

3. Layer Functionality

- **Issue**: Each layer should be assigned a specific set of functions to avoid redundancy and overlap. The functions should be distinct and non-overlapping to maintain the modularity of the network design.
- **Consideration**: The division of functions among layers should be logical, ensuring that each layer performs a well-defined role within the overall network architecture.

4. Protocol Design

- **Issue**: Each layer must use protocols to carry out its functions. Protocols define the rules and conventions for communication between entities in the same layer across different network nodes.
- **Consideration**: Protocols should be efficient, robust, and flexible, capable of handling errors, supporting various communication needs, and adapting to different network conditions.

5. Addressing and Naming

- **Issue**: Each layer needs a mechanism for identifying and addressing entities, such as devices, processes, or sessions. Addressing ensures that data is delivered to the correct destination.
- **Consideration**: The addressing scheme should be scalable, unique, and consistent across the network. It should also support routing and forwarding decisions efficiently.

6. Error Handling

- **Issue**: Errors can occur during data transmission, and each layer must have mechanisms for detecting, reporting, and correcting these errors.
- **Consideration**: The error-handling approach should be effective in maintaining data integrity and reliability while minimizing the performance impact on the network.

7. Flow Control and Congestion Control

- **Issue**: Layers responsible for data transmission must manage the flow of data to prevent overwhelming the network or the receiving device.
- **Consideration**: Flow control mechanisms should ensure that the sender does not overwhelm the receiver, while congestion control mechanisms should prevent the network from becoming overloaded.

8. Security

- **Issue**: Each layer must address security concerns, such as confidentiality, integrity, and authentication.
- **Consideration**: Security measures should be integrated into the design of each layer, ensuring that data is protected from unauthorized access and tampering.

9. Data Representation

- **Issue**: Different systems may represent data differently. Layers must handle data format conversion and translation to ensure compatibility across diverse systems.
- **Consideration**: Data representation should be standardized within the layer to facilitate interoperability while allowing for necessary conversions to support different end systems.

10. Implementation Independence

- **Issue**: The design of each layer should allow for independent implementation. Different layers can be implemented using various technologies and strategies as long as they adhere to the defined interfaces and protocols.
- **Consideration**: Ensuring implementation independence promotes flexibility, allowing network technologies to evolve without requiring a redesign of the entire model.

By addressing these design issues, network architects can create robust, flexible, and efficient networking models that support a wide range of communication needs and technologies.

[3] Explain [4] i) Router ii) Switch

i) Router

- **Function**: A router is a networking device that forwards data packets between different networks. It acts as a gateway between networks, directing data from one network to another based on the destination IP address in the packet. Routers are crucial for connecting different networks, such as a local area network (LAN) to the internet.
- **How it Works**: Routers analyze the destination IP address of each packet, consult a routing table (a list of paths to various network destinations), and determine the best path to forward the packet. They can also perform network address translation (NAT), which allows multiple devices on a LAN to share a single public IP address.

- **Use Case**: Routers are used in homes, offices, and data centers to connect local networks to the internet or to link multiple networks together within an organization.

ii) Switch

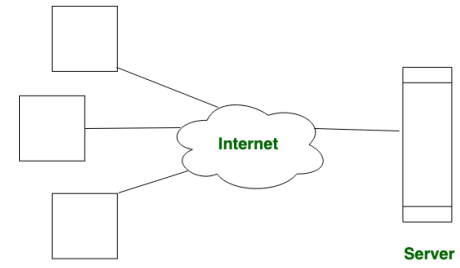
- **Function**: A switch is a networking device that operates at the data link layer (Layer 2) of the OSI model. It connects devices within the same network (usually a LAN) and uses MAC addresses to forward data only to the specific device that needs it, rather than broadcasting to all devices on the network.
- **How it Works**: Switches receive incoming data packets, read the MAC address of the destination device, and send the packet directly to that device. Unlike hubs, which simply broadcast data to all devices, switches efficiently manage traffic within a network by reducing unnecessary data transmission.
- **Use Case**: Switches are commonly used in network environments such as office buildings, data centers, and homes to connect multiple devices (like computers, printers, and servers) within the same network, enhancing performance and security

[4] Explain Client Server and Peer to Peer Network. [6]

In the world of network architecture, two fundamental models are widely utilized to structure data exchange and resource sharing. For the purpose of this discussion, two types of networks are available; the **Client-Server Network** and the Pe**er-to-Peer Network**. All the models have their strengths, weaknesses, and appropriate applications that make them suitable for use. An understanding of these differences will assist in choosing suitable approaches for different networking requirements.

What is a Client-Server Network?

This model are broadly used network model. In the Client-Server Network, Clients and servers are differentiated, and Specific servers and clients are present. In Client-Server Network, a Centralized server is used to store the data because its management is centralized. In Client-Server Network, the Server responds to the services which is requested by the Client.



Client-Server Network Model

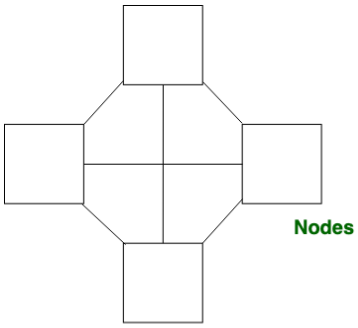
What is Peer-to-Peer Network?

This model does not differentiate the clients and the servers, In this each and every node is itself client and server. In Peer-to-Peer Network, Each and every node can do both request and respond for the services.

- Peer-to-peer networks are often created by collections of 12 or fewer machines. All of these computers use unique security to keep their data, but they also share data with every other node.
- In peer-to-peer networks, the nodes both consume and produce resources. Therefore, as the number of nodes grows, so does the peer-to-peer network's capability for resource sharing. This is distinct from client-server networks where an increase in nodes causes the server to become overloaded.

CNS Question bank answers

- It is challenging to give nodes in peer-to-peer networks proper security because they function as both clients and servers. A denial of service attack may result from this.
- The majority of contemporary operating systems, including Windows and Mac OS, come with software to implement peer



Peer-to-Peer Network Model

Difference Between Client-Server and Peer-to-Peer Network

Client-Server Network	Peer-to-Peer Network
In Client-Server Network, Clients and server are differentiated, Specific server and clients are present.	In Peer-to-Peer Network, Clients and server are not differentiated.
Client-Server Network focuses on information sharing.	While Peer-to-Peer Network focuses on connectivity.
In Client-Server Network, Centralized server is used to store the data.	While in Peer-to-Peer Network, Each peer has its own data.
In Client-Server Network, Server respond the services which is request by Client.	While in Peer-to-Peer Network, Each and every node can do both request and respond for the services.
Client-Server Network are costlier than Peer-to-Peer Network.	While Peer-to-Peer Network are less costlier than Client-Server Network.
Client-Server Network are more stable than Peer-to-Peer Network.	While Peer-to-Peer Network are less stable if number of peer is increase.
Client-Server Network is used for both small and large networks.	While Peer-to-Peer Network is generally suited for small networks with fewer than 10 computers.

CNS Question bank answers

[5] Draw Manchester and differential Manchester code for the bit sequence: 0100110 [5]

Manchester and Differential Manchester encoding are methods used to encode digital data into a binary signal. Here's how to encode the bit sequence 0100110 in both Manchester and Differential Manchester code:

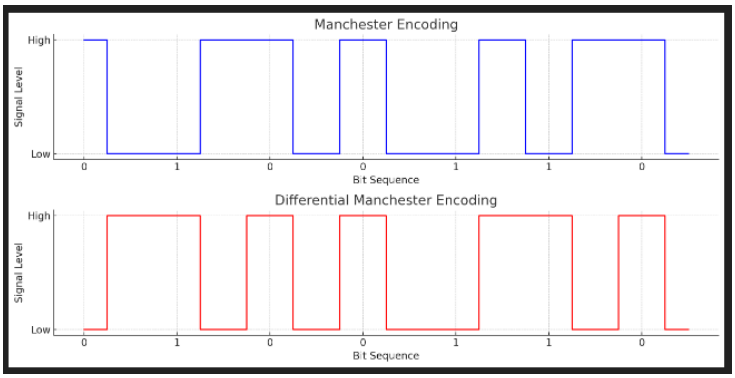
1. Manchester Encoding:

- In Manchester encoding, each bit is represented by two levels:
    - A 0 is represented by a high-to-low transition.
    - A 1 is represented by a low-to-high transition.

2. Differential Manchester Encoding:

- In Differential Manchester encoding, the presence of a transition at the beginning of the bit period represents a 0, and the absence of a transition at the beginning of the bit period represents a 1. Additionally, there is always a transition in the middle of the bit period.

I'll now draw the corresponding waveforms for both encodings.



Here are the Manchester and Differential Manchester encoded waveforms for the bit sequence 0100110:

- **Manchester Encoding**: Each 0 is represented by a high-to-low transition, and each 1 is represented by a low-to-high transition.
- **Differential Manchester Encoding**: A transition at the beginning of the bit period indicates a 0, while no transition at the beginning indicates a 1. There is always a transition in the middle of the bit period.

Manchester Encoding	Differential Manchester Encoding
Manchester encoding s a synchronous clock-encoding technique used by the physical layer to encode the clock and data of a synchronous bit stream.	Differential Manchester encoding is a line code in which data and clock signals are combined to form a single 2-level self-synchronizing data stream
Low to High represents 1 and High to Low represents 0.	No transition at the start of a bit period represents 1 and transition at the start of a bit period represents 0.
It provides better signal synchronization.	It provides less signal synchronization as compared to manchester encoding.

Manchester Encoding	Differential Manchester Encoding
Signal rate is the drawback of manchester encoding as there is always one transition at the middle of the bit and maybe one transition at the end of each bit.	It maps at least one transition per bit time and possibly two bits. Its modulation or signal rate is two times that of NRZ. Hence it requires more bandwidth.
Used by IEEE 802.3 specification for Ethernet LAN	Used by IEEE 802.5 specification for Token Ring LAN

[6] Explain Star and Bus topologies. [4]

Star and Bus topologies are two fundamental types of network topologies that define how devices (or nodes) are interconnected in a network. Each has its own structure, advantages, and disadvantages.

1. Star Topology

Structure:

- In a star topology, all devices (nodes) are connected to a central device called a **hub, switch, or router**.
- The central device acts as a mediator, managing and directing all the communication between the nodes.
- Each node has a direct point-to-point connection to the central device, but there are no direct connections between the nodes themselves.

How it Works:

- When a device wants to communicate with another device on the network, it sends data to the central hub, which then forwards the data to the destination device.
- The central hub can also manage the data traffic, ensuring that data is efficiently routed between devices.

Advantages:

- **Easy to Manage:** Centralized control makes it easy to manage and monitor the network.
- **Scalability:** Easy to add or remove devices without disrupting the network.
- **Fault Isolation:** If one connection fails, it doesn't affect the entire network, as only the connection to the central device is impacted.

Disadvantages:

- **Single Point of Failure:** If the central hub fails, the entire network goes down.
- **Higher Cost:** Requires more cable and infrastructure (the hub or switch) compared to some other topologies.
- **Traffic Congestion:** The central hub can become a bottleneck if it cannot handle high data traffic.

Use Cases:

- Commonly used in home networks, offices, and organizations where centralized control and easy management are important.

2. Bus Topology

Structure:

- In a bus topology, all devices (nodes) are connected to a single central cable, known as the **bus** or **backbone**.
- The bus acts as a shared communication medium, and all nodes are connected to it via drop lines.
- Data sent by any device is broadcasted to all devices on the network, but only the intended recipient accepts and processes it.

How it Works:

- When a device sends data, it travels along the bus until it reaches its destination.

- Devices are typically connected via a connector and the bus ends with terminators to prevent the signal from reflecting back.

Advantages:

- **Cost-Effective:** Requires less cabling compared to other topologies, making it cheaper to set up.
- **Simple Layout:** Easy to implement and extend.
- **Efficient for Small Networks:** Works well for small networks with limited data traffic.

Disadvantages:

- **Difficult to Troubleshoot:** Identifying faults can be difficult, as any break in the bus affects the entire network.
- **Limited Length and Speed:** The length of the bus is limited, and as more devices are added, network performance can degrade.
- **Data Collisions:** Multiple devices sharing the same bus can lead to data collisions, which can slow down the network.

Use Cases:

- Historically used in small, simple networks, such as early local area networks (LANs) and small office setups. It's less common in modern networks due to its limitations.

Comparison:

- **Star Topology**:
  - Centralized control and easy fault isolation.
  - More robust and scalable.
  - More expensive and has a single point of failure.
- **Bus Topology**:
  - Simple, cost-effective setup.
  - Less scalable and more prone to network disruptions.
  - Efficient for small networks but less suitable for larger ones.

Understanding these topologies helps in designing networks that are efficient, reliable, and suited to specific needs.

[7] Give brief about design issues in DLL. [6]

The Data Link Layer (DLL) in the OSI model is responsible for ensuring reliable data transfer between two directly connected nodes over a physical medium. The design issues in the Data Link Layer are crucial for maintaining data integrity, managing error detection, and controlling data flow. Here are the key design issues:

1. Framing

- **Issue**: Data from the network layer is transmitted as a continuous stream of bits. The Data Link Layer must organize this data into manageable units called frames.
- **Consideration**: Framing involves creating boundaries for these frames so that the receiver can recognize the start and end of each frame. Techniques like character stuffing, bit stuffing, and using special delimiter characters are used to achieve framing.

2. Error Control

- **Issue**: During transmission, data can become corrupted due to noise, interference, or other issues in the physical layer.
- **Consideration**: The Data Link Layer must implement error detection and correction mechanisms to ensure data integrity. Techniques like checksums, cyclic redundancy checks (CRC), and error-correcting codes (e.g., Hamming code) are employed to detect and correct errors.

3. Flow Control

- **Issue**: If the sender transmits data faster than the receiver can process it, the receiver's buffer may overflow, leading to data loss.

- **Consideration**: Flow control mechanisms ensure that the sender does not overwhelm the receiver by adjusting the transmission rate. Protocols like Stop-and-Wait, Sliding Window, and flow control flags are used to manage this process.

4. Error Detection and Retransmission

- **Issue**: Despite error control mechanisms, some frames may still arrive corrupted or may be lost during transmission.
- **Consideration**: The Data Link Layer needs to detect such errors and, if necessary, request retransmission of the affected frames. Automatic Repeat reQuest (ARQ) protocols, such as Stop-and-Wait ARQ, Go-Back-N ARQ, and Selective Repeat ARQ, are used for this purpose.

5. Medium Access Control (MAC)

- **Issue**: In shared communication mediums, multiple devices may try to send data simultaneously, leading to collisions and network congestion.
- **Consideration**: The MAC sublayer of the Data Link Layer handles the problem of determining which device has the right to use the communication channel at any given time. Techniques like Carrier Sense Multiple Access (CSMA), Token Passing, and Time-Division Multiple Access (TDMA) are employed for efficient medium access.

6. Addressing

- **Issue**: Data needs to be sent to the correct destination device on a network, especially in networks with multiple devices.
- **Consideration**: The Data Link Layer assigns unique addresses, known as MAC addresses, to each device on the network. These addresses are used to ensure that frames are delivered to the correct destination.

Summary:

The design issues in the Data Link Layer are centered around ensuring reliable communication between two directly connected devices. Framing, error control, flow control, error detection and retransmission, medium access control, and addressing are critical aspects that must be carefully designed to maintain data integrity, manage network traffic, and ensure efficient communication in a network.

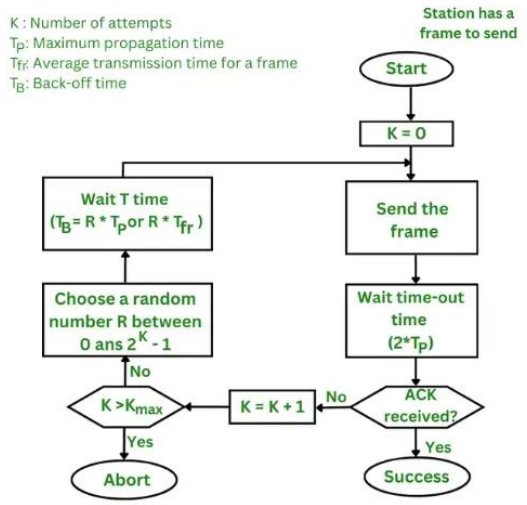
[8] Differentiate between Pure and Slotted ALOHA [5]

Aloha is a type of Random access protocol it was developed at the University of Hawaii in early 1970, it is a LAN-based protocol this type there are more chances of occurrence of collisions during the transmission of data from any source to the destination, Aloha has two types one Pure Aloha and another Slotted Aloha.

Pure Aloha

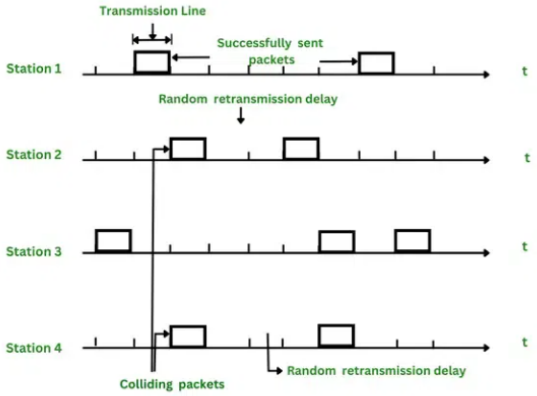
Pure Aloha can be termed as the main Aloha or the original Aloha. Whenever any frame is available, each station sends it, and due to the presence of only one channel for communication, it can lead to the chance of collision.

In the case of the pure aloha, the user transmits the frame and waits till the receiver acknowledges it, if the receiver does not send the acknowledgment, the sender will assume that it has not been received and sender resends the acknowledgment.



Slotted Aloha

Slotted Aloha is simply an advanced version of pure Aloha that helps in improving the communication network. A station is required to wait for the beginning of the next slot to transmit. The vulnerable period is halved as opposed to Pure Aloha.



Slotted Aloha helps in reducing the number of collisions by properly utilizing the channel and this basically results in the somehow delay of the users. In Slotted Aloha, the channel time is separated into particular time slots.

Differences Between Pure Aloha and Slotted Aloha

Pure Aloha	Slotted Aloha
In this Aloha, any station can transmit the data at any time.	In this, any station can transmit the data at the beginning of any time slot.
In this, The time is continuous and not globally synchronized.	In this, The time is discrete and globally synchronized.
Vulnerable time for Pure Aloha = 2 x Tt	Vulnerable time for Slotted Aloha = Tt
In Pure Aloha, the Probability of successful transmission of the data packet **= G x e^{-2G}**	In Slotted Aloha, the Probability of successful transmission of the data packet = G x e^{-G}
In Pure Aloha, Maximum efficiency **= 18.4%**	In Slotted Aloha, Maximum efficiency = 36.8%
Pure Aloha doesn't reduce the number of collisions to half.	Slotted Aloha reduces the number of collisions to half and doubles the efficiency of Pure Aloha.

[9] Explain PPP. [4]

Point-to-Point Protocol (PPP) is a data link layer protocol used to establish a direct connection between two networking nodes. It provides a standard method for transporting multi-protocol datagrams over point-to-point links, such as between a computer and an Internet Service Provider (ISP). PPP is widely used for internet access over dial-up, DSL, and other point-to-point connections.

Key Features of PPP:

1. **Encapsulation**:
    - PPP encapsulates network layer protocol information (e.g., IP packets) within PPP frames, which are then transmitted over the physical link.
    - The basic PPP frame format includes fields like a flag, address, control, protocol, payload (data), and frame check sequence (FCS).
2. **Link Control Protocol (LCP)**:

- LCP is responsible for establishing, configuring, testing, and maintaining the PPP link.
- It negotiates options such as maximum frame size, authentication method, and whether to use compression.

3. **Authentication**:
   - PPP supports authentication mechanisms to verify the identity of the connecting devices.
   - The two most common methods are Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).
   - PAP sends the username and password in plain text, whereas CHAP uses a more secure challenge-response mechanism.
4. **Network Control Protocols (NCPs)**:
   - NCPs are used to negotiate and configure different network layer protocols (e.g., IP, IPX, AppleTalk) that will be transported over the PPP link.
   - Each network layer protocol has its own associated NCP to manage the configuration of that protocol.

Advantages of PPP:

- **Multi-Protocol Support**: PPP can carry multiple types of network layer protocols, making it versatile.
- **Error Detection**: PPP includes mechanisms for detecting errors in the transmitted frames, helping to ensure data integrity.
- **Compression and Encryption**: PPP can optionally compress and encrypt data to optimize performance and security.

Use Cases:

- PPP is commonly used in **dial-up** connections, **DSL**, and **VPN** links where a direct, point-to-point connection between two devices is required.
- It is also used in **serial** connections and **point-to-point** leased lines.

Summary:

PPP is a robust and versatile protocol for establishing and maintaining point-to-point links, providing essential services like encapsulation, authentication, and network layer protocol configuration. Its ability to support multiple protocols and provide secure and reliable connections has made it a widely adopted standard in various networking scenarios

[10] Sender Sends code 1001101 justify receiver using Hamming code. [6]

Hamming Code Error Detection and Correction

Hamming code is a technique used to detect and correct single-bit errors in transmitted data. It works by adding parity bits at specific positions in the data to form a codeword. The receiver can then use these parity bits to check for and correct errors.

Problem Statement: The sender transmits the code 1001101, and the receiver needs to use Hamming code to justify (verify) if the received data is correct or if there are any errors.

Step-by-Step Solution

1. **Determine the Number of Parity Bits Needed**:

CNS Question bank answers

- Let the number of data bits be d (which is 7 in this case: 1001101).
- Let the number of parity bits be p.
- The total number of bits in the codeword will be n = d + p.
- Parity bits are placed at positions that are powers of 2: 1, 2, 4, 8, etc.

To determine the number of parity bits, we need the smallest p such that:

2p≥d+p+12^p \geq d + p + 12p≥d+p+1

For d = 7:

- If p = 3, then 23=82^3 = 823=8 which is less than 7 + 3 + 1 = 11.
- If p = 4, then 24=162^4 = 1624=16 which is greater than 7 + 4 + 1 = 12.

So, we need 4 parity bits.

2. **Determine Positions of Data and Parity Bits**:
   - The codeword will have 11 bits (7 + 4).
   - Place the data bits at positions that are not powers of 2:
     - Data positions: 3, 5, 6, 7, 9, 10, 11
   - Place the parity bits at positions that are powers of 2:
     - Parity positions: 1, 2, 4, 8

Place the data bits (1001101) into the appropriate positions:

less
Copy code
Position: 1 2 3 4 5 6 7 8 9 10 11
Bits: P1 P2 1 P4 0 1 1 P8 0 1 1

3. **Calculate the Parity Bits**:
   - **P1** checks positions: 1, 3, 5, 7, 9, 11 P1=1⊕1⊕0⊕1⊕0⊕1=0P1 = 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 = 0P1=1⊕1⊕0⊕1⊕0⊕1=0
   - **P2** checks positions: 2, 3, 6, 7, 10, 11 P2=0⊕1⊕1⊕1⊕1⊕1=0P2 = 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 = 0P2=0⊕1⊕1⊕1⊕1⊕1=0
   - **P4** checks positions: 4, 5, 6, 7 P4=0⊕0⊕1⊕1=0P4 = 0 \oplus 0 \oplus 1 \oplus 1 = 0P4=0⊕0⊕1⊕1=0
   - **P8** checks positions: 8, 9, 10, 11 P8=0⊕0⊕1⊕1=0P8 = 0 \oplus 0 \oplus 1 \oplus 1 = 0P8=0⊕0⊕1⊕1=0

So, the codeword the sender transmits should be:

Copy code
01100110101

4. **Receiver's Task**:
   - The receiver checks the parity bits using the same positions:
   - If all parity checks are correct (i.e., no error is detected), the data is accepted.
   - If a parity check fails, the receiver calculates the error position and corrects it.

Conclusion

- The sender's code 1001101 is transmitted with parity bits as 01100110101.

- The receiver uses the parity bits to check for errors. If the parity checks pass, the data is correct. If they fail, the receiver identifies and corrects the erroneous bit.

This process ensures that single-bit errors can be detected and corrected by the receiver, providing reliable data communication.

[11] Explain IEEE 802.3 frame format. [5]

The IEEE 802.3 standard, commonly known as Ethernet, defines the frame format used for data transmission in wired local area networks (LANs). The Ethernet frame structure is crucial for ensuring that data is correctly formatted and transmitted over the network.

IEEE 802.3 Frame Format

The IEEE 802.3 frame format is composed of several fields, each serving a specific function in the data transmission process. Here is a breakdown of the frame format:

1. **Preamble (7 bytes or 56 bits):**
    - **Purpose**: The preamble is used to synchronize the receiver's clock with the sender's clock. It consists of a pattern of alternating 1s and 0s (e.g., 10101010...).
    - **Details**: This ensures that the receiver is ready to process the incoming frame by the time the actual data begins.
2. **Start Frame Delimiter (SFD) (1 byte or 8 bits):**
    - **Purpose**: The Start Frame Delimiter marks the end of the preamble and indicates the start of the actual frame. It is a specific pattern 10101011.
    - **Details**: The SFD helps the receiver identify the beginning of the frame's data.
3. **Destination MAC Address (6 bytes or 48 bits):**
    - **Purpose**: This field contains the MAC address of the destination device (the device that the frame is intended for).
    - **Details**: The MAC address is a unique identifier for network devices, ensuring that the frame reaches the correct recipient.
4. **Source MAC Address (6 bytes or 48 bits):**
    - **Purpose**: This field contains the MAC address of the source device (the device that sent the frame).
    - **Details**: It allows the recipient to know where the frame originated.
5. **Length/Type (2 bytes or 16 bits):**
    - **Purpose**: This field can serve two purposes:
        - **Length**: If the value is less than or equal to 1500, it indicates the length of the data field in bytes.
        - **Type**: If the value is greater than 1500, it indicates the protocol type being carried in the payload (e.g., IPv4, ARP).
    - **Details**: This field helps in identifying the size of the data or the type of protocol used.
6. **Data and Padding (46-1500 bytes or 368-12000 bits):**

- **Purpose**: This field contains the actual data being transmitted. If the data is less than 46 bytes, padding is added to meet the minimum frame size requirement of 64 bytes.
- **Details**: The padding ensures that the frame is large enough for proper network operation.

7. **Frame Check Sequence (FCS) (4 bytes or 32 bits):**
   - **Purpose**: The FCS is used for error detection. It contains a cyclic redundancy check (CRC) value calculated based on the contents of the frame.
   - **Details**: The receiver recalculates the CRC and compares it to the FCS value to check for errors during transmission.

Summary of the IEEE 802.3 Frame Format:

Field Name	Size	Purpose
Preamble	7 bytes (56 bits)	Synchronizes the clocks of sender and receiver.
Start Frame Delimiter	1 byte (8 bits)	Marks the start of the actual frame.
Destination MAC Address	6 bytes (48 bits)	Specifies the receiver's MAC address.
Source MAC Address	6 bytes (48 bits)	Specifies the sender's MAC address.
Length/Type	2 bytes (16 bits)	Indicates the data length or protocol type.
Data and Padding	46-1500 bytes	Contains the actual data and padding if necessary.
Frame Check Sequence	4 bytes (32 bits)	Provides error detection using CRC.

This structured format ensures that Ethernet frames are transmitted reliably over a network, with clear identification of the source and destination, as well as mechanisms for error detection and data integrity

[12] Explain Stop and Wait Protocol. [4]

The **Stop-and-Wait Protocol** is a simple flow control method used in data communication to ensure that data is transmitted reliably between two devices. It is commonly used at the Data Link Layer and sometimes at the Transport Layer.

How the Stop-and-Wait Protocol Works:

1. **Data Transmission:**
   - The sender transmits one frame or packet of data at a time.
   - After sending the frame, the sender stops and waits for an acknowledgment (ACK) from the receiver before sending the next frame.
2. **Acknowledgment (ACK):**
   - The receiver receives the frame, checks it for errors, and sends an acknowledgment (ACK) back to the sender if the frame is received correctly.
   - If the frame is corrupted, the receiver discards it and does not send an acknowledgment.
3. **Timeout and Retransmission:**
   - The sender starts a timer after sending each frame.

- If the sender does not receive an acknowledgment within the timeout period, it assumes that the frame was lost or corrupted and retransmits the same frame.

4. **Sequential Process:**
    - This process repeats for each frame, with the sender only sending a new frame after receiving an acknowledgment for the previous one.

Advantages of Stop-and-Wait Protocol:

- **Simplicity:** The protocol is easy to understand and implement, making it suitable for simple communication systems.
- **Error Control:** It ensures that data is transmitted accurately by requiring the sender to wait for confirmation before proceeding.

Disadvantages of Stop-and-Wait Protocol:

- **Inefficiency:** The protocol is inefficient for high-speed networks because the sender must wait for an acknowledgment after each frame, leading to idle time and underutilization of the network.
- **Low Throughput:** The waiting period between frames can significantly reduce the overall throughput, especially if the round-trip time (RTT) between sender and receiver is high.

Summary:

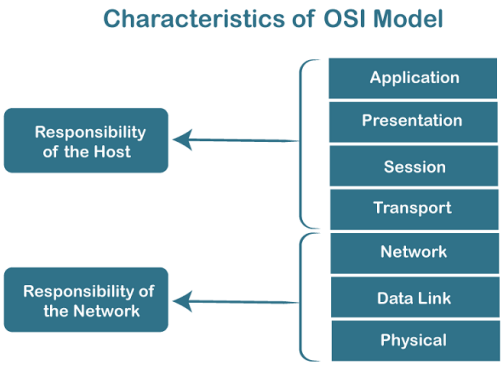
The Stop-and-Wait Protocol is a basic method of ensuring reliable data transmission, where the sender waits for an acknowledgment before sending the next frame. While it provides error control, its simplicity leads to inefficiency, making it less suitable for high-speed or long-distance communications.

[13] Draw and explain OSI Model. [6]

OSI Model

- OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.

Characteristics of OSI Model:

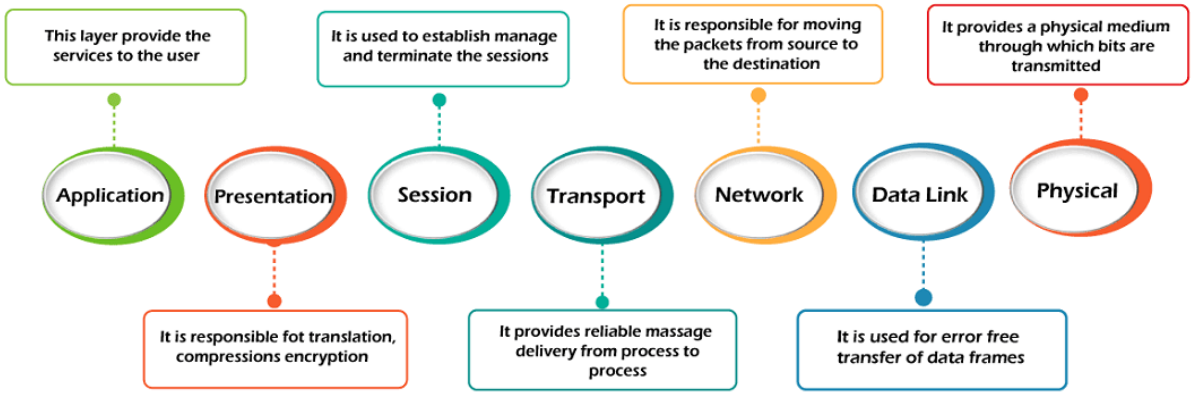


- The OSI model is divided into two layers: upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

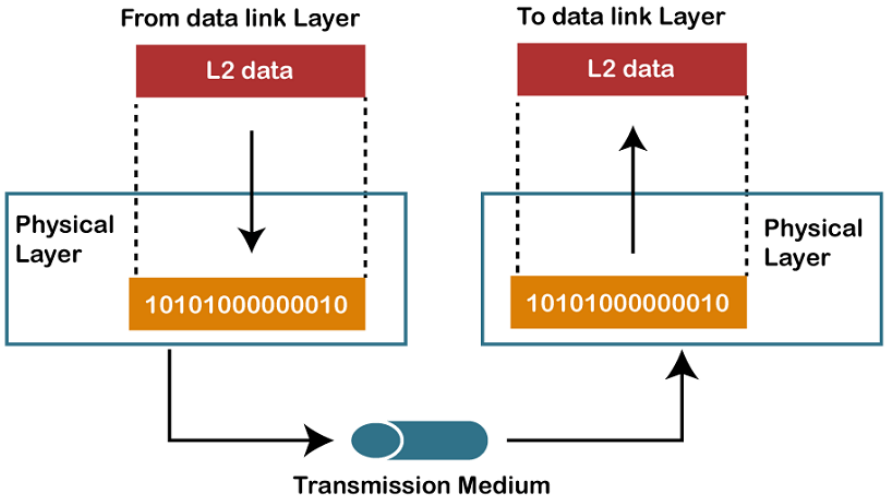
7 Layers of OSI Model

There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

1. Physical Layer
2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer



1) Physical layer

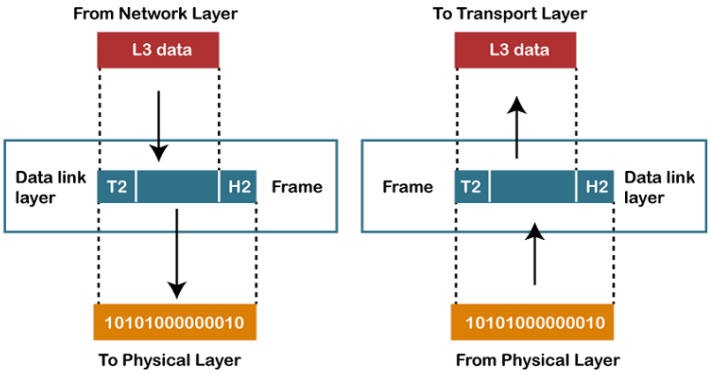


- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

- **Line Configuration:** It defines the way how two or more devices can be connected physically.
- **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- **Topology:** It defines the way how network devices are arranged.
- **Signals:** It determines the type of the signal used for transmitting the information.

2) Data-Link Layer



- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub-layers:
    - **Logical Link Control Layer**

- It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
- It identifies the address of the network layer protocol from the header.
- It also provides flow control.

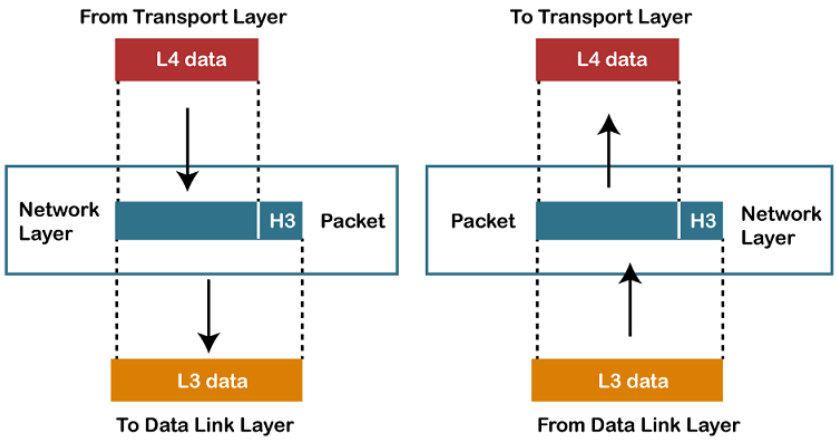
- **Media Access Control Layer**
  - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
  - It is used for transferring the packets over the network.

Functions of the Data-link layer

- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

- **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

3) Network Layer



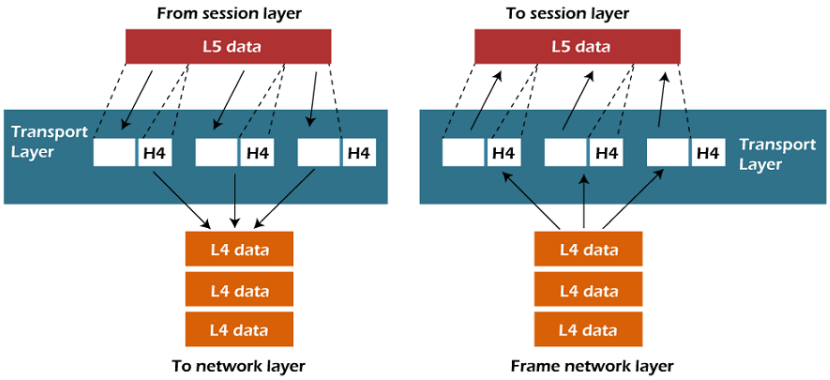
CNS Question bank answers

- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

- **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

4) Transport Layer



- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

- **Transmission Control Protocol**
  - It is a standard protocol that allows the systems to communicate over the internet.
  - It establishes and maintains a connection between hosts.

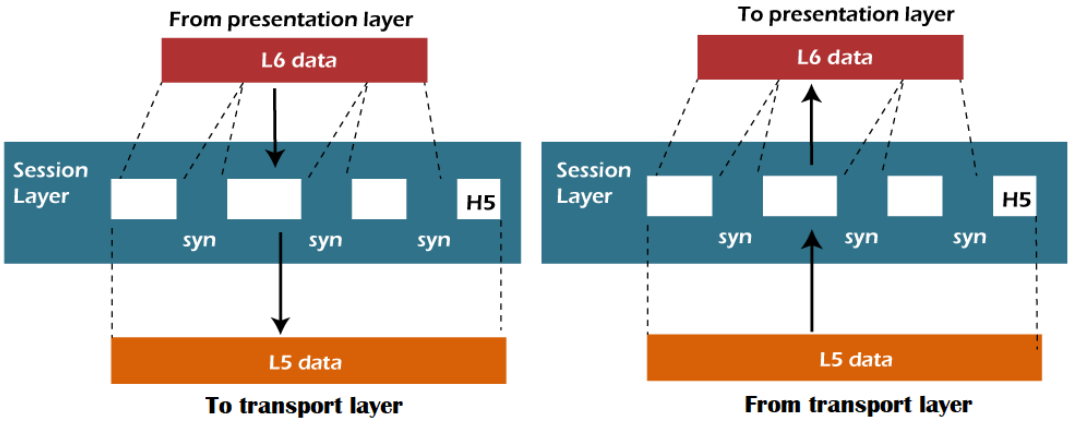
- When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.

- **User Datagram Protocol**
  - User Datagram Protocol is a transport layer protocol.
  - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Functions of Transport Layer:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

5) Session Layer



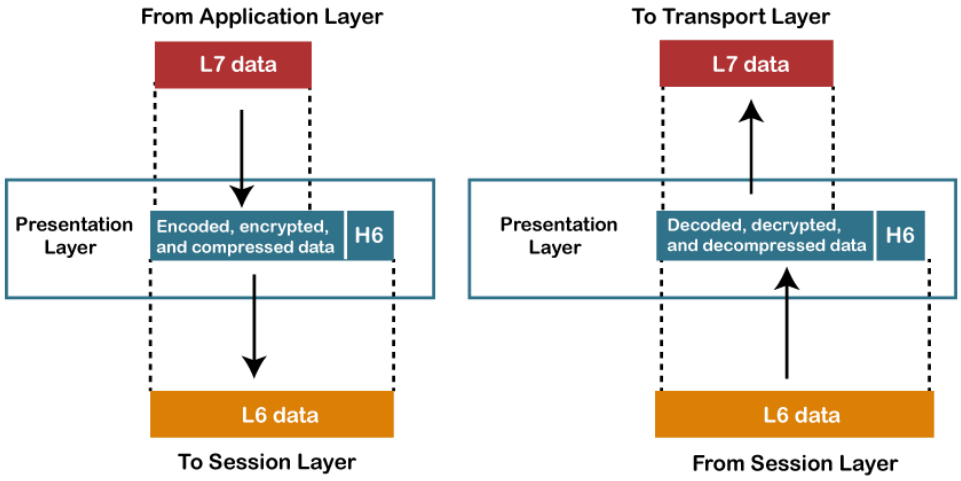
- It is a layer 3 in the OSI model.

- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

- **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

6) Presentation Layer

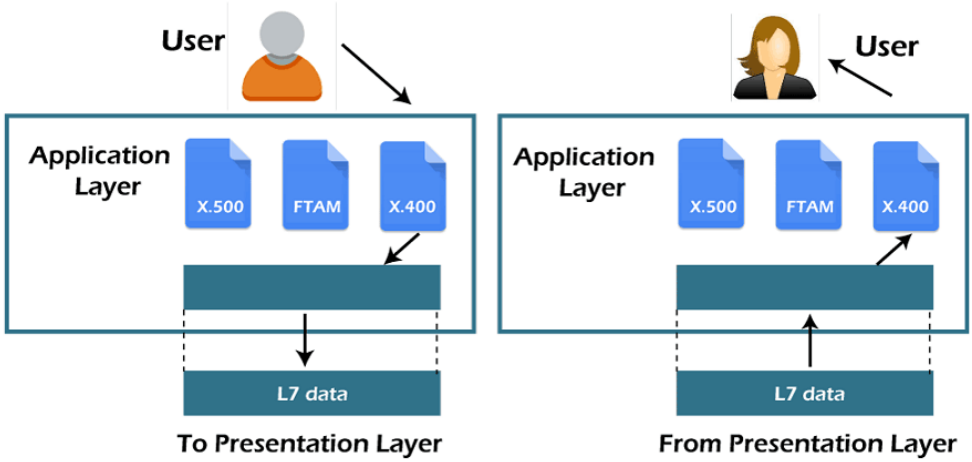


- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
- **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

7) Application Layer



- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.

Functions of Application layer:

- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.
- Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

[14] Explain Direct Sequence Spread Spectrum. [5]

Direct Sequence Spread Spectrum (DSSS) is a method used in wireless communication to spread the data signal over a wider frequency band than the minimum bandwidth necessary to transmit the data. Here's a breakdown:

1. **Spread Spectrum Technique**: DSSS is a type of spread spectrum technique, which means it spreads the signal over a wide frequency range. This helps in improving the signal's resistance to interference and eavesdropping.
2. **Chipping Sequence**: In DSSS, the data signal is multiplied by a pseudo-random noise (PN) sequence, also known as the chipping sequence. This PN sequence has a much higher frequency than the data signal, which spreads the data across a broader frequency range.
3. **Modulation**: The data signal is modulated using this chipping sequence. This modulation process effectively spreads the signal over a wider bandwidth. The chipping sequence is usually a binary sequence that changes at a much higher rate than the data bits.
4. **Receiver Side**: At the receiver, the signal is demodulated by correlating it with the same PN sequence used for spreading. This process reconstructs the original data signal from the spread spectrum signal.
5. **Advantages**: DSSS provides several advantages, including resistance to interference, better security, and improved performance in noisy environments. The spreading of the signal helps in minimizing the impact of narrowband interference and makes the signal harder to intercept and jam.

In summary, DSSS spreads the signal over a larger bandwidth by multiplying the data with a high-frequency PN sequence, enhancing signal robustness and security.

[15] Explain i) Router ii) Switch. [4] REFER Q3.

[16] Explain TCP/IP Model. [6]

The TCP/IP model is a conceptual framework used to understand and design network communications, specifically for the internet. It consists of four layers, each responsible for different aspects of communication:

1. **Network Interface Layer (Link Layer)**:
    - **Function**: Handles the physical and data link aspects of communication. It manages the hardware interface and protocols needed for the transmission of data over a specific network medium (e.g., Ethernet, Wi-Fi).
    - **Protocols**: Ethernet, Wi-Fi, ARP (Address Resolution Protocol).
2. **Internet Layer**:
    - **Function**: Responsible for addressing, routing, and forwarding data packets across different networks. It ensures that packets are delivered from the source to the destination, potentially across multiple networks.
    - **Protocols**: IP (Internet Protocol) is the primary protocol at this layer. It includes IPv4 and IPv6. Other protocols include ICMP (Internet Control Message Protocol) and IGMP (Internet Group Management Protocol).
3. **Transport Layer**:
    - **Function**: Manages end-to-end communication and error recovery. It ensures that data is transmitted accurately and reliably between hosts.
    - **Protocols**: TCP (Transmission Control Protocol) provides reliable, connection-oriented communication, while UDP (User Datagram Protocol) offers connectionless communication with less overhead.
4. **Application Layer**:
    - **Function**: Provides network services directly to end-user applications. It handles high-level protocols and services that interact with software applications.
    - **Protocols**: Includes a wide range of protocols such as HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), and DNS (Domain Name System).

Key Concepts:

- **Encapsulation**: Each layer adds its own header (and sometimes trailer) to the data, creating a packet with multiple layers of information. For example, data from the application layer is encapsulated in a transport layer segment, which is then encapsulated in an internet layer packet, and finally in a network interface layer frame.
- **Decapsulation**: At the receiving end, each layer removes its respective header/trailer to extract the data and pass it to the next layer.

The TCP/IP model is foundational to the functioning of the internet and many other networking environments. It is designed to be simple, robust, and adaptable to various networking technologies and applications

[17] Draw Manchester and differential Manchester code for the bit sequence: 01001011. [5] [REFER Q5]

[18] Explain Ring and Mesh topologies. [4]

Ring Topology and **Mesh Topology** are two different network topologies used in networking and telecommunications. Here's an explanation of each:

Ring Topology:

1. **Structure**: In a ring topology, each device (or node) is connected to exactly two other devices, forming a circular or ring-like structure. Data travels in a unidirectional or bidirectional manner around the ring.
2. **Data Transmission**: Data is transmitted in one direction (unidirectional) or both directions (bidirectional) around the ring until it reaches the intended recipient. In a unidirectional ring, data passes through each node in a single direction, whereas, in a bidirectional ring, data can travel in either direction.
3. **Advantages**:
    - **Predictable Data Transmission**: Because data travels in a defined path, there is minimal chance of data collisions.
    - **Simple Setup**: Easy to set up and configure.
4. **Disadvantages**:
    - **Failure Impact**: If one node or connection fails, it can disrupt the entire network unless there is a redundant path (in bidirectional rings).
    - **Maintenance**: Adding or removing devices requires the network to be temporarily disconnected.

Mesh Topology:

1. **Structure**: In a mesh topology, each device is connected to every other device in the network. This can be done in a full mesh, where every node is directly connected to all other nodes, or in a partial mesh, where only some nodes are interconnected.
2. **Data Transmission**: Data can take multiple paths to reach its destination, providing redundancy and fault tolerance. If one connection fails, data can be rerouted through alternative paths.
3. **Advantages**:
    - **High Fault Tolerance**: Because of multiple paths, the network is more resilient to failures and can continue to operate even if one or more connections fail.
    - **High Performance**: Redundant connections can enhance network performance by providing multiple paths for data to travel.
4. **Disadvantages**:
    - **Complexity**: Setting up and maintaining a mesh network can be complex and expensive due to the high number of connections required.
    - **Cost**: The cost of cabling and hardware can be high, especially in a full mesh topology.

In summary, ring topology offers a simple and predictable network structure but can be vulnerable to disruptions, while mesh topology provides high redundancy and fault tolerance at the cost of increased complexity and expense

CNS Question bank answers

[19] Justify answer using CRC for divisor: 1101 dividend: 100100. [6]

Cyclic Redundancy Check (CRC) is a method used to detect errors in digital data. To perform CRC using a given divisor and dividend, you need to follow these steps:

Given:

- **Divisor (Generator Polynomial)**: 1101
- **Dividend (Data to be transmitted)**: 100100

Steps to Perform CRC:

1. **Append Zeros to Dividend**: Append n−1n-1n−1 zeros to the end of the dividend, where nnn is the length of the divisor. Here, the divisor is 1101, which has 4 bits. Therefore, append 3 zeros to the dividend.
    - Dividend with appended zeros: 100100000
2. **Binary Division**: Perform binary division of the dividend by the divisor using XOR operation.

Division Process:

- **Initial Dividend**: 100100000
- **Divisor**: 1101

3. **Align the Divisor with the Most Significant Bit**:

1001 (first 4 bits of dividend)

1101 (divisor)

4. **Perform XOR Operation**:

1001

XOR 1101

0100 (remainder after first step)

5. **Bring Down the Next Bit**:

0100 0 (bring down next bit)

6. **Align the Divisor**:

1000 (next 4 bits including the brought down bit)

1101 (divisor)

7. **Perform XOR Operation**:

1000

XOR 1101

0101 (new remainder)

8. **Bring Down the Next Bit**:

0101 0 (bring down next bit)

9. **Align the Divisor**:

1010 (next 4 bits including the brought down bit)

1101 (divisor)

10. **Perform XOR Operation**:

1010

XOR 1101

0111 (new remainder)

11. **Bring Down the Next Bit**:

0111 0 (bring down next bit)

12. **Align the Divisor**:

1110 (next 4 bits including the brought down bit)

1101 (divisor)

13. **Perform XOR Operation**:

1110

XOR 1101

0011 (new remainder)

14. **Bring Down the Next Bit**:

0011 0 (bring down next bit)

15. **Align the Divisor**:

0110 (next 4 bits including the brought down bit)

1101 (divisor)

16. **Perform XOR Operation**:

0110

XOR 1101

1011 (new remainder)

17. **Bring Down the Next Bit**:

1011 0 (bring down next bit)

18. **Align the Divisor**:

0110 (next 4 bits including the brought down bit)

1101 (divisor)

19. **Perform XOR Operation**:

0110

XOR 1101

1111 (new remainder)

20. **Bring Down the Next Bit**:

1111 0 (bring down next bit)

21. **Align the Divisor**:

1110 (next 4 bits including the brought down bit)

1101 (divisor)

22. **Perform XOR Operation**:

1110

XOR 1101

0011 (final remainder)

Final Remainder:

The final remainder after performing the binary division is 0011. This remainder is the CRC value.

Conclusion:

For the given divisor (1101) and dividend (100100), the CRC remainder is 0011. This remainder is appended to the original data for error-checking purposes.

[20] Explain IEEE 802.15 frame format. [5]

The IEEE 802.15 standard covers wireless personal area networks (WPANs), and the frame format can vary depending on the specific substandard, such as 802.15.1 (Bluetooth), 802.15.4 (used in Zigbee), etc. Here's a general explanation of the frame format for IEEE 802.15.4, which is commonly used in low-rate WPANs like Zigbee:

IEEE 802.15.4 Frame Format

1. **Frame Control**: This field contains information about the type of frame, addressing modes, and other control information. It is 2 bytes long.
    - **Frame Type**: Indicates whether the frame is a data, acknowledgment, command, or beacon frame.
    - **Frame Version**: Specifies the version of the frame format.
    - **Security Enabled**: Indicates whether security is enabled for this frame.
    - **Frame Pending**: Used in the acknowledgment frame to indicate if more frames are pending.
    - **Ack Request**: Indicates if the sender requires an acknowledgment.
    - **Intra-PAN**: Specifies if the frame is for intra-PAN communication.
2. **Sequence Number**: This is a 1-byte field used to identify the frame uniquely and to help with frame sequencing.
3. **Addressing Information**: This section can contain several addressing fields, including:

- **Source Address**: The address of the device that sent the frame. It can be 2 bytes (short address) or 8 bytes (extended address).
- **Destination Address**: The address of the intended recipient of the frame. It can also be 2 bytes or 8 bytes.
- **Addressing Mode**: Indicates the length and type of the addressing information.

4. **Frame Payload (Data)**: This is the actual data being transmitted in the frame. Its length can vary based on the application and the size of the data being transmitted.
5. **Frame Check Sequence (FCS)**: This is a 2-byte field used for error checking. It contains a Cyclic Redundancy Check (CRC) value to detect errors that may have occurred during transmission.

Frame Format Diagram

```
+-----------------+-----------------+-----------------+-----------------+-----------------+-----------------+
| Frame Control   | Sequence Number | Addressing Info | Payload         | Padding (if any) | Frame Check     |
| (2 bytes)       | (1 byte)        | (variable)      | (variable)      |                  | Sequence (2 bytes) |
+-----------------+-----------------+-----------------+-----------------+-----------------+-----------------+
```

Explanation of Key Fields:

- **Frame Control**: Determines the type and handling of the frame. It's essential for proper frame processing.
- **Sequence Number**: Ensures proper sequence of frames, especially useful for managing retransmissions and detecting lost frames.
- **Addressing Information**: Contains the source and destination addresses, which are crucial for routing and delivering the frame to the correct recipient.
- **Frame Payload**: Carries the actual data or commands being transmitted.
- **Frame Check Sequence**: Helps in detecting errors during transmission to ensure data integrity.

Each field plays a vital role in ensuring that the data is transmitted correctly and efficiently in a WPAN environment.

[21] Give brief about design issues in DLL. [4] [REFER Q7]

[22] What is sliding window protocol? How it works? [6]

The sliding window protocol is a method used in network communications to manage the flow of data between a sender and a receiver. It is designed to handle the transmission of multiple frames of data before receiving an acknowledgment for the previous ones, thereby improving the efficiency and utilization of the network. Here's an overview of how it works:

Sliding Window Protocol Overview:

1. **Concept**:
   - The sliding window protocol uses a "window" to manage the number of frames that can be sent before needing an acknowledgment. The size of this window defines how many frames can be in transit at any given time.

2. **Window Size**:
    - **Sender Window**: The number of frames that the sender is allowed to transmit without receiving an acknowledgment.
    - **Receiver Window**: The number of frames the receiver is capable of accepting and buffering.

How It Works:

1. **Initialization**:
    - The sender and receiver agree on the window size at the start of the communication.
2. **Sending Frames**:
    - The sender can send multiple frames, up to the window size, without waiting for acknowledgments. Each frame is assigned a sequence number.
3. **Acknowledgment**:
    - As the receiver processes frames, it sends acknowledgments (ACKs) back to the sender. An acknowledgment typically includes the sequence number of the last correctly received frame.
4. **Sliding the Window**:
    - **On Receiving ACKs**: When the sender receives an acknowledgment, it slides the window forward, allowing the next set of frames to be sent. For example, if the window size is 4 and frames 0-3 are sent, upon receiving an ACK for frame 0, the window slides, allowing frames 4-7 to be sent.
    - **On Timeouts or Errors**: If an acknowledgment is not received within a certain time frame (timeout), or if an error is detected, the sender may retransmit the unacknowledged frames.
5. **Receiver Handling**:
    - The receiver maintains a buffer to store incoming frames and may send acknowledgments for successfully received frames. The receiver's window size dictates how many frames it can buffer before it has to process or discard additional frames.

Example of Sliding Window Protocol:

1. **Initial State**:
    - **Sender Window**: Frames 0, 1, 2, 3 are in the window.
    - **Receiver Buffer**: Empty initially.
2. **Sending Frames**:
    - The sender transmits frames 0, 1, 2, 3.
3. **Receiving and Acknowledgment**:
    - The receiver receives frames 0, 1, 2, 3 and sends an ACK for frame 3.
4. **Sliding the Window**:
    - Upon receiving the ACK for frame 3, the sender slides the window forward, allowing it to send frames 4, 5, 6, 7.
5. **Handling Errors**:
    - If the receiver detects an error or if a frame is missing, it may request a retransmission of that frame.

Advantages:

- **Efficiency**: Increases throughput by allowing multiple frames to be in transit before requiring an acknowledgment.
- **Flow Control**: Helps in managing the rate of data transmission, preventing buffer overflow at the receiver end.
- **Error Handling**: Supports retransmission of lost or corrupted frames.

Summary:

The sliding window protocol enhances the efficiency of data transmission by allowing multiple frames to be sent before needing an acknowledgment, with the window size controlling the flow of data. This protocol is widely used in various network communication protocols, including TCP, to manage data flow and ensure reliable communication.

[23] Explain CSMA in detail. [5]

Carrier Sense Multiple Access (CSMA) is a network protocol used to manage how multiple devices access a shared communication medium, such as a network channel or bus, to avoid collisions and ensure orderly transmission of data. Here's a detailed explanation:

CSMA Overview

CSMA is a protocol used in networking to control access to a shared communication medium by multiple devices. The fundamental idea is that each device listens to the medium before transmitting data to ensure that it is not currently in use. If the medium is busy, the device waits until it becomes free.

Key Principles of CSMA

1. **Carrier Sensing**: Each device on the network listens to (senses) the medium to determine if it is free or occupied before attempting to transmit data.
2. **Multiple Access**: Multiple devices have access to the same communication medium. The protocol ensures that they can share the medium without causing collisions.
3. **Collision Avoidance**: Although CSMA cannot entirely prevent collisions, it helps in reducing the likelihood by making devices listen before transmitting.

Variants of CSMA

1. **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)**:
    - **Used In**: Ethernet networks.
    - **How It Works**:
        1. **Carrier Sense**: The device listens to the network to check if it is idle.
        2. **Transmit**: If the medium is free, the device starts transmitting data.
        3. **Collision Detection**: While transmitting, the device continues to listen to the medium to detect if a collision (another device's transmission) occurs.
        4. **Collision Handling**: If a collision is detected, the device stops transmitting and sends a special signal (jam signal) to notify all devices about the collision. The devices then use a backoff algorithm to wait for a random period before attempting to retransmit.

- **Advantages**: Improves efficiency and reduces the chance of collisions by detecting and managing them in real time.
- **Disadvantages**: Collision detection is less effective in full-duplex systems, where devices transmit and receive simultaneously.

2. **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)**:
   - **Used In**: Wi-Fi (IEEE 802.11) networks.
   - **How It Works**:
     1. **Carrier Sense**: The device listens to the channel to check if it is idle.
     2. **Backoff**: If the channel is busy, the device waits for a random backoff time before checking again.
     3. **Request to Send (RTS)**: To avoid collisions, the device may send an RTS message to the receiver to request permission to transmit.
     4. **Clear to Send (CTS)**: The receiver responds with a CTS message if it is ready to receive. This informs other devices to hold off their transmissions.
     5. **Transmit**: After receiving the CTS, the device transmits its data.
     6. **Acknowledgment (ACK)**: After successful data reception, the receiver sends an acknowledgment to confirm receipt.
   - **Advantages**: Reduces collisions by using handshaking and acknowledgment mechanisms.
   - **Disadvantages**: Adds overhead due to additional control messages (RTS/CTS) and introduces latency.

Summary

CSMA protocols manage access to a shared communication medium by ensuring devices sense the medium before transmitting, thus minimizing collisions and ensuring efficient data transmission. CSMA/CD is commonly used in wired networks, while CSMA/CA is used in wireless networks. Each variant has its advantages and specific applications, depending on the network environment and requirements

[24] Explain PPP. [4] REFER Q9